March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

DDOS Attacks in Application Layer Security and Privacy Requirements for Internet of Things

KOLLA VIVEK, SYAM KUMAR DUGGIRALA, K.PARISUDDHABABU
Department of Computer Science and Engineering
Vignan's Lara Institute of Technology & Science, Vadlamudi, Guntur.
Email: kollavivek@gmail.com, syam.kumar1258@gmail.com, kp.vlits@gmail.com,

Article Info
Volume 83
Page Number: 21584 – 21604
Publication Issue:
March – April 2020

Article History
Article Received: *19 August 2019*
Revised: *27 November 2019*
Accepted: *29 January 2020*
Publication: *6 May 2020*

Abstract-
The Internet of Things (IoT) is one of all the growing technology that has grabbed the attention of researchers from domain and company. the thought within the back of Internet of things is that the interconnection of Internet enabled topics or gadgets to each precise and to people in general, to advantage a number of common dreams. In near to destiny IoT is anticipated to be seamlessly lined into the environment and human could be actually clearly installation during this amount for comfort and simple life fashion. Any protection compromise of the device can at once have a sway on human lifestyles. Therefore protection and privacy of this era is major necessary drawback to resolve. In this paper we tend to gift an intensive check of protection problems in IoT and classify possible cyber attacks on every layer of IoT type. we tend to in addition communicate disputes to straightforward safety answers that embody crypto logical solutions, authentication mechanisms and key manipulate in IoT. Device authentication and acquire right of access to controls is associate degree important place of IoT safety, that is not surveyed up to now. we tend to spent our efforts to preserve the dominion of the art work device authentication and acquire right of access to control ways on a divorced paper.

Keywords*-Internet of Things, Authentication, Access Control, Security, Cyber-attacks, Wireless Sensor Internetworks*

1. INTRODUCTION:

The Internet of Things (IoT) was primarily anticipated in 1999 as a revenue to apprehend inter-connection and information exchange among devices. [1,2]. The huge positioning of IoT makes data security unprecedentedly imperative [3].The term net of things was developed by Kevin choreographer, administrator and founding father of Auto-ID Centre at Massachusetts Institute of Technology [5]. the majority of connected devices is growing exponentially, forming an enormous networks linking sensible devices like sensors and actuators, the alleged net of Things, such systems area unit enforced in numerous fields like sensible demotics, Smart city, sensible health, e-governance, e-education, retail, logistics, Industrial producing and business method management etc.[6]. It permits electronic factor, technology, embedded product like phones, vehicles and alternative electronic devices to be controlled and addressed on net via sensors and actuators victimisation wired or wireless property. Anyone at any time will connect with objects at remote or distance locations via path or network. IoT describes the network connected capability of the computers and every one the various varieties of objects in setting with minimum human interface the objects exchange information with alternative devices on the net.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

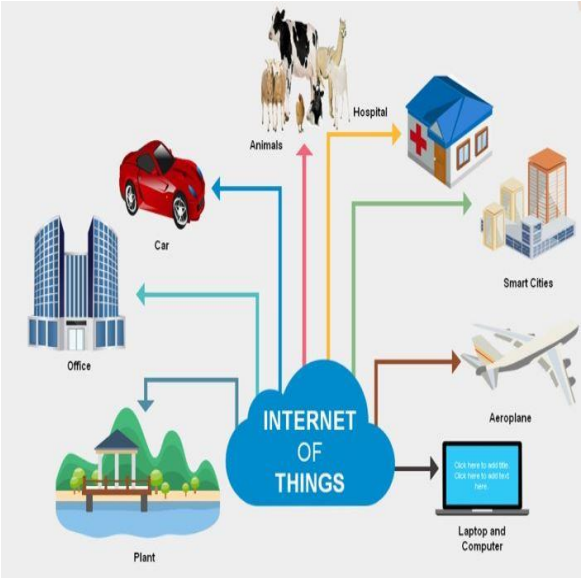


Fig.1:Applications fo IoT

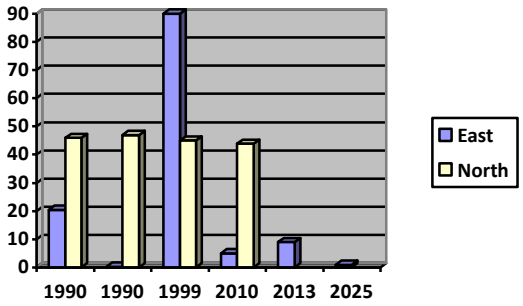
Let us look into definitions that area unit preferred. The International Telecommunications Union (ITU) gave a typical definition in 2012, "A international infrastructure for the knowledge society, enabling advanced services by Interconnecting (Physical and virtual) things supported, existing and evolving, practical data and communication technologies". The IoT was delineate by the net design Board (IAB) outlined as "Internet of Things denotes a trend wherever an oversized variety of embedded devices use communication services offered by the net protocols. Several of the devices, usually known as sensible objects", aren't Strait forwarded by humans, however exists as elements in buildings or Machines are a unit displayed within the atmosphere.

In Atzori et al.[9], diversity of things like sensors, RFID tags , actuators and mobile phones which might move with one another to realize a typical goal". equally from the read of a wise atmosphere, In Gubbi et al.[11] the authors delineate as " Interconnection of sensing and activating devices providing the power to share data across plat-forms through a unified framework, developing atypical operative image for enabling innovative application. Additionally Guillemin and Friess et al.[12] , the authors outlined as "The net of Things permits folks and things to be connected Any time, Any place , anybody with something, ideally victimisation any path or network and any services.

Earlier the IoT afoot with Machine to Machine communication. It indicates 2 machines interactive among themselves, routinely while not human participation in each wired and wireless communication. Here we tend to area unit victimisation 2 finish points for exchanging the knowledge within the systems [4]. It affords a platform to transfer between the objects, that area unit self-organize ,identify themselves victimisation (RFID) frequence identific ation, angular shape Bee and Wireless device network etc. for effective communication [2]. IoT development is step by step inflated altogether the areas and therefore the survey chart is as shown below [6].

Table.1: Survey from 1990 to 2025

Year	Number of Connected Devices
1990	0.3 million
1999	90.0 million
2010	5.0 billion
2013	9.0 billion
2025	1.0 trillion(expecting)



The IoT runson a three-tier architecture. They areapplication, INternetwork and Perception tiers. The application tier is responsible for collecting, analysing, processing the data which is needed. The INternetwork tier is the core of IoT is responsible for reliable and accurate tranfer of data which is collected from end nodes among various wired and

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

wireless INternetworks. And at last the perception tier is responsible for maintaining the different types of sensors like temperature, RFID, proximity sensors etc., every sensor is going to capture the contemts.

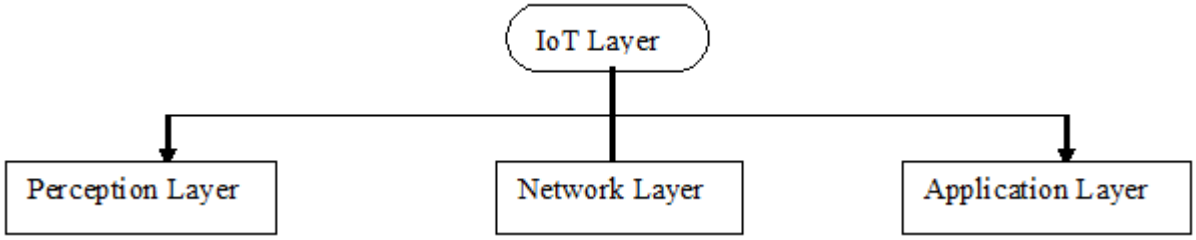


Fig.2:IoT Layers

The victory of the applications and infrastructure of IoT be contingent on IoT security[7]. The security problems like privacy, verification, system configuration, authorization, information storage and management are the real challenges of the IoT Infrastructure. So, the best security principles and standards requirements are essential to advance the IoT Security[8]. All the layers of the protocol stack are defenseless to from the security attacks and threats. So the physical security techniques must be introduced for the securing the IoT from the threats[11].

This paper is planned like, Section I is all about the introduction of IoT layers, applications of IoT and its security measures in all layers. Section II recalls the IoT Functional Model of IoT, Security Architectrure, major security challenges and requirements of IoT. It also exposes a figure ofIoT security architecture. Section III will explains about the authentication protocols of existing IoT technology depending upon the three different types of classification criterias.

