ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2019;4(2):4-19

RESEARCH ARTICLE

A Critical Study on Security Threats, Issues, and Challenges in the Internet of Things

J. Anvar Shathik[1], Krishna Prasad[2]

[1]Department of Cloud Technology and Data Science, College of Engineering and Technology, Srinivas University, Mangaluru, Karnataka, India, [2]Department of Computer Science and Information Science, Srinivas University, Mangaluru, Karnataka, India

Received on: 25-02-2019; Revised on: 10-03-2019; Accepted on: 15-04-2019

ABSTRACT

Smart grid, smart homes, intelligent water networks, and smart transport are the most infrastructural structures possible today to link our planet. The general vision of such systems is usually linked to a sole notion called the internet of things (IoT). In IoT, the whole solid infrastructure is diligently linked to information and communication technology through the use of networked embedded devices, where smart surveillance and control can be done. In such a sophisticated dynamic system, all instruments are interconnected to provide useful measurement and control instructions through the distributed sensor networks. The way we interact with the world around us is fast changing in technology. We are moving to new networking paradigms, the internet of objects (loT), which maintains data generation and internet communication for greater value and service through the worldwide number of interconnected sensors or intelligent objects. The IoT should facilitate the interconnection and sharing of information and useful data through thousands of devices, people, and services. To revolutionize the way the internet works, the IoT seeks to put together the ideas of machine-to-machine connectivity, big data, artificial intelligence, etc., to operate within a shared framework to interconnect cyberspace and human beings, which contributes to the advancement of cyber-physical systems. The idea of IoT has drawn considerable attention to research as the huge connectivity presents several challenges and hurdles, such as heterogeneity, scalability, safety, large data, and power demand. To achieve a stable IoT implementation, several security concepts on each layer should be enforced. The future of IoT can only be secured by discussing and resolving the security problems associated with it. Several researchers have tried by introducing effective countermeasures to resolve the security issues for IoT layers and tools. To date, there are limited surveys that highlight the challenges and issues of the IoT that has been identified as unique to the future internet and that various research communities must address and address. This paper gives an overview of security principles, technology and security challenges, proposed counter-measures, and future directions for IoT security. So far, a limited number of surveys have highlighted the challenges and issues of the IoT, the unique feature of this future network, and which different research groups have to face and address. To date, there are limited surveys that highlight the challenges and issues of the IoT that has been identified as unique to the future internet and that various research communities must address and address. This paper gives an overview of security principles, technology and security challenges, proposed counter-measures, and future directions for IoT security.

Key words: IoT challenges, distributed sensor network, IoT applications, intelligent analytics, IoT services, actuator networks, IoT security, IoT architecture

INTRODUCTION

The internet of things (IoT) is becoming very hyperbolic because of its promises for a smarter future when things and people communicate with one another through wireless technology. It is also commonly used for accessing digital content and services, and other diverse activities across social network applications were about 2 trillion people are using the internet statistically in their daily work. Together with its creation and its wide use, IoT contributed to borderless relations in different fields and contributed society to a new, so-called “Smart living” level of lifestyle and climate.[2] The idea of

Address for correspondence:
J. Anvar Shathik,
E-mail: anvarshathik@gmail.com

"Smart living" emerged from the Smart City system. The IoT serves as a strategic contact to improve a city's competitive profile in this context. Smart living, a clever economy, an intelligent climate, intelligent people, and smart governance have all been classified as one aspect of the literature. To achieve user-focused goals in terms of safety and protection, access and comfort, smart living is every day in our world separated by digital technology and comprises three basic aspects, which are clever technology, intelligent materials, and intelligent design.[3] Concerning IoT as technological advancement, the theory of the diffusion of inventions shows that consumers are far more likely to adopt new technologies depends on their adoption of the technology and their understanding of their application. If consumers see technology as easy to use, they can easily embrace this technology in their daily life. Privacy and protection are other problems related to IoT. The confidentiality and privacy of the device are important for the acceptance of customers in technology. Although IoT is a challenge, it also provides users with contributions.[4] IoT allows users to track, view, and equilibrium their feelings or mental states, by creating a clever assistance system called ambient and gives people with odd activities a better quality of life. In the sense of smart environments, IoT provides users with access to their data from all devices linked to the network. Many believed that IoT use among society gives the information industry new opportunities.[5] The debates have shown that IoT has been used widely and specifically in conjunction with the creation of intelligent life. This paper aims to provide an overview of IoT literature.[6] The literature was motivated by few research questions: (i) Which relate to the challenges of IoT, (ii) security threats and issues in IoT, and (iii) features and control measures of security in IoT. It is connected to studies and reviews of the internet and social media. The second issue of research is based on the IoT's contribution.

Objectives

The objectives are as follows:

1. To identify and analyze the security issues and different threats in an organization.
2. To analyze the motivation for IoT security and also to identify the different challenges in the IoT security.
3. To analyze the research challenges in IoT and to analyze the various radio frequency identification (RFID) and IoT technologies.
4. To analyze the security features of IoT and enforced to achieve a secure communication framework.
5. To identify the security threats in IoT and security requirements for IoT.
6. To provide the IoT security countermeasures and to establish the IoT secured IoT architecture.

RESEARCH METHODOLOGY

The research is performed using secondary knowledge in journal papers, chapters, and conference proceedings. By properly reviewing the articles, the relevant data are collected and analyses conceptually the security threats, issues, challenges, and the various requirements of IoT discussed in various journals and web resources. This paper discussed the IoT security threats, challenges, and various issues and also addressed IoT countermeasures and the import requirements for IoT security.

RELATED WORKS [TABLE 1]

Table 1: Flow of sensor operation

S. No.	Year	Author(s)	Findings/Focus
1	2015	Mahmoud *et al.*[1]	Security issues such as privacy, confidentiality, authentication, access control, end-to-end protection, trust management, and global policies, and standards are thoroughly addressed, we can see how all IoT will soon change.
2	2014	Keoh *et al.*,[2]	The first step toward an interoperable IoT is to standardize communication security for IoT. There are concerns regarding bootstrapping of devices, key management, licensing, privacy, and IoT messages.
3	2014	Abomhara and Køien[3]	The IoT vision would allow people and objects to be linked to everything and everyone anytime, anywhere, and preferably using any path or network and any services. Although RFID and similar technologies make the IoT definition possible, many potential application areas are open for smart devices. However, RFID and other technologies are feasible.

