IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 10, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.282

9940 572 462 | 6381 907 438 | ijareeie@gmail.com | www.ijareeie.com

DOI:10.15662/IJAREEIE.2021.1012021

A Survey on Architecture of IoT: Challenges & Issuses and their Possible Counter Measures

Juhi Singh

Department of Electronics and communication, GLA University, Mathura, India

ABSTRACT: In today's digital transformation IoT is one of the leading component merging with various technologies, protocols, hardware and devices. Due to the diversity of IoT, it is viewed as double-edged weapon as it provides benefits to the users but also leads to attacking threats to security. This paper surveyed about architecture of IoT and issues related to it and how to counter these issues.

KEYWORDS*:* Communication protocol, countermeasures, data analysis, IoT, RFID, security attacks, WSN

I. INTRODUCTION

The term IoT is a revolutionary technology for digital world along with SMAC which was first coined by Ashton in 1999.From architecture of wireless to nanotechnology, dynamic technical innovation has been developed[1] This revolutionary innovation has a wide applications range which includes smart city, control actuation and complex systems maintenance for industry, health & transport. The term "things" denotes physical world (physical events, objects, behaviors and tendencies) and cyber world (cyber events, actions, entities and solutions). IoT can be used in daily purposes as well like doorbells, sensors, DVRs, light bulbs, electric switches and home assistant devices. Industry analysts says around 46 billion IoT devices will be available by 2021 like actuators, devices, sensors [2] About $3.9tn-$11.1tn per year, IoT market will have potential impact by 2025[1].There are two types of crucial concerns for IoT one is security and another one is privacy of data that is the challenge that are facing today. The convergence of internet and objects(machine) leads to new paradigm called M2M. Many capabilities for IoT objects in the network like identification, sensing, processing of data is used for the communication with another device with wider variety to provide services over internet that is core concept of IoT.

It is very important to have some mechanisms to protect the network, data and devices from all kind of attacks as sensors are highly vulnerable against attacks [4] IoT uses two technologies i.e., RFID and WSN. The combination of these technologies results in additional service to the user like RFID is used for location identification whereas to sense the objects around the environment WSN is used. Integration of these technologies can be beneficial into food tracking system and health care system. But the benefits of the combination of these technologies can be threatened by attackers So, the IoT security is very important. For this purpose, communication protocols should be secure to overcome the IoT risks. Encryption algo's must be properly applied to secure the IoT platform and for different security threats advanced techniques should be applied.

Different architectures for IoT has been proposed as there is no standard architecture is available such as three-layer[5], middle-ware-based architecture[6], service-oriented architecture(SOA)[7,8],four-layer[9]and five layer[6]. Three-layer architecture model is a basic model which is composed of physical/sensing, network/protocol and application layers. If middleware layer is added in above model then it is called four-layer architecture, the role of middleware layer is management of service, storage of data and composition of service. Five-layer architecture includes objects, objects abstraction, service management, application and business layers.

II. INTERNET OF THINGS & SECURITY

2.1 IoT Business scheme

Every physical object is interacting through IoT with another objects which makes the world one place. Interaction of physical entities with different environment like work place, family environment, leisure, individual etc are the example . Here is IoT scenario is shown which shows how the IoT will be helpful for various applications

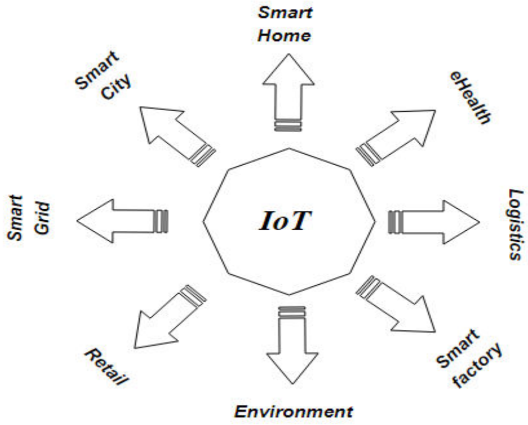


Figure 1IoT for various applications

Smart home: What happens inside the source is get inspected through IoT technology mainly for the purposes of security from thief, comfort like automation of washing clothes, utensils, floor cleaning, opening and closing of curtains with rise and fall of sun, proper use of resources like water and energy.

Smart city: Now-a-days , government makes huge investment on the smart city projects so that ICT will be properly utilized by citizens, organization and institutions.To improve the quality of citizens a smart city should be communicating, adaptable, effective, eco-friendly and ultimately automated[3].

Smart factory: RFID tags are used to track the products with help of IoT. This is the result to reduce the OPEX to increase the productivity. Procedures in the company will be automated using IoT & complex robots takes place in replace of humans to reduce the error and in order to inspects the robots technicians are appointed.

Environment: Sensors and actuators are integrated to track the environment activities like temperature , pressure etc.

Transportation: ITS is the technology used in the transportation for road safety purpose .As they uses sensors, memory, communication, information processing & adaptation so they are called as intelligence.

*eHealth:*As the no of doctors is lesser than the no. of patients so it is very important that some automation is required to diagnose the patient without the presence of doctor .And if suppose doctor is very far away from the patience in case of emergency doctor can diagnose easily that particular patience.

Retail: To improve the business real time information is needed. And to meet the needs of customers Retailing is needed to compare the product price, at lower price other products can be searched.