Motivation

The Internet of things ought to income consumer's receive as proper with to be drastically conscious of the resource of the enterprise. For attaining consider of shopper IoT have to be compelled to affirm strong protection and privacy of its purchasers. though it is a particularly lively evaluation material, there could additionally be very little or no art work revealed, that analysis the security of IoT. But the art work isn't always updated. As new threats in IoT region unit recognized terribly regularly conseq uently we have a tendency to felt a want of ultra-modern and whole evaluation of IoT protection to information investigator some their efforts wished in unique security space. Besides this facilitate layer security in IoT is now not referred to in on the market opinions. we tend to fell the gap with the assist of characteristic and discussing various resource layer security troubles in our paper. Authentication and gather admission to control should be a remarkable protection mission in IoT and lots of labor has been completed inside the place. we offer a have a glance at of the present day authentication and accumulate proper of entry to control mechanisms in IoT.

2.ARCHITECTURE OF IoT

The architecture of IoT Functional Model is shown below. It contains seven functionality groups complimented by two groups they are management and security. The management functional group is responsible to provide the practical concepts essential to theoretically integrate the peculiarities of the IoT world into business processes. The Service Organisation is a dominant Group that acts as a communication hub between several other Groups. The Virtual Entity and IoT Service are responsible for communicating the data among the different levels of abstraction.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

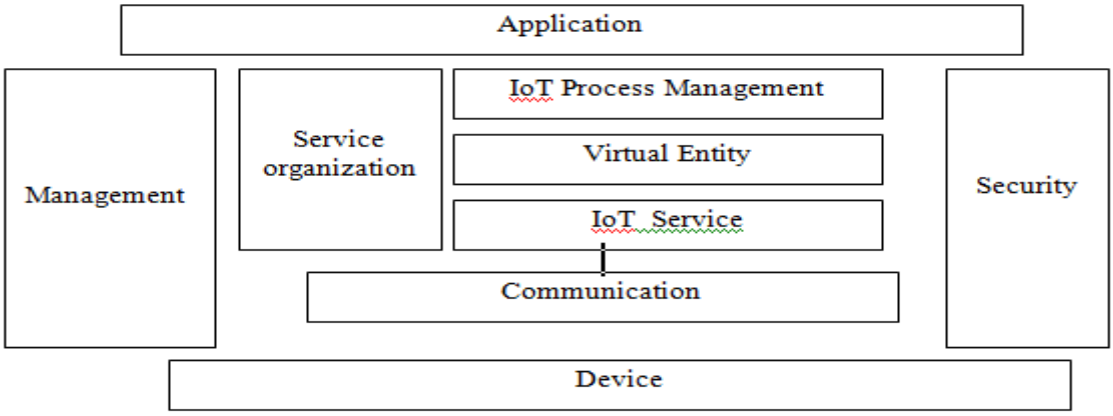


Fig.3: IoT Functional Model

The Communication group summarises the different types of schemes for the interaction which are derived from different technologies which are belonging to different IoT systems and it also provides a similar interface to the services of IoT. It also provides a simple interface for managing the higher level information flow. The management functional will governs all the functions and combines which are need to IoT services. The security group is going to provides different types of security measures and privacy mechanisms of IoT systems. The applications are already discussed earlier and the devices here we will consider are the end systems. These are the different entities which are priticipated under the processing of the functional model of IoT.

SECURITY IN INTERNET OF THINGS (IOT)

Besides massive significance and massive programs of IoT, It is not clean to set up it in project imperative software areas, whereby safety and privateness is of most essential worries. For example a a achievement safety assault on sensible healthcare desktop can intent in loss of many lives of sufferers, at the same time as it may also additionally motive in move Internet loss, and lack of human lives in case of clever transportation device. Security of IoT is a challenging vicinity and require similarly research paintings to cope with these stressful conditions. We speak those security challenges Depending upon the several technologies like cellular Internetworks, sensor Internetworks and the Internet. The term Internet is becoming the IoT [4]. So the IoT system should be free from the security issues and which has to defend the scalability and flexibility of security problems.

Application Service Data Security	Safety Guarantee System
Access and core INternetwork and information security	
Perception layer INternetwork transmission & information Security	
Perception layer local security	

Fig.4:Security Architecture of IoT

.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

Once the attacker gain access on these vulnerabilities then he can exploit the total layer an the main target they focuses oin how to gain acces on authentication, confidentiality, integrity abd other security services [3]. Compromising the security at the specific layer is is vulnerable because of some system flaws and weakness.

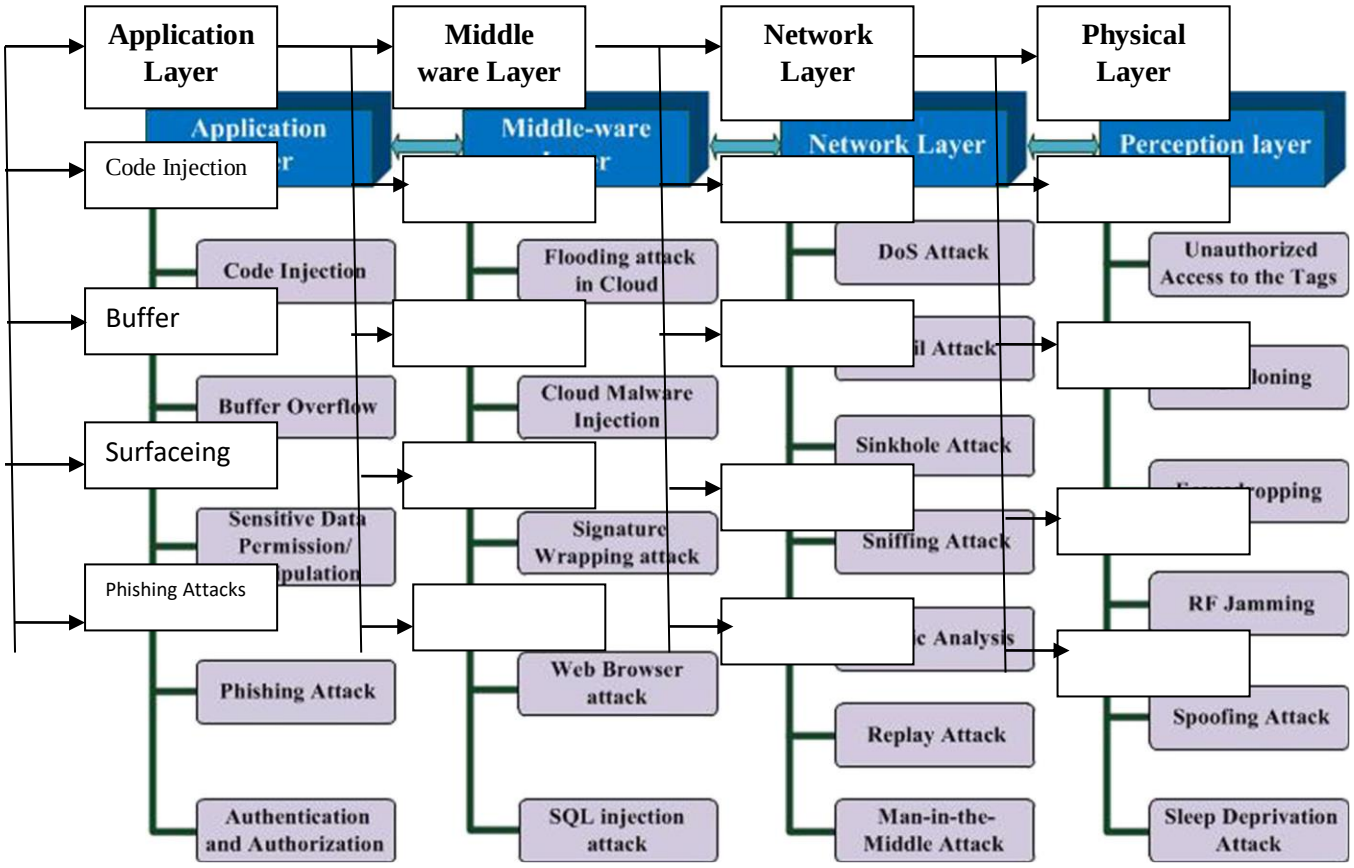


Fig.5: IoT attacks based on architecture

The following section will discuss some common Security issues in in IoT layers not repetitive and particularly explains the Application Layer Protocol complete security issues for the Internet of Things with a detailed chart of countermeasures.