(contd...)

Table 1: ***(Coninued)***

S. No.	Year	Author(s)	Findings/Focus
4	2017	Krishna and Gnanasekaran[4]	The user should deal with and enforce these data protection, security, and limitations so that the ability of IoT technology can be used in positive applications for the user to sustain the IoT technology and applications.
5	2012	Khan *et al.*[5]	The IoT incorporates intelligence into sensors so that information can be communicated, exchanged, and intelligent decisions automatically.
6	2015	Dixit *et al.*[6]	IoT has the potential to become the next internet creation, with a large number of artifacts such as RFID and various sensor types capable of automated data collection and transmission. There are various challenges as a barrier to loT growth.
7	2018	Farhan *et al.*[7]	IoT simply integrates and interconnects numerous devices using the latest communication and computing infrastructure. This enables data to be seamlessly exchanged and collected and makes useful knowledge possible.
8	2018	Jinda *et al.*[8]	When utilizing sensor data, it is the reliance on cell networks, the importance of data from the different devices, the value of networks along with data centers, the need for a stable service system with remote control possibilities, improvements in interoperability requirements, complexity, and accessibility are several of the challenges.
9	2017	Ryan and Watson[9]	The IoT OR methods are divided into "hard" OR tools and techniques which mainly address the technical and business problems of IoT and systems-thinking approaches that can answer technological, business, and non-technical, including social, legal, and ethical questions. The approaches are often aligned in a variety of ways, which include the OR sub-discipline systems thinking.
10	2013	Mahmoud *et al.*[1]	An attack is an incremental infusion attack process, in which the attacker gathers more information on the life or activities of victims through the combination and connection of information gathered from various intelligent objects owned and controlled by the user.
11	2019	Glaroudis *et al.*[11]	Review and comparison were conducted of application protocols such as MQTT, CoAP, XMPP, AMQP, DDS, REST-HTTP, and Web Socket, based on relevant key indicators.

IoT: Internet of things, RFID: Radio frequency identification, OR: Operations research, MQTT: Message queuing telemetry transport, CoAP: Constrained application protocol, XMPP: Extensible messaging and presence protocol, AMQP: Advanced message queuing protocol, DDS: Data distribution service, REST-HTTP: Representational state transfer-hypertext transfer protocol

IOT ARCHITECTURE

IoT has different layer and each layer in IoT is defined by its functions and the devices that are used in that layer. Various opinions exist about the number of layers in IoT. According to several researchers, the IoT works primarily on three levels, called levels of perception, network, and application. Every IoT layer has related security issues inherent in it. Figure 1 demonstrates IoT's basic architectural structure of three layers concerning the tools and technologies that cover each layer.[1]

Perception layer

This layer is also known as the layer of "Sensors." This layer has the function of collecting data from the environment with the aid of sensors and actuators. This layer identifies, gathers, processes, and then transmits the information to the network layer. This layer also collaborates with the IoT nodes in local and short-range networks.[2]

Network layer

The network layer serves the purpose of data routing and transmission over the internet to various IoT hubs and computers. Cloud storage systems, internet gateways, switching and routing tools, etc., run on this layer using some of the latest technologies including Wi-Fi, LTE, Bluetooth, 3 G, and Zigbee. The network gateways serve as mediators between different IoT nodes by aggregating, filtering, and transmitting data from and to various sensors.[2]

Application layer

The application layer guarantees the authenticity, integrity, and confidentiality of the data. At this

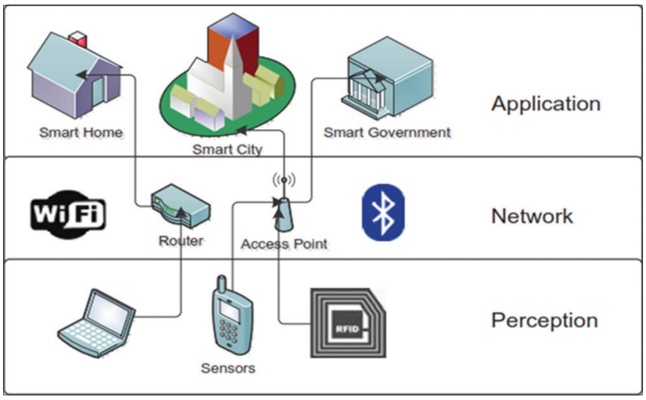

Figure 1: Internet of things architecture

layer, the purpose of IoT or the creation of a smart environment is achieved. The application layer ensures the data are accurate, complete, and confidential. It is an aggregate of the social divide and demand on the IoT and the industry.[2] The layer analyzes the data gathered. It does all the control decisions to get all the recognition, relation, and control information between devices and objects. Intelligence describes allowing the use of smart cloud computing technologies and then transforming the data for better smart power. This layer is also called a process layer.[3]

MOTIVATION FOR IOT SECURITY

The international data corporation expects that by the year 2020 more than 200 million devices will be connected to the internet, with a large portion of these being appliances, there will be a great opportunity for hackers to use their advantage through "Denial of Service" (DoS) attacks, malicious emails from other dangerous Trojans or worms.[4] A recent HP study report says that 80% of IoT devices infringed on the privacy of personal information such as name and date of birth on commercialized IoT deployments, more than 80% failed to provide passwords of adequate duration and complexity and 60% had security vulnerabilities in their user interfaces.[5] The international data corporation expects that by the year 2020 more than 200 million devices will be connected to the internet, with a large portion of these being appliances, there will be a great opportunity for hackers to use their advantage through "Denial of Service" attacks, malicious emails from other dangerous Trojans or worms. A recent HP study report says that 80% of IoT devices infringed on the privacy of personal information such as name and date of birth on commercialized IoT implementations, more than 80% did not allow passwords of adequate length and complexity and 60% had security vulnerabilities in their user interfaces.[6]

