International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# Security Level Key Management Methodologies in IoT mode operations

**Arun Ganji[1], Dr. D. Usha[2]**

**Submitted**: 28/01/2024 **Revised**: 06/03/2024 **Accepted**: 14/03/2024

**Abstract:** Web of Things i.e IOT has given accepting an open door to fabricate strong frameworks and levels. Reliability is the principal worry in Internet of things supplication because of the protection of traded information passing on universal object interaction administrations utilizing restricted assets of object gadgets. From this Proposal as it goes input characterization of Universal object interaction (IOT).methods of activity in light of the conveyance of IoT gadgets, availability to the web, and common field of supplication. To give protection, the administration of clue for open is fundamental. At this paper, As we come across different clue administration conventions concerning IoT which be designated in lattice map connect. The guidedata is connecting between methods of activity and the related reliable clue admin components. The principal focus of this planning format data for originators in choosing the ideal security method that gives the higher split the difference between the necessary security level & IoT framework mode requirements.

***Keywords**:* Security Goals , IoT Security, Key Management, Key Generation, Key Distribution, Modes of Operations, MapLink, IoT Challenges.

## 1. Introduction

The development of conventional organizations begins with associations between PCs till IoT arises. IoT is viewed as another sort of world interconnection of exceptionally heterogeneous gadgets furthermore, machines. The fundamental benefits of this high innovation are given in high coordination web-based entertainment, computerized checking, and making choices in the agreeable manner [1]. Figure1 Shows the information life cycle for any Internet of things structures.

"The figure shows that IoT makes an interconnection between actual world items with the virtual universe of data by recognizing, detecting each other utilizing organization and registering abilities that will permit utilizing them to share data and achieve a few applications whenever, anyplace, with any person or thing utilizing anyway/network with any assistance[1]". The different low power utilization philosophies under IoT for smooth digitized correspondence are:

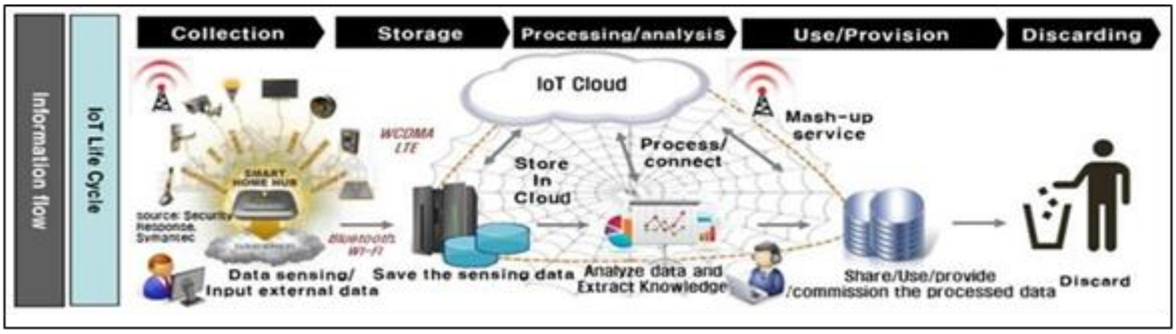


**Fig 1.** life cycle of data with IoT architectures

*Research Scholars[1], Associate Professo[2], Department of Computer Science and Engineering,*
*Dr. M.G.R. Educational and Research Institute, Chennai-95*
*E-mail id [a)]arun.ganji@gmail.com ,[b)]usha.cse@drmgrdudu.ac.in*

**Table 1:** Range of Communication Devices of IOT

| **Communication** | **Distance** | **Device** |
|---|---|---|
| Short Range | < 1 Meter | RFID , NFC |
| Medium Range | 1 m- 10 Km | Bluetooth, Zigbee, LTE,<br>NB_IOT |
| Long Range | >10 Km | LPWAN,VSAT |

Because of gathering an immense measure of information through detecting gadgets, this raises the requirement for a gigantic calculation with restricted assets which are utilized to break down, store and cycle these gathered information. Then again, distributed computing is helpful for taking care of enormous information acknowledging time unwavering quality, adaptability, adaptability, andsecurity as displayed.