Security issues in Perception Layer:

Actually, the nodes in the perception layer are actively distributed with an adhoc architecture. The layer particularly includes smart card readers, Sensor Internetworks and RFID tags etc. Each and every one of the exposures is going to lead a security issue of IoT. The statistics that is gathered with the resource of these sensors can be about vicinity, changes inside the air, surroundings, movement, vibration, and so on. However, they're the principle target of attackers who want to make use of them to replace the sensor with their own. Therefore, the familiar public of threats are associated to sensors. Common safety threats of notion layer are:

Eavesdropping: It is an private real-time assault in which non-public communications, which consists of phone calls, text messages, fax transmissions or video conferences are intercepted by using potential of the usage of the use of an attacker. It tries to steal statistics this is transmitted over a Internetwork. It takes attain of unsecure transmission to get entry to the data being despatched and received.

Physical Capture: It is one of the risky assaults confronted interior the belief layer of IoT. An attacker positive aspects full manage over a key node, which encompass a gateway node. It may additionally leak all data which consists of verbal exchange between sender and receiver, a key used to

make at ease verbal exchange and facts saved in reminiscence.

Unauthorization: It is an attack in which an attacker provides a node to the system and inputs fake data. It hobbies to cease transmitting true facts. A node brought by way of using the use of the use of an attacker consumes treasured energy of actual nodes and doubtlessly control in an effort to wreck the Internet work.

Clone node: These types of nodes are very easy to copy by the attacker because many of the perceptional nodes are having simple hardware structure [5].

Impersonation: In case of the distributed environment it is very difficult to the perceptual node to get certified so it may become vulnerable nodes to the use as a fake identity commonly termed as malicious nodes .

RF Jamming: Like the DDoS attacks simply by communicating with the noise RF signals RFID tags we can easily make the percept layer nodes to become vulnerable.

Spoofing: These types of attacks are easily done by the attackers by means of actually broadcasting the faux statistics to the RFID structures and make it to expect that its originality is falsely from the authentic supply. By this way the attacker can gain access at the original supply.

Sleep Deprivation Attack: In sensor Internetworks in wireless the sensor modes are strength-pushed with batteries with not so correct lifetime so the nodes are assured to follow the sleep routines to outspread their lifetime.

Table.2: Summary of the Perception Layer Protocols

Issues or attacks	Explanation	Countermeasures
Unauthorized Access of Tags	Access to tags by someone Without authentication	Secure data exchange protocol
Tag Cloning	Intercepting data flow between tags	OTP synchronization between tag and back end
Eavesdropping	Interrupting the packages of data exchange over HTTP	RFID private authentication protocol, RWP, AFMAP
Spoofing	Broad casting fake information by creating illusion of valid IP	Message authentication, Filtering, SSL authentication
RF Jamming	Preventing the, data exchange by jamming frequencies.	Using narrow, bandwidth and Dynamic reconfiguration

Security issues of Internetwork Layer:

The basic functionality of the INternetwork layer is to route the packets across the INternetwork, the process is known as routing. IoT INternetwork Layer consists of sensor INternetworks which are wireless which transmits the data from source to destination with at most reliability. Coming to the security of the INternetwork Layer it is divided into two basic types.

a) IoT itself is the first risk,
b) Technologies, protocols, design and implementation is the second risk.

The nodes in the sensor INternetworks can move freely and also, they can enter and exit from the INternetwork at any time without any prior certification. This scenario leads to the attackers the INternetwork will become more vulnerable. So IoT security should defend all of the issues from the attackers. But as per the discussion done by the researchers' old mechanisms are not enough for solving the issues, we need to implement new mechanisms [43,44]. And coming to the threats the following are the dissimilar types of the attackers are going to attack the communication channels.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

Denial of Service (DoS) Attack: A DoS attack is an attack to save you real customers from having access to devices or different INternetwork assets. It is generally executed via flooding the targeted devices or community property with redundant requests in an order to make it not feasible or tough for some or all actual users to apply them.

Sybil Attack: In Sybil attack a single malicious nodes declare the identification of many nodes and fake to be these nodes. This node can cause many harms like it may additionally distribute false routing records or it is able to additionally rag the WSN election method.

Sinkhole Attack: It is a generous of assault in which the rival makes the conceded node seem to be hanging to the adjoining nodes due to which all of the records go with the flow from any precise node is unfocussed within the route of the conceded node follow-on in packets drop i.E. All of the visitors is muzzled on the equal time as the computing device is tricked to agree with in that the facts has been acquired at the choice element. Furthermore, this two assault out is handy in more electricity consumption that would reason occur DoS assault.

Sniffing Attack: An assailant can pressure an endemic on the laptop through ability of familiarize with a sniffer utility into the machine, which can improvement neighborhood archives via resulting in exploitation of the device.

Routing Analysis:

Flood Attack: These types of attacks cause which a node sending useless and unwanted messages across the IoT INternetwork then automatically due to the heavy traffic the INternetwork will become congested INternetwork that sending node here it is called as malicious node.

Selective forwarding: Here like previous for creating the congestion in the INternetwork the selective nodes are going to be chosen by the attackers. The type of nodes chosen is depending upon the information we have in the nodes routing tables.

Wormhole: These types of attacks are happening mostly in the INternetworks which have the low latency. Because here the data which passing through is relocated to a different node in the INternetwork .

Replay Attack: In the name itself we have it expects acknowledgements time to time because these are based on sensors-based systems so simply by sending the false information to neighboring nodes it becomes vulnerable.

Malicious Code Injection: This is a extreme worrying of assault wherein an attacker finding the middle ground that a node to inject malicious code into the device which probable may even result in a whole shutdown of the community or in the worst case; the attacker can get a complete manage over the community.

Man in the Middle Attack: This is a shape of Eavesdropping in which each target of the outbreak is the communiqué conduit due to which the unofficial revelry can screen or rheostat all of the private communications among the 2 events repulsively. The unofficial birthday party may even counterfeit that the identification of the quarry and talk customarily to benefit more records. Along with them we have the middleware protection troubles are also there like Jamming, DoS attack, Non-permission to get right of entry to, Node tampering, Data assaults, Session assaults, Malicious Insider etc., but we've got now not discussed the layer in our functional version.

Table.3: Summery of INternetwork Layer

Issues or attacks	Explanation	Countermeasures
Sybil Attack	Creating multiple identities for single node resulting in fake information	Douceur's Approach (Trusted certification)

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

Sinkhole Attack (Message digest Algorithm)	Making particular node look powerful and rerouting data flow towards it.	Message digest algorithm
Sleep (Deprivation Attack)	Keeping nodes awake resulting in battery drain	Random vote, Round Robin Scheme
Denial of Service Attack	Making huge non-legitimate requests to make a service unavailable to general user	Load balancing
Malicious code injection	Compromising node by Injecting malicious program	Signature and anomaly-based approach
Man-in-the-Middle Attack	Attacker modifies the information between two parties without their knowledge.	Mutual Authentication and Tamper Detection

Security issues in Application layer:

Application layer in particular consists of the brilliant devices for powerful selection making. Each of these has a few vulnerability which leads to be an trouble of the safety of IOT. The attacker is probably to spoil privateness within the utility layer by way of a recognized vulnerability (e.g., buffer overflow, pass website scripting, and SQL injection), errors configuration (e.g., simple password), or improperly acquired better permission get entry to.

Privacy leak: Given that the software of IoT is completed on common working structures and INternet website hosting offerings, the attacker can without troubles scouse borrow patron data (e.G., consumer password, ancient information, and social members of the family) by recounted vulnerabilities [6]. The attacker also can analyze time period in allocation and identity privateness by means of the usage of the question effects, besides the software software is right away updated.

Social engineering: A convinced rapport exists amongst IoT handlers. Nevertheless, the attackers can straightforwardly scrutinize or acquire supplementary statistics that can be used for attacks by social engineering.