COMPARISON OF IOT APPLICATION PROTOCOLS

Latency

The latency of the transmission of data from source to destination (i.e., server to client) is one of the most significant parameters for the assessment of a network's performance and the protocols of that network within the IoT system. The Latinity of the message queuing telemetry transport (MQTT) and constrained application protocol (CoAP) is studied in a clear, uncompromising Local Area Network (LAN) scenario and includes numerous fairly comparative studies.[11] A fascinating comparison has been made, such as CoAP, MQTT, and Web Socket. The authors calculated the round time trip, i.e., the cumulative time from IoT device to server (broker) from starting a packet to receiving server response on the node. In such instances, the IoT system and server were connected by an inter-service provider (ISP) or a mobile network to the same LAN.[12] The findings show that the time between three protocols when MQTT with quality of service (QoS) 0 is used in the case of LAN and ISP connections are comparable. MQTT with QoS 1 has a much greater delay than the packet size. For mobile networks, the QoS 0 MQTT performs best while the QoS 1 protocols are in descending order with CoAP, Web Socket, and MQTT. The LAN is contrasted with CoAP, MQTT, and extensible messaging and presence protocol (XMPP). MQTT QoS 0 looks a little better than CoAP and XMPP has two magnitude latencies higher.[14]

Demand on bandwidth and throughput

A major communication parameter is a bandwidth needed in any telecommunications system, especially in IoT applications in which IoT devices can be too numerous, while the spectrum resources available for the creation of the application are generally limited. For those protocols which have higher overheads and/or need more packet exchanges because their structure and the transport layer used, it is common for the required bandwidth to be higher.[11] The throughput, by comparison, relates to the effective usage of usable spectrum and to the efficiency of the network that is efficiently transmitted per unit of time. Overall, CoAP is subject to lower bandwidth requirements due to the use of the user datagram protocol (UDP) and the least overhead. The use of UDP in CoAP leads, however, to worse performance than MQTT which also exceeds advanced message queuing protocol (AMQP). The worst result was shown by XMPP.[13]

Power consumption and energy

Energy consumption is a parameter of significant importance for IoT since the majority of IoT systems are based primarily on batteries, not on a central supply power supply. For example, energy efficiency and power efficiency are important in the use of IoT application protocols. The life of the sensor battery is tested on an Institute of Electrical and Electronics Engineers (IEEE) 802.11ah IoT network. In all cases, the MQTT and CoAP comparative results showed that CoAP is stronger with a gain decreases of 10–60% when the frequency of message decreases and the size of the messages increases.[12] However, it was clear that the battery life was controlled by the networking protocol and the overall contribution of the application protocol was nearly insignificant.[13] The battery life of IEEE 802.11ah was calculated to be 20 times shorter. The protocols MQTT, CoAP, and HyperText Transfer Protocol (HTTP) showed that the energy consumption of MQTT is marginally lower than that of CoAP, with HTPP much higher than both MQTT was more suitable for IoT messages without power restrictions in basic IoT situations, while CoAP was more effective in terms of power management capabilities.[14]

Recent IoT applications' development

In addition to the comparison of application layer protocol features and performance given in the preceding parts, it is worth noting the preferences in IoT application developer adoption of protocols. Related surveys have been carried out in recent years, namely, 2017 and 2018, by the IoT Working Group on the Eclipse, IoT Initiative, and the Open Mobile Alliance or IoT Council and AGILE-IoT H2020 [Table 2].[13]

CHALLENGES OF IOT

Like many other emerging IT and networking technologies, the IoT also has several obstacles or problems that are raised are discussed in the section below.[3]

Interoperability

IoT needs the ability of various devices at different levels to communicate and share data between them. Since in the IoT, it is important to incorporate many heterogeneous devices and different communication technologies into the interoperability of data produced by the resources of the IoT which poses a great challenge for a generic loT solution at a global level.

Security

Security is one of the key concerns of any industry. One of the important aspects of the IoT is to think about security. It has a broad range of securities such as systems, networks, customers, and data. IoT computer security can open up a range of possible consumer threats through unauthorized access, abuse of customer personal data, and promotion of attacks on other interconnected systems that can affect individuals.[3,5]

Table 2: Comparison of IoT application protocols

Key performance indicator	Most promising protocol				Least promising protocol
Latency					
Over a LAN	CoAP	MQTT QoS0	AMQP	HTTP/REST	XMPP
Over a mobile network	MQTT QoS0	CoAP	WebSocket	MQTT QoS1	
Bandwidth consumption	CoAP	MQTT	AMQP and XMPP	DDS	HTTP/REST
Throughput	MQTT	DDS	CoAP	AMQP	XMPP
Reliability	MQTT	AMQP	CoAP	HTTP/REST	
Energy consumption	CoAP	MQTT	AMQP	HTTP/REST	
Developers preference in recent IOT applications	MQTT	HTTP/REST	WebSocket	HTTP 2.0	CoAP, AMQP, XMPP,DDS
Researchers preference in IOT agriculture applications	MQTT	HTTP/REST	CoAP		

MQTT: Message queuing telemetry transport, CoAP: Constrained application protocol, XMPP: Extensible messaging and presence protocol, AMQP: Advanced message queuing protocol, DDS: Data distribution service, IoT: Internet of things, REST: Representational state transfer, HTTP: Hypertext transfer protocol

Enterprise

The rising volume of data, with the countless devices increasing safety uncertainty, would also pose major security challenges. That, in effect, would impact the availability criteria, which are also expected to increase, placing business processes in real-time at risk.[16]

Storage management

IoT is a mix of different forms of heterogeneous internet tools. Devices produce read-only data or contact with other apps. A large amount of data will still be produced from different parts of the world, and storage management needs a boast to handle these large volumes of data. In fact, storage management will expand unexpectedly as will a number of devices that connect to the internet and start sharing information.[16]

Server technologies

As the loT devices continue to develop, more high-speed calculations needed for these devices can be downloaded to servers. The servers may also include another program, which will need to run a complete loT network. Thus, trends in loT that also influences server technology development. More and more high-end servers are expected to play a key role with more developments in loT.[16]

Data center technologies

Growth in the IoT poses numerous security, capability, and analytics challenges. The re-structuring of data centers is important to retain and processes data produced by a lot of devices effectively. A lot of data generated by the system must be processed, the collection and processing of single data from both technological and financial perspectives will be challenging. "Instead, they need to connect loT-generated data to several, dispersed little data centers are greater, where initial processing may occur to provide a form of real-time capture and reply values."[17]