IoT is based on several technologies like

- RFID
- NFC
- Sensors
- Actuators
- WSN
- M2M
- 3G/4G
- IPv6 and 6LoWPAN

Abbreviations

ACLS	Access Control Lists
AMQP	Advanced Message Queuing Protocol
BLE	Bluetooth Low Energy
CERP-IoT	Cluster of European Research Projects-Internet Of Things
CoAP	Constrained Application Protocol
DDS	Data Distribution Service
DoS	Denial of Service
DP	Differential Privacy

DVRS	Digital Video Recorder
EPC	Electronic Product Code
FIPS	Federal Information Processing Standard
HTTPS	Hypertext Transfer Protocol Service
ICT	Information Communication Technology
ITS	Intelligent Transport System
LLN	Low power Lossy Network
M2M	Machine-to-Machine
MQTT	Message Querying Telemetry Transport
NFC	Near Field Communication
RFID	Radio Frequency Identification
SMAC	Social, Mobile, Analytics &Cloud
TLS	Transport Layer Security
WiMAX	World Wide Interoperability for Microwave Access
WSN	Wireless Sensor Networks

2.2 IoT architecture

According to CERP-IoT, IoT defines as a the infrastructure of dynamic global network having the capabilities of self-configuration based on interoperable protocols of communication where physical & virtual objects have identities, physical attributes and virtual personalities that uses intelligent interfaces and information network are integrated with it.[35].A new vision of IoT is introducedfor information and communication technologies, people can connect from anywhere at any time with temporal and spatial dimension.

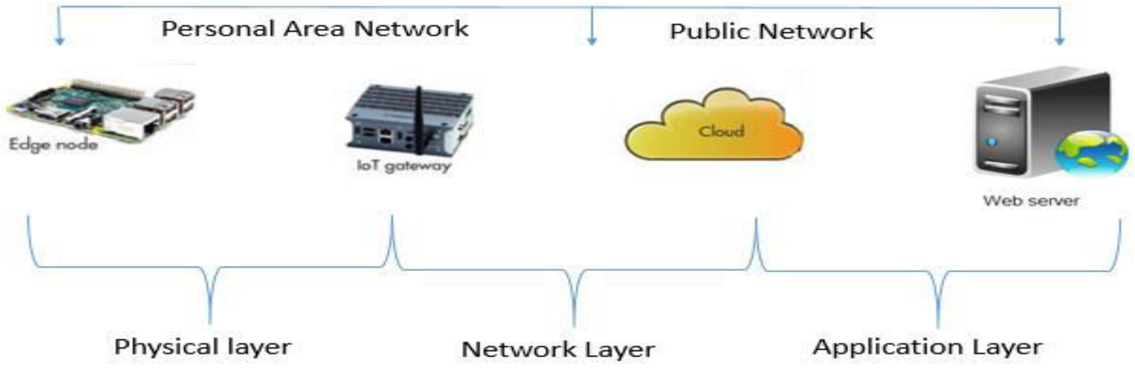


Figure 2 Abstract level of 3-layer architecture of IoT

2.2.1 3-layer IoT Architecture Model

Three- layer architecture of IoT includes: Application layer, network layer and physical layer. To collect the real time data sensing realizes a comprehensive perception through sensors and tags which is done by physical layer. For reliable data transmission network layer is responsible and from sensing to application layer data is acquired. Data processing and intelligent control is done by application layer including cloud computing.

2.2.2 4-layer IoT Architecture Model

Four-layer IoT architecture involves physical, network, middleware and application layer. The task of the middleware layer includes:

- Management of service
- Storage of Data

- Composition of Service

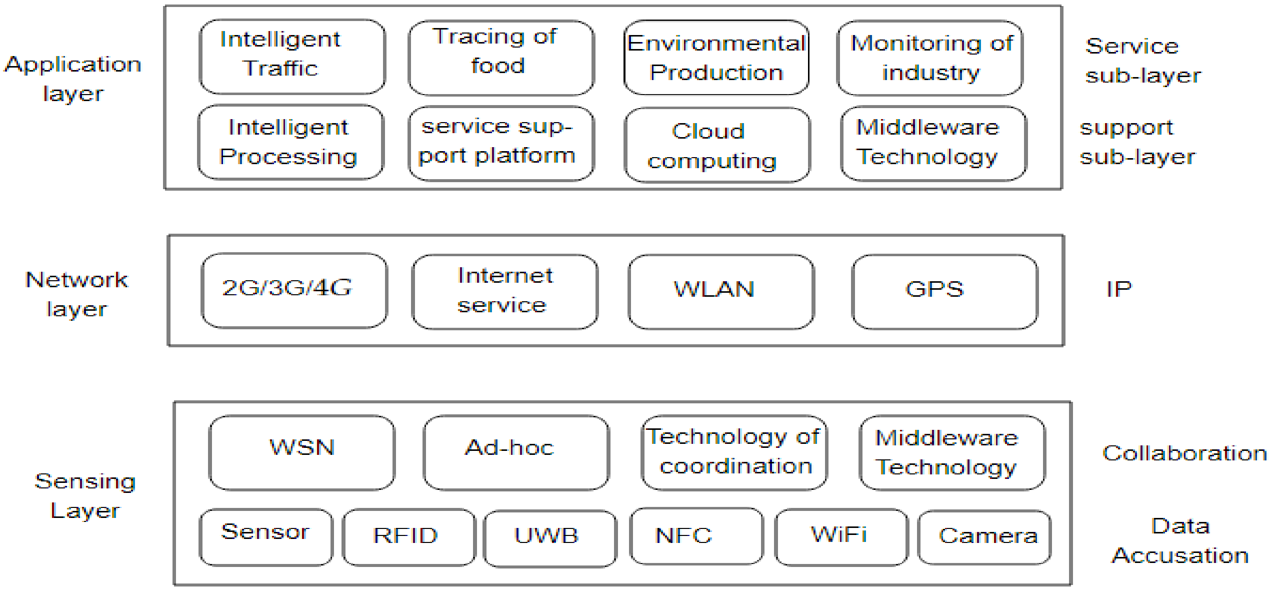


Figure 3 IoT 3-layer Architecture Model

2.2.3 5-layer IoT Architecture Model

ZigBee, Wifi, Ethernet, LTE, 5G, Bluetooth are the different wired and wireless protocol that are cover by network and protocol layer.