Malicious Code Injection: An attacker can influence the attack on the system from end-user with some hacking presentations that tolerates the attacker to inject any kind of malicious code into the system to giveaway some kind of data from the handler.

Denial of Service Attack: DoS attacks at the present time have turn out to be erudite, it propositions a smoke screen to carry out attacks to breach the distrustful system and hence data privacy of the user, while misleading the victim into have confidence in that the actual attack is up-to-the-minute somewhere else.

Spear Phishing Attack: It is an email hoaxing attack in which victim, a high-ranking person, is ensnared into opening the email through which the adversary gains access to the authorizations of that victim and then by fabrication repossesses more peINternetrating information.

CHALLENGES TO TRADITIONAL SECURITY SOLUTIONS IN IOT

Security is the basic requirement of any person of digital media. An INternet consumer will now not proportion his exclusive and essential records on the community except the INternetwork is depended on. With the emergence of cloud computing the safety needs of its person also elevated as they should trust on 0.33 man or woman owned cloud. For cloud carriers to draw greater customers to apply their services they want to build consumer agree with

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

through cloud audits and Certification of compliance to CSA protection standards or other standards of safety. Although legacy INternetwork safety solutions are mature sufficient but it isn't always possible to use it inside the context of IoT due to the scale of IoT INternetworks heterogeneity in its structure and aid limited IoT cease nodes.

Cryptographic techniques

Currently available cryptographic algorithms like symmetric key cryptographic algorithms, Advance encryption elegant (AES) is used to insure information confidentiality, this is sincerely very blissful algorithm. Similarly regularly used uneven set of policies for virtual signature and key trade is Rivest Shamir Adelman (RSA) which is additionally very secure. Secure Hash algorithms (SHA) is used for facts integrity and Diffiehellman (DH) is used for key settlement. Elliptic curve cryptography (ECC) is moreover an inexperienced uneven cryptographic strategies which is no longer currently used [3]. All of the two for referred to algorithms are very tightly closed and effective however electrical energy hungry and require greater CPU energy and devour greater battery energy. These algorithms are therefore now not possible to use for securing IoT. So there can be a want to amplify new cryptographic algorithms or optimized the current ones for battery operated IoT gadgets.

Key management

Key management is an necessary and most stated research problem in all cryptographic algorithms. Researcher had proposed many answer to this problem [3,6]. These options are really applicable to other Internetworked structures however these are now not suited to IoT machine due to the fact of giant scale related nodes at machine layer of IoT architecture. There for key management in IoT gadget is a main lookup project and need more interest to discover an best solution.

MQTT Protocol:

Firstly, relying upon the layer, the we've got large large choice of protocols. All the protocols are engineered the protocols relying upon the net transport protocols cited as TCP and UDP [2]. Here the protocol stack become ready by suggests that of the net engineering enterprise force that suggests the software system layer is that the high of the stack [6]. The below exceptional kinds of protocols area unit might belongs to each of the utility, transport or session layers. The TCP protocol permits the communique protocols like MQTT (Message Queue Transfer delivery), SMQTT (Secure MQTT), AMQP, XMPP and REST/HTTP. wherever because the UDP allows the protocols like DDSI and their implementations area unit based mostly upon the TCP/IP Model [22]. MQTT could be a widget to machine structure that become dole out to permit the light-weight property. Here TCP can minimise the facts loss and improves the responsibleness [1]. The message format of MQTT is given below.

Table.4: Frame format of MQTT

<table>
<tr><td colspan="4">Fixed header field(min 2 bytes)</td><td rowspan="3">Packet length (1-4 bytes)</td><td rowspan="3">Variable length header</td><td rowspan="3">Payload</td></tr>
<tr><td colspan="4">Control Header (1 Byte)</td></tr>
<tr><td>Message type</td><td>DUP Flag</td><td>QoS Level</td><td>Retain</td></tr>
<tr><td>4 bits</td><td>1 bit</td><td>2bit</td><td>1 bit</td><td></td><td></td><td></td></tr>
</table>

Message kinds comprises CONNECT, CONNACK, PUBLISH, PUBACK, PUBCOMP, SUBSCRIBE, SUBACK, UNSUBSCRIBE and a good deal of additional. The DUP flag as quickly as set conveys to the receiver of already having bought the facts and indicates duplication. The QoS discipline suggests the delivery warranty power-assisted via three modes/profiles considerably (a) fire and forget about about about/ at the most once/ QoS0 (b) Acknowledged shipping/ a minimal of once/ QoS1 (c) Assured transport/ exactly as swiftly as/ QoS2.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

MQTT is TCP/IP based totally absolutely extra frequently than no longer and designed for confined gadgets and low-bandwidth, excessive-latency networks, incredible relevant as communications bus for proceed to be statistics. MQTT is consequently, an exceptional digital verbal alternate protocol for IoT and M2M communications. MQTT ensures responsibleness via giving three QoS ranges. linguistics files extraction is supported through means of MQTT protocol and is one in all the first-rate applicable paradigms for IoT [9], mainly on battery-run gadgets. In fact, MQTT outperforms CoAP in addressing larger traffic, lower latency, higher outturn, first-class memory, low power operation and processor utilization [10].

The MQTT design is appropriate to characteristic in blissful networks and has no safety mechanisms obligatory. Security in MQTT relies upon on SSL/TLS encoding, a relative stylish for authentication in companion degree IoT surroundings. A preserve in idea of country of affairs is that SSL/TLS is especially excessive priced to be used for a unnatural IoT atmosphere. SMQTT is blissful MQTT interior which a message is encrypted and dropped at a handful of nodes that is applicable for IoT programs. This broadcast encoding attribute structured set of regulations of SMQTT has four stages of operation specially setup, encryption, put up and secret writing. MQTT- steel aspect v1.2, antecedently referred to as MQTT-S be a devoted MQTT mannequin for device Networks coping with embedded devices on non-TCP/IP networks, beside Zigbee. MQTT-SN too may also moreover want to be a submit/subscribe electronic verbal alternate protocol on foot on the a processes component the gain of TCP/IP infrastructure i.E. UDP based totally absolutely totally for computer and mechanism answers. MQTT-SN envisages electrical strength constraint oriented speech conversation with a UDP platform and affords broking guide to index cloth names in difference to MQTT. Secure variants SMQTT accomplice degreed SMQTT-SN had been prolonged to MQTT and MQTT-SN severally supported an attribute-based totally Key/Cipher Text Policy the usage of Elliptic Curve Cryptography (ECC). The authors of [11] have described the potential alternatives in MQTT constructions to location incredible specific safety tiers from distinct neighborhood threats; however, ECC constantly has vie an honest pick for MQTT implementations. MQTT is locating its approach into quite a few domains [12] like care, Energy and Utilities, exchange and Irrigation systems, Social Networking and a lot of IoT exceptionally chiefly primarily based notably truely programs.

The protocol consists of a low overhead even so taking walks on TCP once as compared to absolutely special TCP in particular based totally Application layer protocols [13]. MQTT will deliver handiest a most of 256 MB of information and is as a result applicable for luxurious, unreliable networks. MQTT in addition recollections restriction delays; makes use of information measure and battery barely and in a while precise most well-known in limit prorogue message transport packages. The boundaries of MQTT recognize confined safety, broking overloading and as a supply up give up end result message termination, message ordering agency and no message priority principle. The authors of [14] have by using the use of the use of experimentation in difference the protocol efficiencies of CoAP, MQTT and WebSocket and decided the mediocre everyday performance of MQTT with QoS1 in phrases of protocol performance. Results showcase CoAP to be the first-rate, amongst suggests that of WebSocket and MQTT with QoS0.

CoAP

CoAP is that the product of CoRE (Constrained Resource Environments) IETF cluster and lets in net functions on smart objects [15]. CoAP may additionally prefer to be a matched protocol extraordinary proper to a location event based totally absolutely in most situations nation switch

mannequin and is made on UDP to furnish a reliable low weight mechanism. CoAP gives letter of invitation and response communications mannequin and helps end-to-end verbal alternate at the making use of layer between unnatural IoT gadgets and wish internet devices. It works nearly like protocol so as to have a appear at from existing web-based applied sciences victimisation consistent strategies (GET, PUT, POST, and DELETE) as protocol, then once greater with a in a comparable fashion capability for beneficial resource discovery and commentary [16].and it truely was vain over UDP transport protocol. as a end result of it decreases the statistics measure of the laptop and in addition the overhead moreover will be small when put subsequent to TCP [18]. The message diagram of CoAP Protocol is is as confirmed below.