Lack of common standards

loT is a complex interconnection of heterogeneous sensors, actuators, and software that communicate and exchange information with their protocols. There is no universal standard but development is making developers work with the guidelines. Their absence is one possible concern. For instance, the foundation of Eclipse had its Open loT Stack for Java released. This open-source software platform offers all the major loT specifications and provides the basis for the construction of loT gates and intelligent home automation systems. Similarly, ETSI and oneM2 M are currently under standardization efforts.[15]

Data privacy control

A lot of data is generated by various LOT devices which are used to ensure that the data are privately accessible and stored by a user. It is a critical problem that can facilitate or deter several users around the world. International loT-specific data privacy policies and standards need to be defined and developed. This lets organizations from various parts of the world share and provides their services across national borders and builds customer confidence about the confidentiality of their data when using a loT of products.[16]

Data sharing

The number of consumers buying these goods from different companies has increased accordingly since the loT system will be trillions by 2020. Such customers' data can also be of great use to other businesses. Corporations also provide the nominal cost of such data. This knowledge may be used for various purposes, such as advertisement, product, or service surveys.[17]

Consumer needs

As people take an interest in a loT of technology and take part in various rates, tremendous growth in this sector has been observed in the past few years. This indicates that customer needs and interests play an important role in the advancement of technology. However, some challenges can influence the growth of any sector. If consumers do not believe, for example, that a product or technology needs to be developed in the future, then it may disincentive stockholders to invest capital in the sector, which can also affect technological development. There are few points to promote the need for loT for consumers:[15]

Challenges in big data

IoT collects and aggregates large quantities of data that intelligent objects and is one of the IoT's most striking features. Techniques to translate this data into useful knowledge will need to be created. Data are doubling every 2 years and in the next 4 years are projected to hit 44 bytes. 5Vs are important challenges for IoT applications such as value, velocity, volume, variety, and veracity.[17]

Velocity

Velocity refers the speed of data collection, transmission, and processing. Different speeds for cessation data depend on the application type. In certain applications, data can be managed in a very short time while real-time processing, for example, analysis systems, is available in other applications.[3]

Variety

Variety refers to various forms of data gathered by devices such as smartphones, computers, and senor apps. The data content is unstructured in various forms, including audio, video, pictures, XML, plain text, and C-SV. There should be accurate and coherent management of the variety of data.[16]

Volume

Volume is the sum of all forms of data obtained from various sources, stored, retrieved, and modified. IoT generates massive amounts of exponentially growing data. The question is whether we can combine volume and speed are not.[17]

Value

The next move is to find out the importance of the data once the huge data have been correctly collected. Different algorithms, such as feature extraction, AI trend analysis, enabling informed decision-making within the time frame necessary, thus constitute another challenge.[15]

Veracity

It means making sure that the data gathered and stored are accurate. This might mean filtering out any unwanted or corrupted data to enhance the quality of the application. Veracity refers to the trustworthiness of the data. The quality of the data being analyzed refers to veracity. High-tranquility data contain several important documents that make a major difference to the overall outcomes. On the other hand, low truthfulness data contain a high percentage of insignificant information. Noise is called the invaluable in these data sets. Data from medical experiments and trials will be an example of a high veracity data set.[17]

RESEARCH CHALLENGES FOR IOT

Identification of radio frequency

It automatically consolidates and tracks the electromagnetic fields. RFID is a barcode substitute. For reading printed barcodes, a laser-based optical scanner is used. To define and obtain data, we need a simple view. The benefit of RFID is that there is no need for a sight scan line. RFID is planned as an integral component of IoT.[7] The first term IOT was used over a decade ago by the RFID community. RFID is one of the tools that IOT uses to recognize and link objects to the internet. Virtually every IOT app combines the world of physics and digital. RFID combines these fields with data that define a specific entity at an exact time and location. IoT issues with RFID are that the way lower data are converted into higher data. The study framework for the group discussed the problems in the paper. This system is known as RFID. It provides a small world for IoT projects, societal problems, and device inquiries. They also created and organized a series of IoT web-based user rates and resources into the RFID framework. There are various RFID and IoT technologies.[8]

Architecture

Architecture is a dynamic structure that has been carefully planned. This is the process and the product of structural planning, design, and building. IoT consists of three architecture styles, −3, 4, and 5, as described in Section 2. The design in three layers cannot articulate the IoT's entire features. Hence, the development of a new five-layer IoT architecture is established. The wireless sensor network (WSN) viewpoint is primarily focused on research related to IoT architectures.[9] IoT is an IoT architecture that combines actuators and WSNs with standard networks. A lot of work was done to develop an IoT-based architecture. Specific architectures based on IoT include the accessibility and security architecture in medical settings, the digital traffic safety architecture, the human neural network on the infrastructure of social institutions, an elderly health monitoring infrastructure, and the architecture for intelligent health systems. Energy is regarded as a valuable IoT network resource because of the battery operation of devices required for IoT applications.[11]

Energy efficiency

The IoT has become an omnipresent concept in the past few years, but the possible rise in power demand until now is a forgotten feature of the IoT. IoT objects are considered to be accessible at all times by other objects. It indicates that the system absorbs electricity itself. Enabled devices have already had a global energy consumption of 615 TWh in 2013. The new battery-powered edge devices IoT technology is a pioneer for specific low-power communication requirements.[8] If the battery has to be replaced every few months, the users will not accept and use edge devices. Improving the energy efficiency of powered edge devices is a priority. The key part of the research is already underway for powerful networking in WSNs to set up a green IoT and also a solution to automate systems to incorporate reliable and energy-efficient IoT. A survey on energy management problems and solutions for IoT objects are being carried out in wireless network solutions. An effective and efficient real-time information transmission for cooperative MAC structure, energy-intensive data collection for WSN, and IoT, with comprehensive sensor sensing at the sensor node and power-efficient sensor nodes for fall detections network, are also suggested.[9]

Smart home

There are many devices in the houses today to entertain the people living in them and to sustain them. Home automation is targeted at the community of all apps and applications used for comfort and protection by consumers.[7] Domestic automation systems include lighting, heating, ventilation, door control, and window control in general. The home automation system includes integrated network components with various specifications such as future-professional, moderate cost, setup effort, overhead implementation, accessibility, and safety and user interaction. A network that serves the growing aspects of home automation is IPv6 and low-power wireless personal area network (6LoWPAN) while concepts from the web support consumers and developers alike.[9] The combination of keep in touch technology and closed-loop health-care services provides home automation for older people in IoT. A lot of home automation has been achieved with wireless local area network a low-cost energy efficient, intelligent home, with arduino based tasks, cloud-based networks, and mobile devices, ZigBee, android, web-based IoT, and cloud-based smartphone. Many other traditional approaches for smart home architecture based on IoT are further suggested.[10]