TCP/IP, UDP/IP and TLS/SSL are the protocols of transport layer. In termsof low consumption , to meet IoT requirement various application protocols are developed like AMQP, CoAP and MQTT

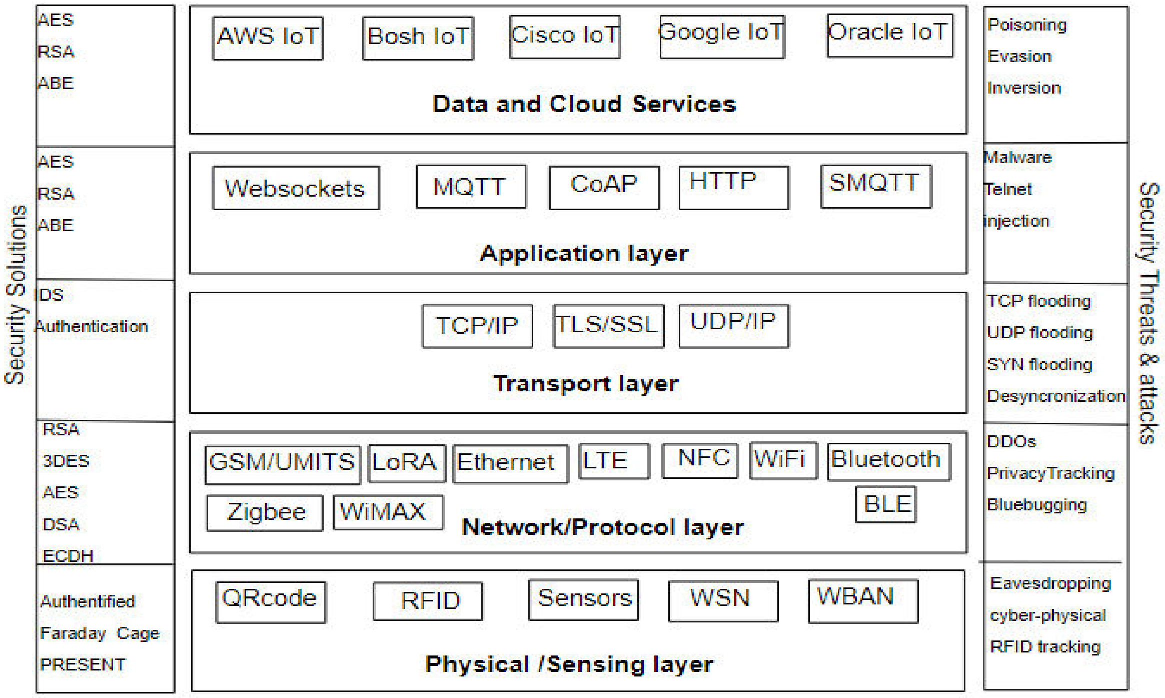


Figure 4 IoT proposed architecture

Main cloud-based IoT frameworks are presented by data and cloud services. Default Telnet and SSH account are Malware access to IoT devices. To infect the LINUX operating system of IoT device Telnet forces the port to disable it. Injection untrusted data is sent as a command or query to an interpreter. To stop or reducing the activities many packets are sent simultaneously as a flood called TCP flooding. To detect this attack SVM classifier is used. UDP flooding is similar as TCP flooding. To stop UDP flooding a state machine and a hashing table detection scheme is used on router. Without having TCP handshake procedure connection is established is called SYN flooding. SYN message can be changed to change the state in the server side that is the solution against SYN flooding. TCP de-synchronization is one which breaks the sequence of packets by wrong sequence number. To avoid this authorization is required.IDS and VPN are the solution for man-in-middle problem when hacker tries to intercept the confidentiality and integrity for two-end data transfer. When network or machine resource unavailable DDoS is an attempt. When someone tries to steal the information of authorized user via IoT network this problem is called eavesdropping also called sniffing or snooping.

Table 2 Description of layers IoT architecture with threats and their possible countermeasures

layer	Common attack	Description	countermeasures
Data and cloud services	Poisoning	To decrease the clustering process input of incorrect data	Sanitization of data
	Evasion	To evade the system from malware or spam adversarial sampling is generated	Retaining learning models
	Impersonate	Deep neural based DNN algorithm for unauthorized access	DNN defensive distillation
	Inversion	To compromise the data privacy for gathering information bot ML models	DP technique
Application	Malware	Access to IoT devices using Telnet or SSH account	Disabling of telnet and SSH account
	Telnet	To infect LINUX operating system	Disabling of port no. of Telnet
	Injection	Untrusted data in form command is sent to an interpreter	Validation of input control
Transport	TCP flooding	Sending of many packets simultaneously as a flood through TCP protocol	SVM classifier
	UDP flooding	Sending of large number of packets simultaneously as a flood through UDP protocol	State machine and a hashing table detection scheme is used on router
	SYN flooding	Establishment of connection without following the TCP handshake procedure.	To change the state in the serve side
	TCP desynchronization	Breaks the sequence of packets by wrong sequence number.	Authentication of packets
Network	Man-in-middle	Violation of confidentiality and integrity in data transfer	IDS and VPN
	DDoS	Network resource unavailable	Hop counting, SYN-cookies, Ingress/Egress filtering
	Replay	Reorder of data and manipulation of stream of messages.	Message Timelines
Physical	Eavesdropping	Information stealing	Faraday cage
	Cyber-physical	Physical attacking on device through IoT	Identification of faulty nods using detection algorithm
	RFID Tracking	Imitation ,modification of contents and disabling of tags	Faraday cage