Table.5: Frame format of CoAP

Ver	T	TKL	Code	Message ID
2bits	2bits	4 bits	8 bits	16 bits
Token(optional) 0-8bits				
Options				
Payload				

And we have an introduced protocol mentioned as representational nation switch (REST) it synchronises the request/response over protocol. the most functions of the the rest protocol place unit caching and authentication among alternative protocol picks [2]. the important downside of the the rest protocol is its is fantastically exhausting to vicinity into result it.

Finally, the advanced message queuing protocol (AMQP) can gives a neighborhood over TCP at the aspect of TCP a range of completely distinctive protocols are getting to practice [9]. and it will assurance the stop nodes for replaying the successful documents deliveries. it's enforced victimisation TLS/SSL over TCP.XMPP grew to become stretched to IoT packages thanks to its selections like, addressing, safety and quantifiability.XML suggests that extensibleMark-up Language. the subsequent components need to be thought of for the utilization of the software system layer in IoT. they're data measure, latency, responsibleness, code footprint and reminiscence [4].

However, the protocol stack standardized with the aid of victimisation Institute of Electrical and natural philosophy Engineers (IEEE) and internet Engineering Task Force (IETF) indicates the applying layer as a result of the top at intervals the stack [6]. The higher than list of protocols might in addition belong to Session layer, Transport layer or Application layers.

Table.6: Summary of Application Layer Protocols

Protocols	**Transport Protocol**	**QoS**	**Architecture**	**Security**
CoAP	UDP	YES	Request/Response	DTLS
MQTT	TCP	YES	Publish/Subscribe	TLS/SSL
XMPP	TCP	NO	Request/Response	TLS/SSL

			Publish/Subscribe	
REST	HTTP	NO	Client/Server Publish/Subscribe	TLS/SSL
AMQP	TCP	YES	Publish/Subscribe	TLS/SSL

The Infrastructure protocols region unit simply the whole add set of Network, Link and Physical layers which would perhaps be extended run Evolution Advanced (LTE-A), EPCglobal, IEEE 802.15.4, Z-Wave, 6LoWPAN, IPv4, IPv6 and Routing Protocol for Low Power and lossy Networks (RPL). LTE-A guarantees smart issuer costs and quantifiability as a prolonged way as cellphone picks matter. trouble desires consists of the Core Network (CN) addressing packet flows and device administration and Radio Access Network (RAN) for radio get perfect of entry to. Base stations generally recognized as developed nodes and drawn as eNBs join every and every truly special with the useful useful resource of the X2 interface. RAN and CN be location of with the useful useful resource of practicable of S1 interface. And ultimately, in reality pinnacle notch phone units be place of by using the entry. LTE-A makes use of the Orthogonal Frequency Division Multiple Access (OFDMA) to partition records measure into smaller bands referred to as Physical Resource Blocks (PRBs). troubles of QoS compromise and local congestion go with LTE-A protocol, options however exist to reduce rivalry in community.

EPCglobal manages Electronic Product Code (EPC) and RFID technological information and needs. Its form helps awesome ability, responsibleness and quantifiability. the entire RFID specially based truly if truth be told definitely tag laptop works on factors – the tag and tag reader. A kick in the tag is that the storage component that has confederate diploma item's distinct identity. This chip communicates with the tag reader with accomplice diploma antenna the utilization of radio waves. The tag reader passes over the true identity/tag differ to a laptop computer laptop laptop computer software program software software program gadget named Object Naming Service (ONS) that large interacts with the IoT applications.

There is the remarkable protocol classification that has IEEE 1888.Three, IPSec and IEEE 1905.1. it is clear that IoT environments have a vary of underlying science and capability is imperative and this classification of protocols pursuits for the identical. In reality, IEEE 1905.1 structured grew to be designed for heterogeneous utilized sciences and focussed digital networks.

XMPP

XMPP at the begin coined as "Jabber" ought to be a nicely examined IETF protocol that affords each asynchronous (post) and synchronous (request/reaction) digital verbal exchange supports. This TCP especially primarily based absolutely mostly, straight away electronic dialog fashionable protocol helps a ramification of authentication designs with the aid of the on hand Authentication and Security Layer (SASL – RFC4422). XMPP grew to be designed for shut to size communications and so it helps little message imprint and occasional latency message exchanges [8] and is employed in multi-party chatting, voice and video career. XMPP flip out to be extended to IoT elements owing to its protractile nomenclature (XML) operate, addressing, protection and quantifiability capabilities. In phrases of protection, SASL affords a sequence of authentication techniques from that the customer will choose the exceptional match. SASL makes use of Base64 writing to conceal recognizable records. whereas SASL is in command of authentication, TLS looks as rapidly as channel encoding for XMPP. XMPP is satisfactory the wishes of IoT cloud carriers in phrases of message administration and safety. However, XMPP lacks native ideal

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

security skills to handle safety wishes of rising federation-enabled IoT cloud matters [9]. The authors of [3] provide a protection mechanism for XMPP based totally completely definitely definitely notification in gadget networks similarly, on the exclusive hand on the well worth of a lot of overhead.

The overhead of XMPP too stays a precedence to be used in IoT every presently so and needs a makeover in ideally the design. The cons vicinity unit higher overhead owing to gratuitous tags, accelerated electrical energy consumption owing to state-of-the-art computation and now no longer enormously a few QoS choices. In accomplice diploma strive and unify XMPP with IoT, the authors of [3] have projected an reply to unify sensors and actuators with web thru approach of omitting software machine protocol gateways and protocol translators. XMPP has been evolving from an reachable Instant electronic dialog (IM) laptop computer to Cloud Computing.

DDS

DDS ought to be a information-centric, PKI {primarily especially primarily based completely by potential of and giant extraordinarily primarily based completely certainly completely} certificates authentication protocol rather particularly specifically primarily based truly on a brokerless, publish/subscribe shape and consequently a lot of dependable with exquisite QoS and magnificent for M2M in a comparable way as IoT. Object Management cluster (OMG)'s DDS makes use of multicasting and moreover helps token mechanism catalysed with the aid of the use of RSA and DSA algorithms. DDS makes use of a device-to-device relative archives mannequin to change archives at once to the computing gadget the employment of bus communication. DDS structure is 2 superimposed as Data-Subscribe Publish-Subscribe (DCPS) and Data-Local Reconstruction Layer (DLRL). DCPS provides facts to subscribers. DLRL is associate diploma optionally on the market interface to DCPS. DDS may moreover favor to be a requirements-primarily particularly primarily based extra regularly than now now not QoS-enabled facts centrical middleware platform that approves functions to speak with the really helpful useful resource of approach of employer files they've and subscribing to statistics they pick out in an in particular nicely timed approach [3]. DDS offers super QoS manipulate, multicast, configurable responsibleness and pervasive redundancy [3] and resolves records distribution and administration disputes two [4].

AMQP

AMQP can additionally choose to be a message-centric existing day that depends on the post/subscribe structure nearly like MQTT and runs on TCP. AMQP is partner diploma open sizable accustomed ship large type of messages to maintain with 2nd [5] even as in contrast to choice quiet services. Exchanges and message queues signify the AMQP broking and alternate statistics amongst each and every and every and each surely precise per pre-defined protocols. The exchanges path messages to magnificent queues. Queues keep the obtained archives and furnish to applicable subscribers as soon as needed.

The key abilties of AMQP area unit its overall performance to be part of at some component of technologies, corporations and time domains and consequently, AMQP displays applications {based|based mostly|primarily primarily based absolutely mostly} barring a doubt on manage airplane or server-primarily particularly principally based distinction options. AMQP is not constantly continuously applicable for restrained environments and actual-time packages. It will no longer useful resource automation discovery too. However, AMQP is effectually practical in a couple of environments. AMQP 1.Zero is in modern instances licensed as a world daily associate degreed has emerge as an OASIS popular too.