SECURITY THREATS IN IOT

The three key problems with IoT are anonymity, the confidentiality of business processes, and third-party capability. It is recognized that the IoT environment has communicated through public untrustworthy networks four interconnected components, such as people, objects, software, and hardware. Security, privacy, and open confidence issues must be addressed.[3] Therefore, as addressed herein, concerns concerning users, servers, and trusted third parties should be answered. Safety can then be defined as an organized framework of concepts, beliefs, principles, policies, procedures, techniques, and assurances that are necessary to avoid deliberate or unexpected threats to system assets and the system as a whole. The rest of this section discusses several IoT-related attacker models, an overview of IoT security problems, and IoT security requirements. All such interactions shall also be protected through one means or another to ensure that all interested Parties have information and service provocation and to limit the number of incidents that affect the entire IoT.[15]

Intruder model

A Dolev-Yao (DY) form of an intruder is usually believed. It is a network-operating attacker that can intercept any or all messages passed between IoT-devices and hubs. The DY attacker meets the NSA significantly. However, while the potential of these attacks is somewhat unlikely, it should be noted, “these attacks just strengthen, they never get worse.”[16] Therefore, the protection from our IoT infrastructure is considerably higher to be immune from DY intrusions. We assume that physical compromises are not great and therefore, in the worst-case scenario, only affect a limited number of IoT devices. The IoT architecture must, therefore, be configured to deal with compromising devices and to be able to detect them.[17]

Denial-of-service (DoS) attacks

This kind of attack aims to discourage planned devices and/or network users. Most IoT devices are vulnerable due to low memory space and limited machine resources to attacks by resource usage. Moreover, the vast majority of security measures involve a high overhead device and are not sufficient for resources managed by IoT. Because IoT attacks can often be highly expensive, researchers have arranged extraordinarily to distinguish between different types and techniques to prevent attacks. There are several DoS attacks, such as intercom channels and computer resources such as bandwidth, memory, disk space, or processor time that can be initiated against IoT.[16]

Physical attacks

Such assault tampers with hardware components. Due to the volatile and distributed nature of IoT, most equipment is typically vulnerable to physical attacks in outdoor environments.[15]

Attacks on privacy

As IoT provides large volumes of information through remote access mechanisms, privacy protection in IoT is becoming more and more difficult. To monitor the adversary, the information collected with very low risks should not be physically present. The most popular attacks on user confidentiality include elimination and passive monitoring, traffic analysis, and data mining.[16]

CHALLENGES IN THE IOT SECURITY

The IoT is a multi-domain environment with a wide range of devices and services connected for information exchange. The protection, confidentiality, and trust requirements of each domain can be met. There are several barriers to protection and privacy to build safer and more easily available IoT devices and services at low costs. Such problems are mentioned below.[3]

User privacy and data protection

IoT protection is an imperative problem for the omnipresent nature of the IoT world. Things are interconnected and data are communicated and shared through the internet, making user privacy-sensitive in many research projects. Through extensive data protection work has already been carried out, many topics need to be further studied. Information collection protection, data storage and control, and data security continue to be accessible for study.[15]

Authentication and identity management (IDM)

The process and technology used to manage and ensure secure access to and protection of information and resources are a combination of authentication and IDM. In the case of the IdM, authentication should be checked for the identity establishment between two communicating parties.[15] It is important because many users and devices will trust one another, to look at how identity authentication can be handled in the IoT. There have been many of these open science issues, for example. To identify all uniquely, an effective IDM approach should be established. Mobility, confidentiality, pseudonyms, and anonymity aspects need further investigation and analysis.[15]

Trust management and policy integration

Trust plays a key role in building stable communication between objects in an unpredictable IoT environment. IoT will take two dimensions of trust into account: Confidence in interactions between individuals and confidence in the system from the users’ point of view. In the context of IoT, the primary goal of confidence research is to first create new decentralized trust models.[16] Second, it introduces cloud computing trust mechanisms and, third, build applications based on node faith. Applications based on confidence should be developed in a complex and collaborative IoT-environment. Automated trust assessments should be carried out, preferably independently. There are several ideas for automatic confidence assessment and one of the most important of them is the reputational subjective logic method.[17]

Authorization and access control

The authorization permits you to determine if a person or entity may once establish a resource. Control access means controlling access by granting or refusing access to services in compliance with a set of criteria. Access controls generally carry out the authorization. For authorization and access control, a safe link between a variety of devices and services is crucial. The main problem, in this case, is to allow access control rules to be developed, understood, and manipulated. The next access control provides additional detail.[15]

End-to-end security

At endpoints between IoT and IoT applications, protection is equally important. For IoT-restricted tools, it is not enough to use encryption and authentication mechanisms in packets. For packets, it is not enough. Protocols and algorithms must be reliable and safe for verifying individual identities for both purposes for full end-to-end security. At the end of the game, IoT protection means that both ends usually depend on a non-accessibility contact and that nobody else can change the data while on the go. Proper and comprehensive security, which would not be possible without many applications, is important.[16]

Attack resistant security solution

A variety of computers with different memory volumes and limited computer resources are connected to the internet. Such tools can have security solutions that are resistant to threats and lightweight because they can attack. Devices will allow for external mitigation measures such as service denial, flood attacks, and more.[15]

SECURITY REQUIREMENT FOR IOT

IoT has been one of the main components of the future internet with an immense effect on the social and business climate. In the face of attacks or identity theft, more IoT applications and services are vulnerable. Advanced technology is required in several areas to protect IoT against these attacks. Authentication, confidentiality, and integrity of data are more important.[3,16] IoT security issues. Problems to prevent data theft, authentication is required to connect the two devices and exchange some private and public keys through the node. Privacy means that the data are secured from unauthorized users in an IoT program. Data integrity prohibits any alteration of human in the middle data, ensuring the data inserted into the receptacle stays unchanged and passed on by the sender. A series of IoT safety components are presented.[18] In dealing with IoT protection concerns, Vermesan and Friess addressed security and privacy criteria as follows:[19]

- Lightweight and symmetric solutions to support resource-constrained devices.
- Lightweight key systems for the management to enable confidence and the distribution of encryption materials through minimal communications and processing resources, per the resource, restricted nature of many IoT devices.
- Cryptographic techniques allow the processing and sharing of protected data without access to other parties.
- Concept supporting techniques, including data identification, anonymity, and authentication.
- Keep as local as possible information utilizing decentralized computers and key management.
- Prevention of the privacy of the location and personal information that people may want to keep private through IoT-related exchanges.