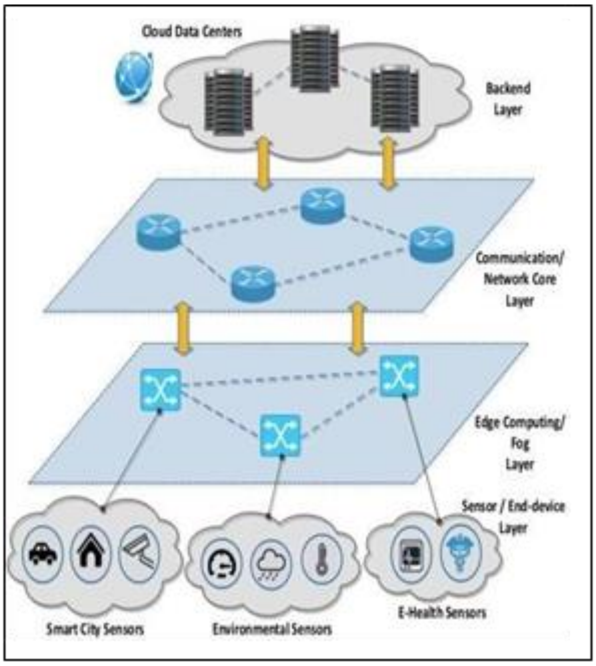


**Fig-2** :Edge Computing Communication Stack

From Figure-2 it shows mist processing [2,11] which is shown near the ground for saving of costly correspondence. Its primary design is ideal execution of IoT with the cloud by applying information put away, handled, separated, and investigated on the edge of the organization first previously moving to the cloud."IoT security is the innovation region worried about defending associated gadgets and organizations on the web[5]". It assumes a driven part with no edge for mistake or deficiency of supply. Thusly, security is significant for conveying great assistance with proficient expense, the board, and observing [3,4].

### 1.1 The principal security objectives are:

1. Concealment, which is a primary security issue to safeguard client information and secure client security.
2. Admittance (Access) control system is included two phases which are validation what's more, approval.
3. Testimonial (Authentication) been the primary period of any entrance control component which can decide the specific personality of the getting to party to lay out the trust of the framework.
4. Approval gives a component to connect a explicit gadgetto specific consents.
5. Probity is a compulsory objective in security to safeguard information by any means phases of its lifecycle. It implies guaranteeing that information is complete, unique, predictable, inferable, and exact.
6. Retraction keeps clients from denying sending or gettingan input for sure for really sent or got. All the mentioned security objectives can be acknowledged by various Strategies of safety components for Cryptography which is encryption and Cryptosystem

with validation also, check endorsement.

At this point, It is been zero in on arrangement of internet of things methods of activity with the two primary security key the board components. In the writing, unique arrangements are proposed to take care of the issue of key age and conveyance for IoT frameworks. Proposing a planning between these arrangements and each IoT methodof activity. This guide will assist the originators with choosing the ideal security methods that give the best split the difference between the necessary security level and IoT framework mode limitation

## 2. Literature Review

### ➢ Key management

"Key management refers to the management of cryptographic keys in a cryptosystem as shown in Key administration alludes[1]" to the administration of crypto logic keys in a cryptosystem as displayed in

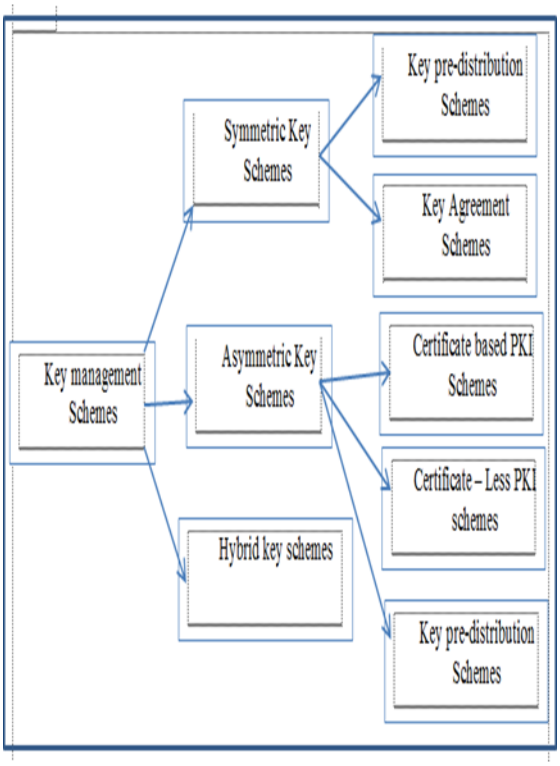

Key management Schemes
Symmetric Key Schemes
Asymmetric Key Schemes
Hybrid key schemes
Key pre-distribution Schemes
Key Agreement Schemes
Certificate based PKI Schemes
Certificate - Less PKI schemes
Key pre-distribution Schemes

**Fig 3.** Classification of Key management

The picture indicates the 3 cryptographic strategies that are summed up underneath

- ***Symmetric:*** It is a solitary common mystery key among the source and the beneficiary. At this class, the input to the board is characterized into pre-conveyed method and key settlement one. In redistributed, the mystery key is being conveyed previously any framework arrangement by Time Trigger Protocol. Then, the key understanding affirms the understanding of gatherings on a normal mystery key to be utilized after sending.