III. DETAILED DESCRIPTIONS OF IOT LAYERS

3.1 Physical Sensing layer

QR codes, sensors, RFID, WSANs and WBANs are the components of physical sensing layer. To identify objects in the IoT network RFID uses a universal unique identifier called EPC. RFID supports in various applications like aviation food safety, retailing, supply chain management, public utilities etc.WSN is the second element for high radio coverage

and communication which is the another core of the IoT. Sensing, computing and communication. Sensing,computing and communication capabilities are supported by wireless system. Through RFID tags IoT is benefited.
*Security Threats and countermeasures:*Weak privacy suffered by RFID, it is described by ISO/IEC 18000. The effective solutions for RFID are Faraday cage, tag-killing, tag-blocking & re-encryption. 3 kinds of attacks i.e., eavesdropping, cyber-physical and RFID tracking suffers the physical or perception layer.

3.2 Network / Protocol layer

To establish the connection for communication and exchange of data in IoT systems, communication protocols are the main components. ZigBee, 3G/4G/5G wireless communication, Wifi, Bluetooth are the parts of network/protocol layer. IoT communication protocols are divided into two sub-layers: sensor based network and gateway network.
For wired and wireless communication networks, various protocols of communication are used to ensure the communication. These protocols are 6LoWPAN, RPL, NPC, Bluetooth, Wi-Fi, ZigBee, WiMAX, 3G/4G/5G. IEEE 802.15.1 is for Bluetooth which is used for tracking. FIPS- ECDH are used by Bluetooth for key generation like Diffie-Hellman key. ZigBee has the IEEE 802.16 standard, it is a low-cost and low-energy device. It has an advantage and disadvantage for one-time transmission of the unprotected keys. Wi-Fi has IEEE 80211i/e/g standard. Wi-Fi has the advantage of mobility and efficiency but has disadvantage of low range which is limited up to 100m.The collection of wireless broadband standardsis WiMAX which has IEEE 802.16 standard that provides 1.5Mb/s to 1Gb/s data rate. To provide contactless communication, NFC is a technology which is developed in 2002 by Philips and Sony. It is a protocol for half-duplex communication which is short-range. UMTS and LTE are the 3G and 4G mobile communication protocols standards. IPv6 over LoWPAN is called 6LoWPAN has IEEE 802.15.4-2003 that allows wireless connectivity, which is a low-cost communication n/w with limited power & processing connectivity. It is used to connect the physical environment in real world applications e.g., wireless sensors.
Security Threats and countermeasures: Many attacks target the IoT communication protocols like eavesdropping against Bluetooth, NFC, Wi-Fi etc. Other attacks like man-in-the-middle and DoS. Effective solutions to address these attacks like eavesdropping are RSA and Diffie-Hellman for LTE-advanced.

Some attacks for Bluetooth are defined as:

- Bluejacking: For sending unsolicited messages to other enabled devices which exploits OBEX protocol.
- Bluebugging: For leading unauthorized access of the device, this attack exploits the devices to compromise the security purpose.
- Bluemack: It suffers the DoS of the Bluetooth devices. A L2CAP ping request is generated that is similar to ICMP ping attack, after receiving an oversized packet it leads to knocked out condition which turns to DoS.

Effective solution for man-in-the-middle problem are IDS and VPN. Ingress/Egress filtering, D-WARD, Hop Count Filtering and SYN- cookies are DDoS attack countermeasures.

3.3 Transport layer

Working of transport layer is to provide connection-oriented protocol i.e., TCP for reliable application and connectionless protocol for unauthorized applications. To secure transport layer TCP uses TLS, UDP uses DTLS. TLS and SSL are the security protocol which enables a certificate and session key
management. TLS and SSL are highly vulnerable from various attacks such as BEAST, CRIME, Heartbleed and RC4. MQTT which is a lightweight connectivity protocol doesn't include a security layer.
Security Threats and countermeasures: TLS protocol is the most vulnerable against resource exhaustion, flooding, replay and amplification attacks. When message stream manipulated and data packets are reordered to change the meaning the meaning of message that is called replay attack. Setting of timelines of message is the solution to protect the IoT device from replay attack.
Following are the attacks against transport layer:

- TCP flooding
- UDP flooding
- TCP SYN flooding
- TCP desynchronization/TCP hijacking

Effective solution against TLS is DTLS and another is end-to-end tunnel to protect a low power and lossy network. Some proposed solution are Machine Learning(ML) ,DoS and DDoS, Artificial Neural Network(ANN), Back-propagation(BP), Support Vector Machine (SVM) to detect and protect DDoS TCP flooding.

3.4 Application layer

To meet IoT requirement in terms of low consumption and small device capacity various protocols are developed such as AMQP,CoAP, DDS and MQTT. To enhance M2M communication between client and server,MQTT is a specific protocol that works beneath various data-link layers such as Ethernet and Wi-Fi. LTE, 5G & mobile communication are the emergent technologies which a challenge for MQTT or its adaptation. Routing for small, cheap, low-power & low-memory devices in low-bandwidth are the features provided by MQTT. Secure MQTT i.e., SMQTT are the extension of MQTT.