IOT SECURITY ISSUES

IoT is also subject to the typical security objectives of privacy, integrity, and availability (CIA). However, IoT is subject to several parts and system constraints, machine and power supplies, and also the omnipresent and heterogeneous existence of IoT that raises more concerns. This area comprises two parts: The general safety features the IoT requires and the protection problems for each IoT layer.[16]

The security features of IoT

IoT's safety challenges can be split into two classes; technical challenges and security challenges. Due to the heterogeneous and omnipresent existence of IoT devices, technological challenges emerge while security challenges relate to values and functionality to achieve a safe network. Technological challenges usually relate to wireless technologies, scalability, energy, and distributed character, while safety issues need to be guaranteed through authentication, confidentiality, end-to-end safety, integrity, and so on. In the entire production and operating process of all IoT devices and hubs, protection should be implemented in the IoT. Safety is maintained by different mechanisms.[20] All IoT devices should be required to have applications running. When an IoT is enabled, authentication into the network will first take place before the data are collected or sent. Since the computing and memory bandwidth of the IoT devices is minimal, in the IoT network firewalling is required to filter device-directed packets. The system updates and fixes should be enabled in a manner that does not consume additional bandwidth. Given below are the security principles that should be enforced to achieve a secure communication framework for the people, software, processes, and things.[22]

Confidentiality

The confidentiality and availability of the information are extremely essential for approved users only. In IoT, a user may be people, machines, and services as well as internal and external objects. For instance, it is important to ensure that sensors do not disclose the data they collect to the next nodes. Another question of confidentiality is how the data are to be handled. It is essential for IoT users to become aware of the processes for data management, processor manager, and to ensure that the information is protected during the entire process.[21]

Integrity

IoT is focused on the sharing of data between different devices, which is why it is very important to ensure the integrity of the data; to make sure that it comes from the correct source and that data are not corrupted by intended or unintended intervention in the transmission process. Through holding the end-to-end protection in IoT communication, the honesty function can be enforced. The data traffic is handled with firewalls and protocols, but due to the characteristics of low processing capacity at IoT nodes, it does not guarantee security at endpoints.[21]

Availability

IoT's dream is to connect as many intelligent devices as possible. All data should be available for the users of the IoT whenever needed. However, information is not the only component used in IoT devices and services do need to be accessible and available on time to meet IoT requirements.[16]

Authentication

Every IoT object must be able to recognize other objects clearly and authenticate them. However, because of the existence of IoT, this method may be a great challenge; many entities are involved and one thing is that objects can need to first communicate with others. For all of this, in every IoT interaction, a mechanism is required to authenticate entities with each other.[20]

Lightweight solutions

Lightweight solutions are a unique security feature introduced due to computational and power limitations on IoT-related devices. It is not a target in itself but a constraint that must be taken into account when designing and enforcing protocols, whether for IoT data encryption or authentication. Because these algorithms should be operated on limited IoT devices, they should be compatible with the device functionality.[22]

Heterogeneity

The IoT links various organizations with varying capacities, sophistication, and numerous suppliers. The devices have different dates and release versions, use various software interfaces and bit rates, and are designed for a whole range of functions such that protocols can operate in all various devices and circumstances. IoT is intended to connect computers, humans and computers, and human beings to human beings, and thus to link heterogeneous objects to networks.[21] The further difficulty in IoT is that the world is constantly evolving and that a computer may at once be connected to a whole different set of devices. Moreover, an effective key management and authentication protocols must be given for an efficient security cryptography scheme.[22]

Policies

Policies and standards must be established to ensure that data are properly handled, secured, and passed on, but more importantly, a process is required to implement these policies and ensure that every organization follows the standards.[20] In each service involved, service level agreements must be identified. Because of its heterogeneous and dynamic nature, existing policies that are used for computer and network safety may not apply to IoT. The introduction of these policies would build trust among human users in the IoT paradigm, resulting in its growth and scalability.[21]

Key management systems

The devices and IoT sensors need, to ensure that the information is secret, to share some encryption materials. To that end, a lightweight key management system must be developed for any framework that can enable.[22]

IOT SECURITY COUNTERMEASURES

IoT requires security measures across all three layers. Across order to protect confidentiality, authentication, and integrity, IoT requires physical data collection, network routing, and transmission layer and application layer. This section discusses the state-of-the-art safety measures that cover the specific characteristics and safety objectives of IoT.[2]

Authentication measures

A mutual authentication pattern was established by Zhoa in 2011. Hash and extract function is the basis of the scheme. The extraction feature was combined to prevent collision attacks with the hash function. Besides, this scheme offers a strong IoT authentication solution. The extraction of functionalities has the properties of irreversibility needed to ensure protection and is suitable for IoT lightweight. If the application tries to pass data to terminal nodes, and not the reverse, the system focuses on the authentication method. While the device increases safety by minimizing the amount of information sent, it only works theoretically and there is no real evidence to support it.[20] The other approach to IoT sensor nodes is one cipher method once based on a question response mechanism. A pre-share matrix between communicator parties is used to implement this dynamic variable cipher. A random coordinate is generated by the parties to be the coordinate. The key coordination is the thing that is transferred, and not the key itself, between two parties. This coordinate will then generate the key, i.e., password. By encryption of all messages, the username, the system ID, and time stamp are included with the username. The two devices interact by time signals so that the session can be canceled based on them.[20] This chip can be used where IoT protection is not very fragile and critical since the key for various coordinates can be replicated. The security for this particular IoT framework can be improved if the key coordinates are regularly changed. To enforce this task for a large number of IoT devices, the installation of the pre-shared matrix must be safe. Correct access controls are as important as security authentication, and both of these functions are part of IoT security.[21] The IoT Authentication Identity and Capability-Based Access Control were provided for addressing these functions. This research aims at filling the gap with the authentication and access control capabilities of an integrated protocol to achieve mutual identity in IoT. It is consistent with the lightweight, mobile, distributed, and calculation-related nature of IoT equipment plus existing Bluetooth, 4 G, WiMax, and WiFi technologies. The proposed model uses a public key approach.