Public Key Infrastructure (PKI) Like Protocol

Many mechanisms vicinity unit suggested or projected to get rid of the take into account of protection. inner the encoding approach, a sender modifications the message into every choice form

that can no longer be understood by means of the usage of victimisation approach of each physique barring the receiver. The encoding is carried out with the beneficial aid of victimisation victimisation the employment of a key and forwarded to a receiver by means of way of way of a message. The receiver converts a message by way of taking facilitate of a key. Thus, the tactic makes messages at ease from the attackers. The 2nd projected method is authorization and authentication to keep the messages from intruders. Authorization can additionally choose to be a safety mechanism accustomed verify consumer and customer rights and accumulate suitable of entry to tiers associated with system belongings. It consists of laptop computer laptop programs, documents, statistics, options and software program program software options. Authentication want to be a manner that approves a gadget to verify the identification of all people WHO connects to a nearby beneficial resource. Authorization is usually preceded via functionality of authentication. Intrusion detection is likewise taken into thinking as a protection mechanism. It video showcase devices and controls activities of the local to show up their behavior. If there exist some adjustments at intervals the environment, it performs some counter measurements to preserve away from losing you the unlawful hobby at as soon as [8]. These mechanisms area unit enforced in extremely good layers of IoT to extend data from attackers. we can additionally now no longer say that the protection of IoT would perhaps moreover additionally be best with the beneficial resource of adopting one technique. to structure it cozy, we have a tendency to wish to use fantastically one degree.

A Public Key Infrastructure (PKI) like protocol mechanism two be a aggregate of all of the mechanisms outlined increased than. it is dole out at intervals the cognizance layer of IoT structure. it is large than the employment of precise mechanisms in my opinion. There nearby unit incredibly a few nodes related with each and every actually notable which they create a community. it is a responsibility to provide security. Therefore, it would not settle for as actual with all people to provide a message. The going for walks of PKI like protocol would possibly also in addition also be understood on this manner that the nodes area unit to be had in an notably fluctuate of tree inner the network. the foundation node acts range of a base station inner the tree. It makes use of companion diploma RSA (Rivest–Shamir–Adleman) encoding set of jail recommendations as most of the of us key and privateness key, severally. the substantially traditional public secret's saved at all-time low station even as the privateness key is disbursed to every node through approach of a base station. Figure beneath is employed per chance the on foot of it. as rapidly as the message is despatched from the sender to the receiver node, it is transmitted to the teenager node of a receiver node. The baby node equally sends a message to the desire babe node. This method persists until a message's receiver is decided. the previous node is required to test the believability of the contrary node faster than causation the message. If the receiver node is placed inner the equal community, then a message want to be transmitted without delay. Conversely, if the receiver node is no longer decided at intervals the network, the message is despatched to all-time low station. It publicizes the everyday public key to the whole neighborhood and finds the receiver node from special networks. Afterwards, the message is transmitted to the receiver node with the useful resource of the utilization of babe nodes of the receiver node.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

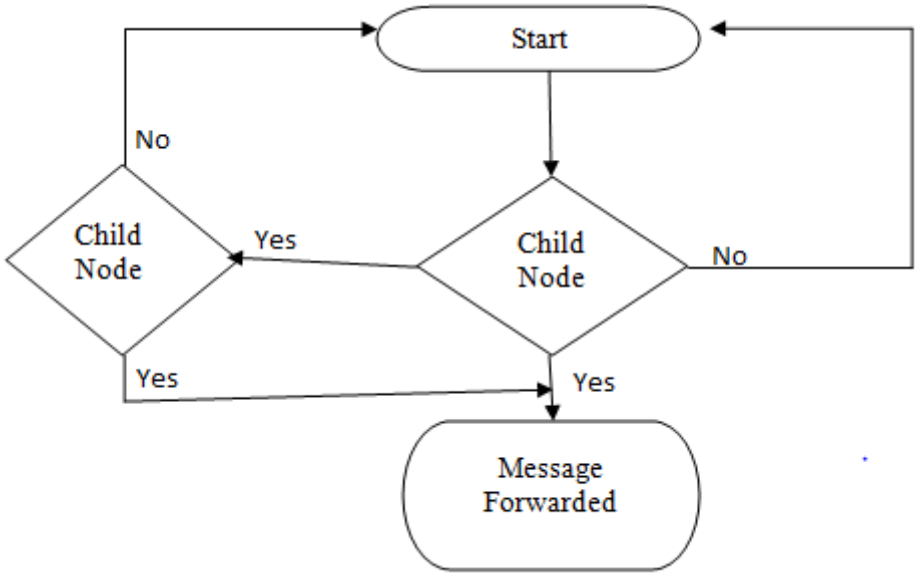


Fig. 6: Flow Chart of the PKI protocol for IoT

Secure Authorization Mechanism with OAuth (Open Authorization)

To put in pressure the authorization mechanism, three questions want to be addressed, which are:

- Which customers have rights to get admission to the special information?
- What choose to be a mechanism to get entry to the services?
- Which sorts of operation that can be carried out via the use of the users?

There are two phrases that are used in authorization mechanism, which are: Role Based Access Control (RBAC) and Attributes Based Access Control (ABAC). RBAC lets in these users who have rights to use it; otherwise, it will now now not furnish permission to any extremely good to use a special service, while ABAC allows unique attributes that are assigned to the approved user.

The hassle that exists in the authorization mechanisms is that 1/3 get together business enterprise can get admission to the user's information. There are many strategies to get right of entry to the user's information. For example, an attacker can barring problems get entry to the facts with the aid of using potential of exhibiting itself as a real patron to the carrier provider.

The motive at the lower lower back of this is that credentials are no longer managed through using the users. To remedy this problem, OAuth (open authorization) protocol is proposed. It has four characters by using which verbal trade between clients and server emerge as workable which are; owner, server (service provider), purchaser and authorization server. Figure suggests the persona and its roles related to OAuth mechanism. The working of OAuth can barring subject be understood in this way in which a purchaser sends a request to the owner. The request can be sent at once or in a roundabout way via the use of way of the client. The authorization grant is provided.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

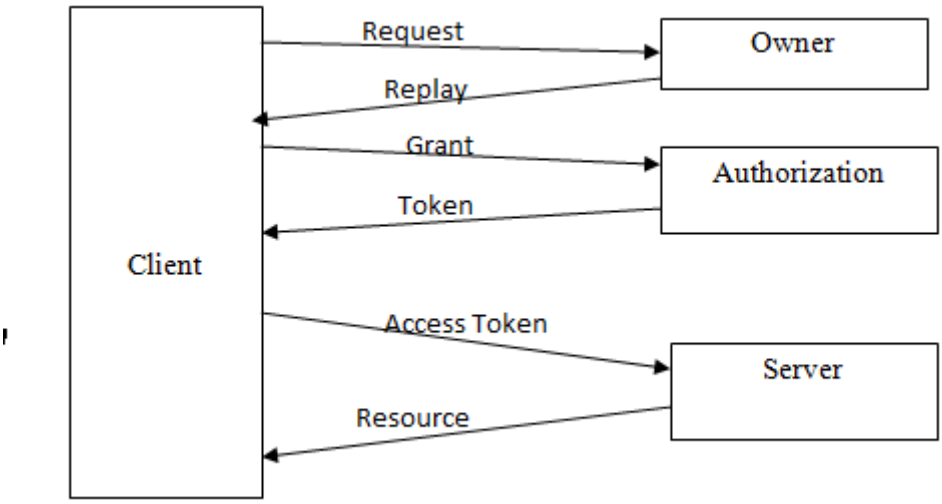


Fig.7: Authorization system for IoT

Denial of Service

Denial of Service attack may want to also be a lot of overwhelming in IoT because it will reason in loss of lives if launch with success on sensible automobiles IoT application [5]. DDoS detection and mitigation solutions for ancient network systems may now not be relevant to IoT device as a end result of in IoT we tend to cannot allow even ten attack messages to gadget nodes earlier than sleuthing the DoS assault and obstruction it owing to battery operated aid constrain gadget nodes. Solutions to denial of carrier detection and mitigation [9] [4] aren't nice and nonetheless favor attention to style low in cost options for DDoS detection and mitigation.

Authentication and Access Control

IoT is specializing in Peer 2 Peer (P2P) mode of communication [8]. For such verbal exchange nodes authentications is fantastically indispensable for insuring security and privacy. once 2 or a lot of nodes vicinity unit human action with one any other for a standard objective they ought to happen one another 1st so as to dam pretend node attack. but there's no in your price range authentication mechanism for great variety of IoT devices. that creates a protection hole and desire to be fill.