Table 3Protocols for different layer of OSI model

OSI Model Layer	Protocol
Application layer	SMQTT
Session layer	SSL/TLS
Transport layer	TCP
Network layer	IPv4 and IPv6
Data-link layer	Ethernet/Wi-Fi

Security Threats and countermeasures: Three types of IoT attacks in the application layer are malware, Telnet and injection. There is one way to stop these attacks is to disable or change the accounts of Telnet and SSH. Telnet port number must disable to prevent from Telnet attack. The effective solution for injection is to prevent the user from entering more or less the required format. Other risks like broken authentication, sensitive data exposure, XML external entities (XEE), broken access control, security misconfiguration, cross-site scripting, insecure deserialization are also security threats. There are two types of TLS are used in the mobile communication one is wireless TLS(WTLS) and another one is datagram TLS (DTLS). Data confidentiality and privacy are the two important factors used in IoT systems which is guaranteed by encryption protocols.

Table 4 Encryption Algorithms for IoT

	Algorithm	*Key size*	*Application*
Symmetric	PRESENT	80/128- bit key length with 64 bits block	RFID
	CELFIA	80/128/192-bit key length with 128 bits block	Digital Right management
Asymmetric	RSA	1764 bytes	Authentication
	Elliptic Curves	1272bytes	Pervasive Computing

3.5 Data and Cloud Services layer

Due to the complexity of distributed computing, involvement of different programming languages and the variety of communication protocols IoT faces many challenges. The management of both hardware and software components along with handling of full infrastructure is needed for the development of IoT applications.

A set of rules and protocols are introduced by cloud-based IoT frameworks for organizing of data management, message exchange between parties involved in the IoT network like devices, the cloud system and users.

There are main five IoT frameworks based on public clouds:

- Amazon
- AWS IoT
- CISCO IoT Cloud Connect
- Google Cloud IoT
- Oracle IoT ecosystem
- Bosch IoT suite

3 components of cloud-based IoT frameworks are: smart devices, sensors, tags etc. IoT data are processed and stored by cloud servers. DTLS, HTTPS, TLS, IPsec are the various protocols used by IoT frameworks to secure communication.

SSL protected API endpoints which is proposed by AWS which ensures confidentiality, integrity and availability. Authentication and authorization secure by AWS. To guarantee the confidentiality, integrity and authentication among different services ATLS is used by Google cloud.

CISCO IoT platform has 4-layers :

1. Sensors layer
2. Multi-service edge layer
3. Core layer
4. Data center cloud layer

Many applications of ML in IoT contexts are there. Broadly ML models are broadly divided into 3 categories-classification, regressionand clustering.

Jammers

Physical layer jammers:

Radio signal is attacked by jammers with Radio Frequency (RF) transmitter. There 3 types of jamming in physical layer that are:

- Constant Jamming: Nonstop random bits are send by attacker.
- Deceptive Jamming: Continuous stream regular packets is send.

. Data packets are jammed by link layer jammers. Difficulties faced in link layer is to predict the arrival of the data packets.

- Random Jamming: Jamming signal is send in random format to save the energy of the jamming device is send by attacker.

Link Layer Jamming:

It is more complicated and energy efficient than physical layer. ACK message i.e., a controlling signal is also send by link layer jamming

Table 5 IoT Machine-learning trends

	Algorithm	*Prediction Complexity*	*Advantages*	*Disadvantages*	*IoT application*
Classification	K-Nearest Neighbors(KNN)	O(np)	Online setting updating is easy	Not good for large data sets as it is unscalable	Smart tourism and citizen
	Naïve Bayes(NB)	O(p)	Scalable is fast and highly	Independence assumptions	Smart agriculture, spam filtering and text categorization
	SVM	O($n_{so}p$)	Better for unbalanced data	Transparency of results are lack	Real time prediction, Detection of Intrusion , attacks and malware
Regression	Linear Regression(LR)	O(p)	High rate processing	Outliers are very sensitive	Energy applications, market prediction
	Support Vector Regression(SVR)	O($n_{so}p$)	Techniques are useful and flexible	Complicated	Smart weather and intelligent transportation systems
Clustering	K-means	O(n2)	Scalable is very fast and highly	K-value predictions are difficult	Smart cities, smart home, smart citizen, intelligent transport
	Density-based approach to spatial clustering of applications with noise (DBSCAN)	O(n2)	Against outlines it is fast and robust	In respect to distance metric performance is sensitive	Smart citizen and smart tourism

Feed Forward Neural Network(FFNN)	O(n2)	Robustness and non-linear	Training time is long	Smart health

Network Congestion
The delay in delivering the data network is the network congestion. **Unfairness** also called as exhaustion based attacks is a repeated collision based attack. It is mostly present in WSN. **Wormhole**is a dangerous attack which is independent of Link Layer Protocols. It is performed at bit level or at the physical layer. **Sinkhole**is a congestion attacks in a group network. **False Routing**is a type of attack at node which tries to make and propagate false information. This attack is mainly done in network layer.

Dropping
Discarding the packet is known as dropping. Two types of this attacking is done one is **Selective forwarding**means some packets are selected and rest are dropped. It is also called Blackhole. **Synchronization attack** is based on OSI model, this type of attack affects mainly affects link layer and transport layer.

Privacy attacks
Data oriented: It consist two types of attacks one is eavesdropping and another one is substitution ,clonage and replay attacks.

Eavesdropping: It is an attack in which attacker tries to steal the information between a reader and to collect the exchanged binary data for that a card measuring the RF field is emitted by the reader.

Substitution, clonage and replay attack: These three attacks are of same kind, which requires data recovery without contact on another card.

Context oriented: It consist three types attacks i.e., traffic analysis, tempering attacks and tag modification.

Traffic Analysis: Attackers may sense the packets or data which is confidential.

Tempering attacks: The difficulty level is higher the most accessed and controlled over the victim hardware component

Tag modification: Attacker can easily modify or delete valuable information could be performed easily by an attacker.

Types of attacks
There are 5 types of attacks i.e., Physical, side channel, Software and network attacks.