Trust establishment

Given that IoT devices can shift physically from one owner to another, trust between both owners should be generated to allow a smooth transfer of the IoT device for access control and permissions. The research introduces the idea of reciprocal confidence in IoT protection through the establishment of a system for access control at the item level.[3] It creates confidence from the production to the operation and transfer of IoT. Two mechanisms build the confidence: The token and the development key. A creative key is allocated by an entitlement program for each new computer that is created. The system manufacturer shall apply this key. The token is designed by the manufacturer or the existing owner and is combined with the device's RFID identification. This mechanism guarantees the device's change of permissions if a new proprietor is named or worked in another office of the same corporation, thus minimizing the new owner's overhead.[20] The owners can alter these tokens if the old token is given to supersede the previous one's permission and access control. This is like replacing the old key when you buy a new home.[21]

Federated architecture

It is difficult to control security because there are no universal policies and standards to control the design and implementation of algorithms in IoT. To overcome the heterogeneity of various devices, software, and protocol, an internal autonomy or centralized system is essential for IoT architecture. The papers suggested a description of Federated IoT, and a model for Access Control Delegation is presented based on this definition. The model presented takes the flexibility and scalability of key features of IoT systems into account. A further attempt has been made to propose a framework for critical infrastructures called the Secure Mediation Gateway (SMGW).[3] This approach is an abstraction of IoT as its relevance is completely different in nature and its operation for any type of distributed infrastructure. SMGW can discover the necessary distributor knowledge from various nodes and can solve the heterogeneity of heterogeneous nodes, whether it be a telecommunications and an electrical, and water distribution node. An additional attempt was made to suggest the SMGW system for critical infrastructure.[20] This method is an abstract of IoT since its application to any distributed network is completely different. SMGW can detect the required knowledge of distribution from various nodes and can solve the heterogeneity of the heterogeneous nodes, be they electrical, water-distribution nodes.[21]

Security awareness

The presence of human users in the IoT network is an essential measure of protection for the success and development of the IoT system. The effect of not using real numbers protecting the IoT. They had access to the IoT devices that had been available publicly through either no-password or by default password. The results recorded were very interesting, and many of these devices were indeed accessible.[20] If people kept on ignoring security and used the minimum quantity of security as the product's default password, this would make the IoT more harmful than good. If one of its devices is not protected, hackers can target the entire network. Confidence between various things and distribute keys through minimum device capabilities.[22]

SECURED IOT ARCHITECTURE

The protection at all levels must be assured by IoT. Therefore, the protection of the whole device, crossing the percept layer, network layer, middleware layer, and application layer, will also refer to IoT security [Figure 2].[4]

Perception layer

Physical security policy

The lower layer of IoT is the perception layer. The acquisition of information across the entire IoT network is irresponsible. Implementation of physical protection of the perception layer shall include security issues including information acquisition security and physical security of equipment such as sensor units, RFID nodes, and sensor terminals.[4]

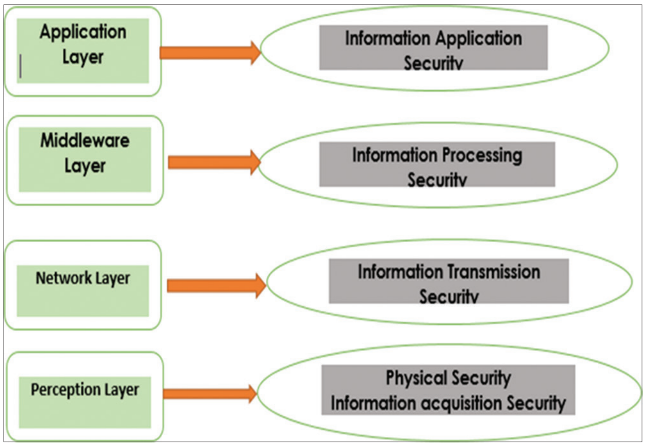
Application Layer
Information Application Security
Middleware Layer
Information Processing Security
Network Layer
Information Transmission Security
Perception Layer
Physical Security
Information acquisition Security

Figure 2: Secured internet of things architecture

Sensor network security policy

Network sensor technology is subject to limitations including catching sensor nodes and gateway nodes physically, attacks for integrity and congestion, DoS attacks, eavesdropping, and replication at nodes. Security policies such as encryption algorithms, key distribution policies, and mechanisms for intrusion detection must be included for building a safety framework for the sensor network. Two of the current security frameworks are the Tiny sec lightweight extensible authentication protocol.[4,23]

RFID security policy

In addition to physical security concerns, it is the responsibility of the sensor to deal with issues relating to the security of information acquisition. Some of the possible attacks include security issues such as wiretapping, tampering, cheating, and replay.[23]

Information acquisition security policy

In addition to physical security concerns, it is the responsibility of the sensor to deal with issues relating to security of information acquisition. Some of the possible attacks include security issues such as wiretapping, tampering, cheating, and replay.[23]

Network layer

Information transmission security policy

The main task of the network layer (second layer) in IoT architecture is to transfer information over the network. As IoT is implemented in the fundamental communication environment, it is susceptible to several attacks, such as DoS attacks, man-in- middle attacks, gateway attacks, and storage attacks. The network can be carried out to prevent such attacks through key management, authentication, intrusion detection, and negotiation.[24]

Middleware layer

Information processing security policy

The middleware layer is responsible for information retrieval and for providing the network layer-application layer interface of the IoT layered architecture. Some of the technical issues currently in existence relate to middleware protection, security, and reliability. Make the middleware layer more stable, ensure confidentiality, and safe storage.[24]

Application layer

Information application security policy

To guarantee unauthorized access and use of data, privacy is the main component of application-layer security. The technology for data manipulation and data encryption are a few techniques that can be used to guarantee the protection of a database through the standard protection security technologies. Data backup and recovery processes have to be performed properly to maintain data protection.[24]

SWOC ANALYSIS

IoT represents innovation clearly. It combines everyday devices with streamlined results. SWOT analysis of the IoT reveals the strengths, weaknesses, opportunities, and threats in this new technology [Table 3].