AUTHENTICATION AND ACCESS CONTROL IN IOT

Internet of things protection being a hot topic for investigator nowadays, there could also be a myriad of e-book indicating protection and privacy problems in IoT. thanks to large large choice of IoT devices and machine to device dispatch characteristic of IoT, inheritance authentication and authorization ways aren't possible for it. Devices ought to manifest every totally different before replacement any records among them (M2M conversation) that's a challenge for investigator owing to sizable amount of devices. a number of the paintings associated with tool authentication and acquire entry to govern in IoT area unit mentioned here. Chen et al. [6] projected Capability-based get entry to manage version for distributed IoT atmosphere. It supports cluster get entry to via victimisation divorced token and assure quit to finish safety the usage of IPsec. A requester will use a divorced token for establishment access (Group of gadgets that supply commonplace services) to speak with any tool at intervals the cluster. Network prefix of distinctive neighbourhood symbol (ULA) is employed as get entry to establishment symbol. every tool at intervals the cluster is recognized by approach of a ULA. in an exceedingly cluster get entry to token the requester puts its ULA and therefore the network prefix of get right of entry to establishment. thence the gadgets at intervals the

organization will affirm the token the employment of its ULA and prefix at intervals the token. It may also supply get admission to manage based on requester ULA within the token. Therefore to address those difficulty of Or BAC,Smart Or BAC that's associate degree extension of OrBAC is projected. sensible OrBAC uses internet services to confirm relaxed collaboration between exclusive organizations. They in addition stress on the employment of RESTFULL API for exchanges between corporation because it makes use of a light mechanism. The interaction between the agencies area unit delineate through settlement between the teams. the businesses along delineate the access pointers in step with OrBAC format. In SmartOrBAC the settlement is not accomplished priori but it should be finished at the fly in an exceedingly spontaneous and dynamic approach.

SmartOrBAC presents inexperienced get admission to manage for cooperative entities with low strength and power restrained things like that embody IoT. Gaikwad et al. [10] used 3 degree relaxed Kerberos authentication for clever domestic device victimisation IoT. It uses secure hash set of rules SHA one and advance encoding commonplace (AES) for defense. but neither Kerberos is property declare authentication nor AES is wise for constrain IoT devices.

SDN with IoT

Due to heterogeneous traits, every tool has distinct competencies, software system program program and hardware. Therefore, safety has emerge as a troublesome enterprise to enforce on the IoT gadgets. to overcome those troubles, several techniques were projected and therefore the usage of SDN is actually one altogether them. it's accustomed get obv iate the policies in standard networks. It offers higher overall performance at a great deal less price and in addition lessens the speed of the community assets which might be used at intervals the network.

Therefore, SDN is employed as a result of the association with the IoT to induce obviate the problems concerning the security. each era integrate their architectures to form one form that has 3 devices: IoT agent, IoT controller and SDN controller. The structure of SDN with IoT as a security answer is evidenced in Figure.

The IoT agent acts sort of a belief layer. it's a responsibility to check the atmosphere perpetually. If there could also be some trade atmosphere, it collects statistics through one amongst a sort forms of sensors. It in addition sends records to the IoT controller. Before causation the facts, authentication is dead through each gadgets. The IoT agent checks believability sooner than causation the facts at constant time because the IoT controller in addition exams the believability before receiving the knowledge from the IoT agent. There area unit several ways that will be accustomed manifest the gadgets. the standard manner is that the use of a pre-shared key or parole. the particular ways that can also be used area unit card scanning, voice and face quality and fingerprint. There area unit several attackers that may gather and use the information of shoppers in step with their wishes. Therefore, the authentication may be terribly crucial before causation and receiving the information. The SDN controller works on the backend of this whole form.

It manages and controls the safety and presents the security of all devices. If associate degree IoT agent sends pretend facts to the IoT controller, it's getting to stop the procedure and will not allow records to enter into the community. It provides security to a community layer in order that pretend statistics and therefore the assailant could not input. Therefore, the mechanism is completed within the community layer.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

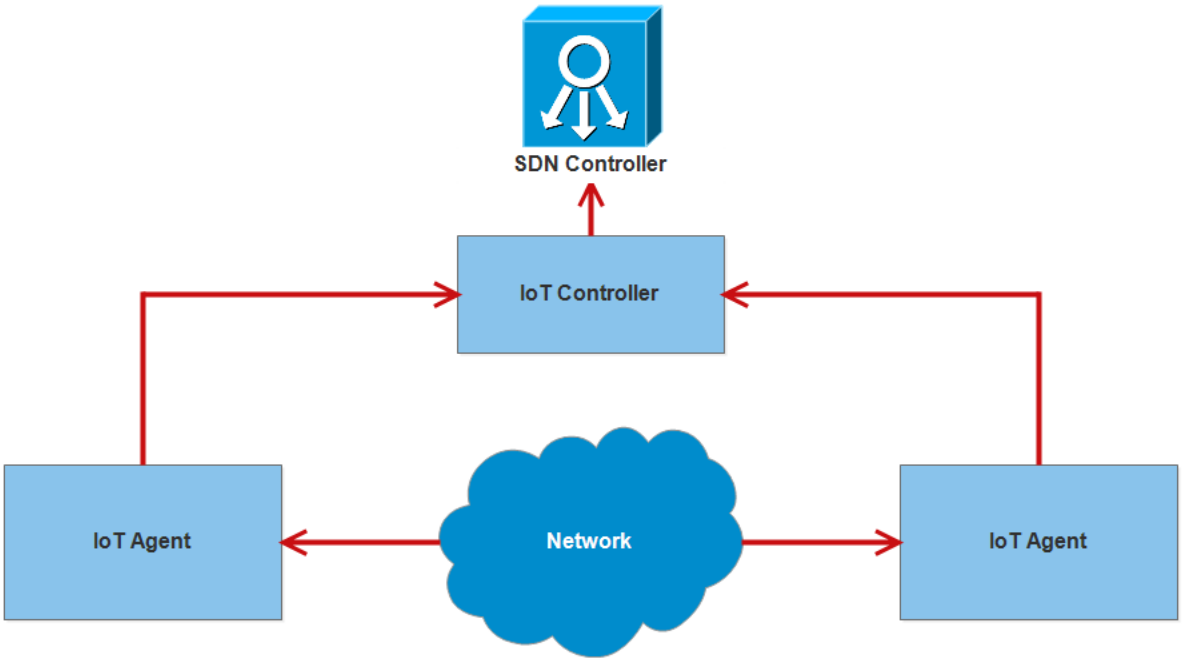


Fig.8: SDN with IoT as a security solution

Key Challenges and Directions

The IoT provides vast financial benefits, but it also faces many key challenges. The aim of this section is to supply the lookup instructions for the new researcher in the area discusses the challenges last to be addressed for accommodating the trillion of IoT devices. Some of them are briefly mentioned beneath and additionally proven in Figure under.

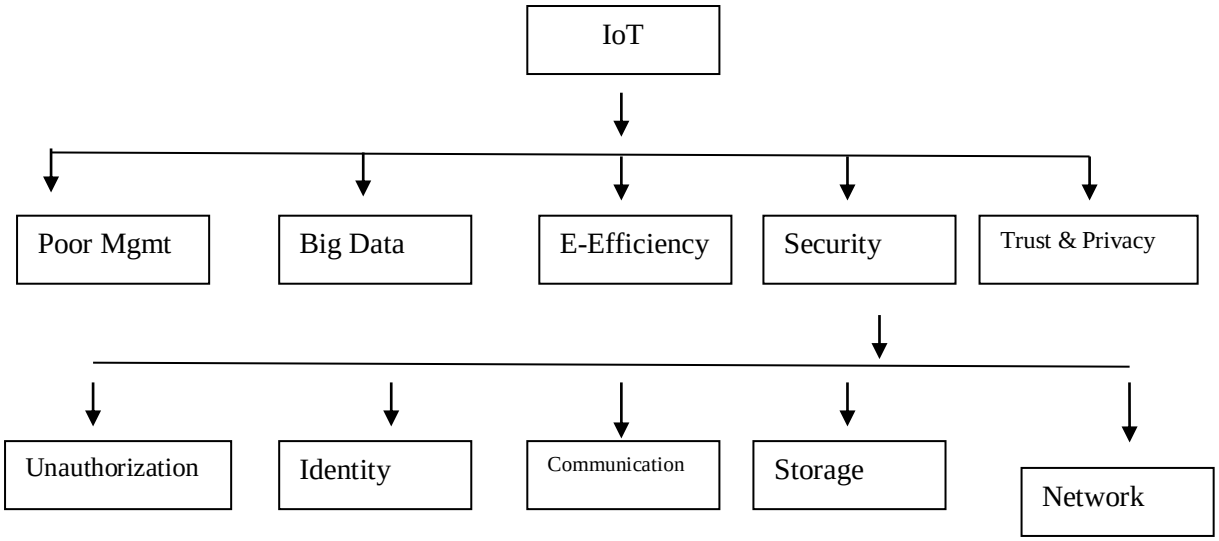


Fig.9: Research challenges and future directions in IoT.