Physical Attacks:
These types of attacks affect the hardware components. Examples are de-packaging of chip, layout reconstruction, micro-probing, particle beam techniques etc.

Side channel Attacks:
From the encryption device the information can be retrieved but it not must be plaintext nor it is cipher text. Timing Examples known-plaintext attacks, chosen-plaintext attack, man-in-the-middle attack etc.
power analysis attacks, fault analysis attacks, electromagnetic attacks and environmental attacks are the examples of side channel attacks.

Cryptanalysis Attacks: Cipher text are mainly affected by these attacks and encryption are break by such attacks.

SoftwareAttacks: Security vulnerabilities are caused by software attacks in any system. They exploit implementation in the system through its own communication interface.
Network Attacks: These attacks affect wireless systems due to broadcast nature of the transmission medium. Active and passive are the two types of attacks.

DoS attacks, node subversion, node malfunction, node capture, node outage, message corruption, false node and routing attacks are the examples of active attacks.
Monitor and eavesdropping, traffic analysis, camouflage resources are the passive attacks.
information is produce by encryption device which is easily measurable, power consumption statistics

IV. WSN

With limited bandwidth and frequency wireless communication takes place through the structure of independent nodes are called WSN. Sensor, microcontroller, battery, radio transceiver and memory. As the communication range of each WSN sensor node is limited, so between source and receiver the multi hop relay of information takes place.

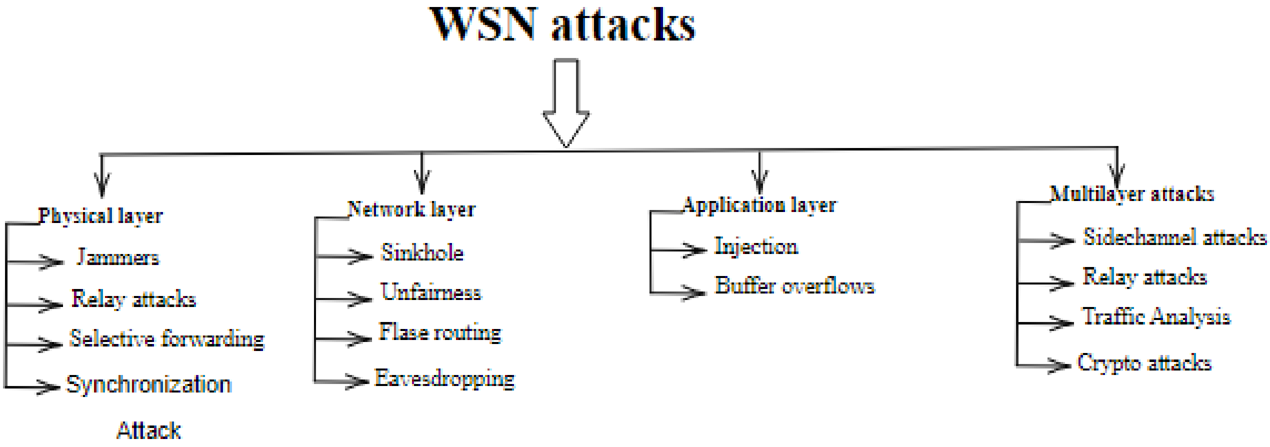


Figure 5 Classification of WSN attacks

V. RFID

A method for storing and retrieving of data by using (RFID tag) that is called marker data remotely or RFID transponder. By transfer of electromagnetic energy RFID system is activated that consists of the two components: RFID tags and RFID readers. RFID tags are the transponder while RFID readers are transceivers.

RFID tags:These are made up of memory units with a unique identifier i.e. is EPC. Interrogators or readers send a signal to the tag and read its response that is two-way radio transceiver. There are two types of tags i.e., active tag and passive tag.

- ***Active tag:*** ID signal is periodically transmitted and has an on-board battery
- ***Passive tag:***It uses radio energy that is transmitted by the reader .This tag is cheaper and smaller asit doesn’t have battery.

RFID readers: This tag is used to track individual objects. It is a device used to collect the information from RFID tag.

DOI:10.15662/IJAREEIE.2021.1012021

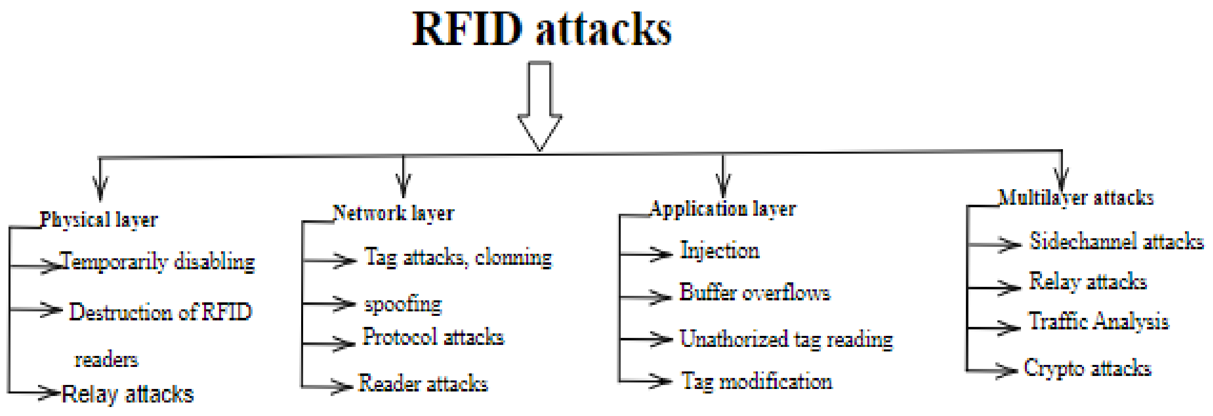


Figure 6 Classification of RFID attacks

VII. COUNTER MEASURES

A. Countermeasure against Jamming

Regulated transmitted power: Before transmitting jamming signal an attacker must be located first to decrease probability.