DISCUSSION AND FUTURE WORK

The world has already begun to see the impact of the internet by realizing the maximum potential of the internet on various applications. The technology used in the IoT certainly needs to overcome the practical challenges of its implementation. Rapid progress in IoT has resulted in a significant problem in the growth of security mechanisms in IoT architecture. While the protection application of IoT is investigated, other areas of safety also need to be studied even more thoroughly. In this paper, security

Table 3: SWOT analysis of IOT

Strength	Weakness
Cost reduction Public interest Innovation Environment friendly Ease of use Beneficial to the workplace	Security Data challenges Huge investments No road map Data is heavy
Opportunities	**Challenges**
Healthcare application Wearables Infrastructure management Making computers more ubiquitous Exciting investment opportunities	Vulnerability to hacker Lack of demand due to high cost Expansive

problems were discussed in every layer in IoT architecture and acceptable strategies for the secure construction of IoT architecture, which can be enhanced with future technical prowess. Besides, problems such as naming and IDM were addressed in the effective realization of IoT standardization. Future research into IoT security issues shall focus on physical hardware security, privacy, and network transmission of information. In addition to effective technical approaches, implementing safe IoT also calls for a range of policies, legislation, and regulations.

CONCLUSION

There are numerous security challenges and requirements that must be addressed. The IoT frames are subject to attacks on every layer. The current state of research in IoT is mainly based on authentication protocols and access control protocols. However, the rapid advance of technology requires the introduction of new networking protocols such as IPv6 and 5 G to achieve the complex mash-up of IoT topology. Various safety issues must be addressed if the IoT architecture is to be expanded from one business to several various companies and systems. The IoT can make a huge difference in the way we live today. However, safety is the main concern when implementing fully intelligent frameworks. If security issues such as confidentiality, authentication, access control, end-to-end safety, trust management, global policies, and standards are fully addressed, we will see everything transformed by IoT soon. The challenges in IoT, such as the requirements for heterogeneous devices, the introduction of key management and identity establishment systems, and the development of trust centers, are currently open to study and involve new identification, software, and hardware technologies. The IoT model originated over the past decade. The IoT has resulted in various risks and attacks against protection or privacy. In this paper, we expressed that the widening of the surface area for external attacks is the product of more and more IoT applications. We have classified and discussed these attacks with possible solutions using the layers of the IoT architecture. We have also summarized existing safety methods and their limitations in different layers so that users can maintain IoT technologies and applications, these concerns and limitations of privacy and security must be resolved and enforced to allow productive applications to exploit the potential of IoT technology. This information will serve as an important contribution to the research community by documenting the current use and security attacks in different layers and by motivating young researchers to create new protocols to deal with security problems concerning the IoT.

REFERENCES

1. Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. Int Conf Intern Technol Secur Trans 2015;1:336-41.
2. Keoh SL, Kumar SS, Tschofenig H. Securing the internet of things: A standardization perspective. Intern Things J IEEE 2014;1:265-75.
3. Abomhara M, Køien GM. Security and privacy in the internet of things: Current status and open issues. Int Conf Priv Secur Mob Syst 2014;1:1-8.
4. Krishna BV, Gnanasekaran T. A systematic study of security issues in internet-of-things (IoT). Int Conf IoT Soc Mob Analyt Cloud 2017;2:107-11.
5. Khan R, Khan SU, Zaheer R, Khan S. Future of internet-the internet of things architecture, possible applications and key challenges. Int Conf Front Inform Technol 2012;1:257-60.
6. Dixit M, Kumar J, Kumar R. Internet of things and its challenges proceedings. Int Conf Green Comput Intern Things 2015;1:810-4.
7. Farhan L, Kharel R, Kaiwartya O. A concise review on internet of things problems, challenges and opportunities. Int Symp Commun Syst Netw Dig Sign Proc 2018;1:1-6.
8. Jinda F, Jamar R, Churi P. Future and challenges of internet of things. Int J Comput Sci Inform Technol 2018;10:13-25.
9. Ryan P, Watson R. Research challenges for the internet of things: What role can OR play. Open Access J Multidiscip Dig Publ Inst 2017;5:1-32.
10. Elkhodr M, Shahrestani S, Cheung H. The internet of things: Vision and challenges. IEEE Tencon Spring 2013;1:207-11.
11. Glaroudis D, Iossifides A, Chatzimisios P. Survey, comparison and research challenges of IoT application protocols for smart farming. Sci Comput Netw 2019;1:2-24.
12. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 2015;4:2347-76.
13. Dragomir D, Gheorghe L, Costea S, Radovici A. A survey on secure communication protocols for IoT systems. Int Workshop Secur Intern Things 2016;1:47-62.

14. Sethi P, Sarangi SR. Internet of things architectures, protocols, and applications. Hindawi J Electr Comput Eng 2017;1:1-25.
15. Mahalle PN, Anggorojati B, Prasad NR, Prasad R. Identity authentication and capability based access control IACAC for the internet of things. J Cyber Secur Mobil 2013;l:309-48.
16. Romana R, Zhoua J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Comput Netw 2013;57:2266-79.
17. Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Security model and threat taxonomy for the internet of things. Commun Comput Inform Sci Springer Berlin Heidelb 2010;89:420-9.
18. Tzounis A, Katsoulas N. Internet of things in agriculture, recent advances and future challenges. Biosyst Eng 2017;164:31-48.
19. Atzori L, Iera A, Morabito G. The internet of things: A survey. Comput Netw 2010;54:2787-805.
20. Zhao K, Ge L. A survey on the internet of things security. Int Conf Comput Intell Secur 2013;1:663-7.
21. Leo M, Battisti F, Carli M, Neri A. A federated architecture approach for internet of things security. Eur Med Telco Conf 2014;1:1-5.
22. Farooq MU, Waseem M, Khairi A, Mazhar S. A critical analysis on the security concerns of internet of things (IoT). Int J Comput Appl 2015;1:111.
23. Ning H, Liu H, Yang LT. Cyberentity security in the internet of things. EEE Comput Soc Comput 2013;46:46-53.
24. Matharu GS, Upadhyay P, Chaudhary L. The internet of things: Challenges and security issues. *Int Conf Emerg Technol* 2014;1:54-9.
25. Verma R, Chandra S. Security and privacy issues in fog driven IoT environment. Int J Comput Sci Eng 2019;7:367-70.