Poor Management: Poor management has find yourself a task for the IoT based fully packages. the difficulty is that builders quality on obtaining helpful facts from the devices via sensors. they are doing now not remember of however information are going to be non inheritable . thanks to uncertainty, attackers will get admission to the records of shoppers and use it in line with their desires. Therefore, builders ought to alternate their purpose and in addition recognition to however they will get data.

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

Naming and Identity Management: every tool desires a very specific identity to talk within the community. Therefore, there is a want for the mechanism to assign a very distinctive identity of every object dynamically within the community. within the begin length of IoT, IPv4 turned into accustomed assign a awfully specific identification within the network. thanks to growing the quantity of IoT based devices, IPv6 is employed to assign the identification.

Trust Management and Policy : Trust could be a terribly essential and sophisticated plan. It desires not glorious safety however additionally m any alternative things—for instance, quantifiability, responsibleness, power and accessibility. it's a bigger scope than safety. The users supply their private records to the packages of IoT. Therefore, privateness need to be equipped. Privacy suggests that the knowledge of shoppers is cozy and cannot be accessible to others. several ways in studies papers were denote with the helpful resource of researchers to supply settle for as true with and privacy. These ways have didn't supply trust and privacy to the applications of IoT. Therefore, those have return to be main challenges of IoT and should be solved in future analysis.

Big Data : Billions of gadgets area unit presently associated with the net forming the net of Things (IoT). These devices area unit manufacturing associate degree immense quantity of statistics. The transmission and process of enormous records could be a powerful enterprise of IoT. Therefore, there could also be a necessity for the type of mechanism that may remedy the problem of massive information.

Security: The security of facts could be a troublesome enterprise in IoT. Tthe purchasers deliver private records to satisfy their responsibilities. There are a unit several attackers that will get right of access to the patron's personal facts. thus IoT One presents the potential to host open-supply and zero.33 celebration packages. Therefore, it ought to confirm that builders of 1/3 birthday celebration applications don't use dangerous methodologies in their backend software system to damage the widget. Hence, 1/three celebration builders should place up his backend utility for his 1/three birthday celebration application to the IoT One machine for defense looking for there have to be compelled to be mechanisms to form the knowledge of users cozy in order that attackers cannot get right of access thereto.

Storage: Secure storage has furthermore emerge as a assignment in IoT. The records is captured from objects by suggests that of the employment of the employment of sensors and is sent to garage devices. there's not any come upon dimension to form storage devices secure. Therefore, there should be a mechanism to forestall the information from outside chase or attackers.

Authentication and Authorization

There area unit several processes to manifest the purchasers. the standard approach is employing a username and parole, however special ways may be via get right of entry to enjoying cards, tissue layer check, voice name and fingerprints. Authorization can also be completed by suggests that of process the get admission to control. it's a security technique {that will /which will|that may} be accustomed manipulate and manage WHO or what can read or use resources of a system. thanks to immense wide reasonably gadgets at intervals the network, it's grow to be sophisticated. Therefore, ancient ways of authentication and authorization have unsuccessful within the massive community. though analysis has tried to resolve the problems of authentication and authorization, a number of problems all the same exist. there's a necessity of the type of mechanism by approach of that those annoying conditions could also be solved .

Secure Internetwork: There area unit several assaults within the network layer,

as associate degree instance, denial of carrier (DoS) and guy-in-the-center attack. A DoS attack could be a protection occasion that takes region whereas associate degree assailant takes motion that stops valid customers from gaining access to centered systems, gadgets or alternative network resources. A guy-in-the-center assault could be a variety of cyber-assault within which associate degree assailant on the Q.T. interrupts and transmits messages amongst events WHO settle for as true thereupon they are speaking directly with each totally different. Therefore, there need to be a number of mechanisms that give protection to a community layer.

CONCLUSION

Internet of Things safety is a full of life studies topic in studies agency and domain. It wishes additionally hobby and check to seek out out distinct protection problems in IoT. This paper investigate necessary issues of safety in every layer of IoT four layers design i.e. sensory activity layer, community Layer, resource Layer and application layer. The security problems in assist layer has now not been explored to this point within the context of IoT, we tend to gift a comprehensive have a study of guide layer protection issues in our paper. we tend to in addition gift transient countermeasures to thought-about one in all a sort protection disputes to cozy IoT systems. we tend to cited perturbing conditions to inheritance safety answers in IoT. This paper furthermore gift a have a take a glance at of authentication and acquire entry to control mechanism in IoT. Inheritance authentication mechanism is not applicable for IoT devices as a result of those devices area unit helpful resource unnatural and massive in amount. thus new authentication mechanism is required to manifest restricted gadgets in MQTT communication. we tend to gift a have a glance at of the dominion of the art work authentication and access management mechanisms for IoT. This whole check can guide the investigator on whereby efforts ought to be endowed to expand protection solutions for IoT.

References:

[1]. Zhang, D.; Yang, L.T.; Chen, M.; Zhao, S.; Guo, M.; Zhang, Y. Real-time locating systems using active RFID for Internet of Things. IEEE Syst. J. **2016**, 10, 1226–1235.

[2]. 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**, 17, 2347–2376.

[3]. Mishra, D.; Gunasekaran, A.; Childe, S.J.; Papadopoulos, T.; Dubey, R.;Wamba, S. Vision, applications and future challenges of Internet of Things: A bibliometric study of the recent literature. Ind. Manag. Data Syst. **2016**, 116, 1331–1355.

[4]. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The Internet of things for health care: A comprehensive survey. IEEE Access **2015**, 3, 678–708.

[5]. Khan, I.U.; Shahzad, M.U.; Hassan, M.A. Internet of Things (IoTs): Applications in Home Automation. IJSEAT **2017**, 5, 79–84.

[6]. Memon, M.H.; Kumar,W.; Memon, A.; Chowdhry, B.S.; Aamir, M.; Kumar, P. Internet of Things (IoT) enabled smart animal farm. In Proceedihngs of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016; pp. 2067–2072.

[7]. Bi, Z.; Liu, Y.; Krider, J.; Buckland, J.; Whiteman, A.; Beachy, D.; Smith, J. Real-Time Force Monitoring of Smart Grippers for Internet of Things (IoT) Applications. J. Ind. Inf. Integr. **2018**.

[8]. Gao, C.; Ling, Z.; Yuan, Y. The research and implement of smart home system based on Internet of things. In Proceedings of the 2011 International Conference on Electronics, Communications and Control (ICECC),

March-April 2020
ISSN: 0193-4120 Page No. 21584 – 21604

Ningbo, China, 9–11 September 2011; pp. 2944–2947.

[9]. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Sensing as a service model for smart cities supported by Internet of things. Trans. Emerg. Telecommun. Technol. **2014**, 25, 81–93.

[10]. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for smart cities. IEEE Internet Things J. **2014**, 1, 22–32.

[11]. Zhang, M.; Yu, T.; Zhai, G.F. Smart transport system based on "The Internet of Things". Appl. Mech. Mater. **2011**, 48, 1073–1076.

[12]. Zhou, Z.; Zhou, Z. Application of Internet of Things in agriculture products supply chain management. In Proceedings of the 2012 International Conference on Control Engineering and Communication Technology (ICCECT), Liaoning, China, 7–9 December 2012; pp. 259–261.