Frequency- Hopping Spread Spectrum: FHSS is a way for carrier fast switching for transmitting radio signals. It reduces unauthorized interception and jamming of radio transmission between tags and reader in RFID and nodes in WSN**.**

Direct-sequence Spread Spectrum: DSSS transmission are done by modulating the Pseudo-noise(PN) digital signal as a modulating signal and a RFcarrier. PN signal is a pseudo-random sequence which has higher chip rate than the original signal. In this process RF signal replace with a larger bandwidth signal with equivalent to the spectrum of noise signal. This noise is filtered out to receive the authenticate signal at receiving end the incoming RF is multiplied with same PN modulated carrier.

Hybrid FHSS/DSSS: The far-near problem is solved by hybrid FHSS/DSSS. Hoped anti-jamming is measured between Hybrid FHSS/DSSS communication.

B. Wormhole Countermeasure

Bound Distance or time & graph theoretic and geometric are the two approaches to countermeasure the wormhole.

C. Replay Countermeasure

Timestamps, one-time passwords and challenge response cryptography are the countermeasures exist to defend against replay attacks. There is a second method for countermeasure in whichto limit the directionality of radio signals using RF shielding.

D. Traffic Analysis Countermeasure

To solve the problem of traffic analysis, sending rate of packets is control in such a way that with same rate packets are sent by every node. By changing the external appearance of packets when packets move forward through a multi-hop sensor network is another way to defend the traffic analysis. This is done by establishing the cluster-key between the neighboring nodes. When packet moves forward then it is encrypted for destination address, packet type, packets contents but then re-encrypted using cluster key. For the receiver to choose the correct cluster key the current senders address will remain same for decrypting the packet.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

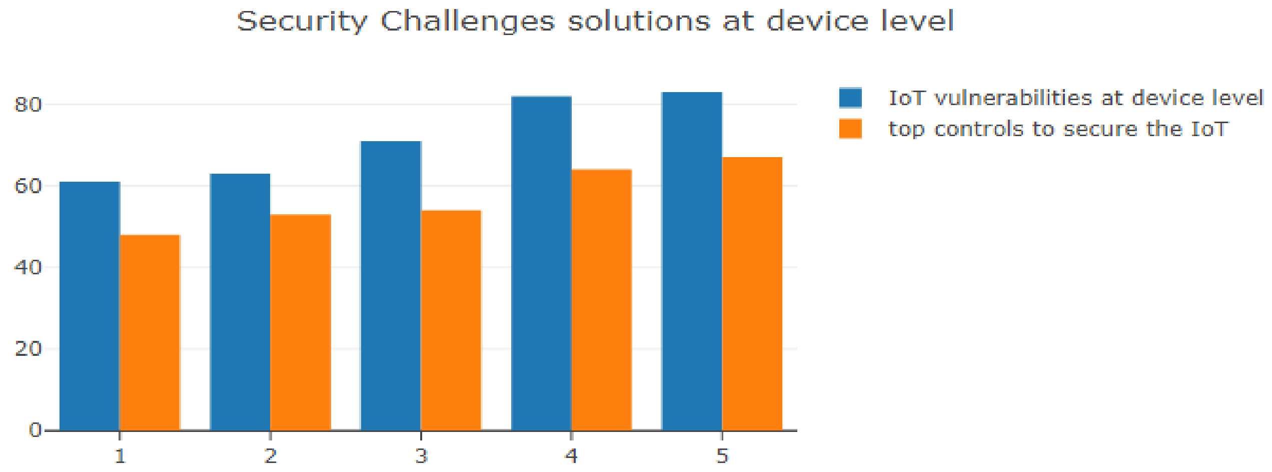
|| Volume 10, Issue 12, December 2021 ||

DOI:10.15662/IJAREEIE.2021.1012021

E. Eavesdropping Countermeasure

Eavesdropping is vulnerable for the communication between WSN and RFID tags as cryptographic protections are given to very few nodes and passive tags. There must be use of proximity of RFID tags due the short range of passive tags. Security issues are solved by data cryptography that prevent against eavesdropping. Symmetric Key Cryptography are used now-a-days in sensors. Shared key is use between two nodes in the whole network.

Security Challenges: Security aspect should be incorporated in the designing phase. Operating system level is introduced in security aspect and extended for the implemented applications through the device stack and having hardware applications. In below figure showing that IoT devices have 70% threat of security and 25% security aspect concerns per device. Having the security concern IoT devices are not designed which leads to management problem in terms of susceptibility and configuration



VIII. OPEN RESEARCH AND FUTURE DIRECTION OF IOT

The most challenging issue of IoT is to secure fully for complete adaptation of IoT in daily life. IoT technology requires more attention in terms of confidentiality which requires more complex system which increases the cost price so it also future challenge.In terms of power requirement, encryption algorithm, energy consumption for IoT devices is a future direction.

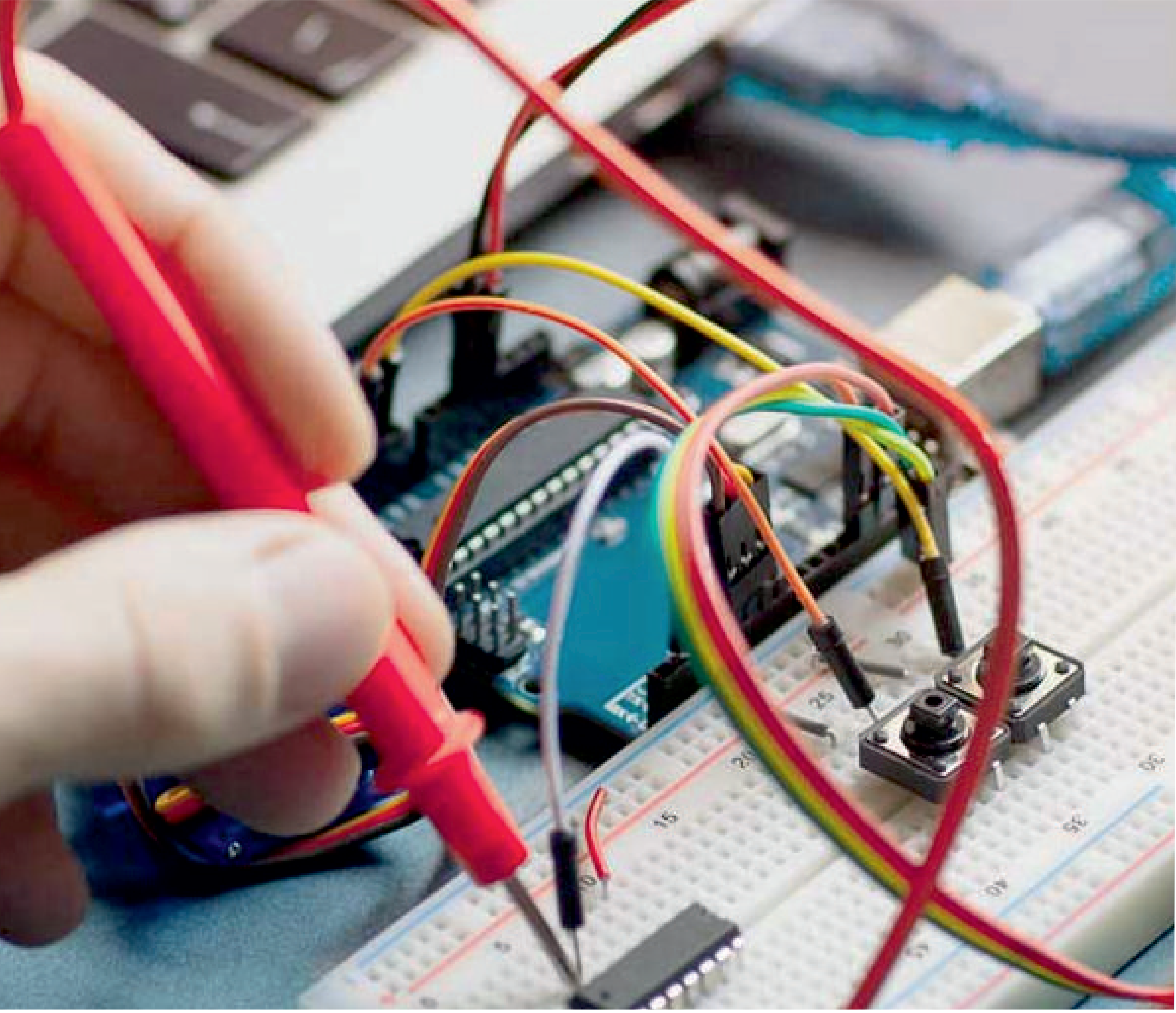
IX. CONCLUSION

The IoT devices are thosein which smart devices are connected to the networks. The architecture of IoT is discussed and the possible attacks with different layer are also mentioned. The mainidea is to highlight the security issues and challenges to the different layers of IoT. Security concerns in various layers with their measures are delivered. There is a limitation of use of cryptography in IoT or may impossible to implement. In this paper 3-layer,4-layer and 5-layer architecture of IoT Machine learning-trends for IoT is also discussed. To secure the IoT devices is a future open research in terms of confidentiality, integrity, access control and authentication. The most focusing attacks in this paper mentioned is WSN and RFID. Possible countermeasure or solution are mentioned.Lightweight encryption algorithm and ML are discussed for 4Gand 5G mobile system and beyond.

REFERENCES

1. Debabrata Singh,2Pushparaj,3Manish Kumar Mishra,4AnilLamba,5Sharabanee Swagatika "Security Issues In Different Layers Of Iot And Their Possible Mitigation",INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 04, APRIL 2020
2. HichemMrabet, Sana Belguith ,AdeebAlhomoud and AbderrazakJemai "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis",29 May 2020; Accepted: 23 June 2020; Published: 28 June 2020

3. **O**tmane El Mouaatamid, Mohammed Lahmer, Mostafa Belkasmi, "Internet of Things Security:Layered classification of attacks andpossible Countermeasures"e-TI – Numéro 9 – 2016 – http://www.revue-eti.net – ISSN 1114-8802
4. Vijaya Lakshmi Paruchuri, ―Data Confidentiality in Cloud using Encryption Algorithms‖, International Journal of Cloud-Computing and Super-Computing, Vol. 3, No. 2, Dec. 2016, pp:7-18.
5. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. J. Inf.
6. 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.
7. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. IEEE Trans. Ind. Inform. 2014,10, 2233–2243.
8. Hammoudeh, M.; Epiphaniou, G.; Belguith, S.; Unal, D.; Adebisi, B.; Baker, T.; Kayes, A.; Watters, P.A service-oriented approach for sensing in the Internet of Things: intelligent transportation systems andprivacy use cases. IEEE Sens. J. 2020.
9. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China,23–25 March 2012; Voume. 3, pp. 648–651.



International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijareeie@gmail.com

Scan to save the contact details

www.ijareeie.com