- ***Unbalanced :*** where a couple of keys is utilized for information trade among shipper and collector picture 3 shows that the uneven key control conspires is characterized into Certificate classification, ensured less classification, and key pre-circulation. The distinction between them is, the presence of an outsider in declaration based plans to guarantee the validness of the client's public key. Then again, in declaration less, the actual clients ensure their own public keys without the presence of Time Triggered protocol

- Mule : It is the blend of balanced and un balanced and key control plans. Key administration incorporates approaches to managing the principal key capacities like age, trade, capacity, appropriation, and invigorating of keys . It incorporates cryptographic convention configuration, key servers, [6] client strategies, and other applicable conventions. Effective key administration is as yet viewed as the primary apparatus for acknowledging security under IoT gadgets which are portrayed by restricted assets. Consequently, necessities to new plans of key age and appropriation are fundamental. In the following subsections, different key age and circulation strategies are recorded.[9].

### ➢ Key Generation

"Key transformation is tied in with proving from a reality where there is no key, to an existence where there is a key. A "key", here, is some worth with the right construction for some cryptographic calculation[1]" for example AES key is a grouping of 256 -192-128 pieces and for a RSA key is a bunch of a couple of enormous whole numbers which satisfy some explicit connections.[8] As the keys have esteem by being capricious by outsiders, key transformation essentially includes utilizing source information that is obscure to others this “Input information" will be irregular qualities got from aappropriate source.

**Overall, key input can be grouped into two sorts:**

- **First,** verified key where one of the correspondence gatherings can confirm the character of the other gadget.
- **Second [10]** an unauthenticated key age which they just produce a couple of keys without confirming each other.

Key conventions are characterized by fundamental variables which are cryptographic strategies, applications, the quantity of confided in individuals, and passes .In the accompanying sections, there are tests of overviewed articles that portray unique key age methods which take place IoT frameworks [11]. Key transformations is talked about improve security in Machine-to-Machine correspondence by giving an programmed key update system for Internet of things gadgets [12] The plan depends on which is a Constrained Application Protocol. Key administration orders the best match to IoT applications. Their trial results show 1 % inactivity upward is added for better security execution. The key status of stream comprises of utilizing pseudo random number for the input of the 20 bits LSB then involving it for the age of the other 32 bit MSB. From the [10] shows a cryptographic Key Producing and Renewing framework which is relevant for bunches of the IoT hubs or other frameworks. Its standard of working comprises of two parts as follows:

- **First:** equipment utilizing known party for key process and security of put away also traded information.
- **Second:** programming utilizing (MQTT) Message Queuing Telemetry Transport convention for trade information between hubs of the KGR framework.

Riddle and Code Secure Components are producing [13] producing private and public key matches in IoT gadget enlistment. It gives solid verification equipment based cryptographic key capacity and cryptographic countermeasures. It holds SHA-256, AES-128, HMAC, secure boot authentication which transforms smallinputs

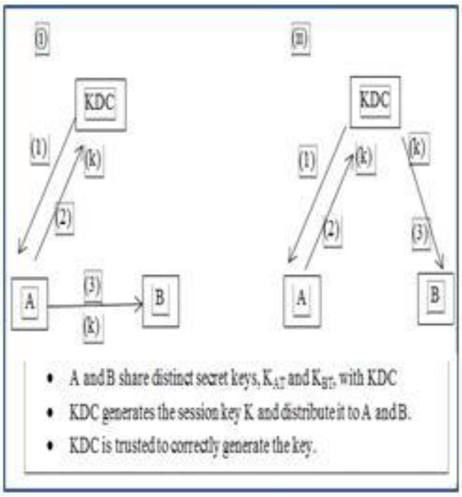
➢ **Key Distribution**

In key dissemination conventions, elements could be in the same or different security areas. Moreover, the Keys are disseminated by consolidating a trusted authority or determined by the actual elements [18]. In this manner, Key appropriation conventions are ordered into two classes:

- ***First:*** highlight point key foundation involves the substances not in the utilization of a confided in power. This technique is applied in little frameworks. The key can either be symmetric so the two gatherings can sharea similar key [15, 30, 36, 39] or deviated key where every one of the gatherings has a public-key with its related confidential key. A public key authentication of the expected beneficiary is for acknowledging information respectability and information beginning validation in a private manner.
- ***Second:*** Key foundation where Trusted Third Party is utilized. TTP is approved to offer key proceedings administrations like age, affirmation, conveyance, and interpretation of keying material [15, 30, 36, 39]. Thus, TTP is considered as Certification Authority (CA) wherein an enormous framework the key administration is coordinated in a progressive manner. Picture-4 Shows the methods of key foundation and commencement as portrayed underneath:

▪ ***KDC*** -Key Distribution Center which fundamental undertaking is to produce and convey keys upon substance demands. As these keys can be conveyed straightforwardly to elements or be sent back to the initiator, who advances them to the substance.

▪ ***KTC*** -Key Translation Center available which itgets the produced key from the substance. As this handles over the same way as referenced in Key distribution center by all things considered sending it straightforwardly to the nextsubstance or sending it back to the principalsubstance, which advances it to the subsequent substance. Keeping in thought that on accountof awry key, every element gets a suitable public declaration by reaching its position [15, 30, 36, and 39].



- A and B share distinct secret keys, $K_{AT}$ and $K_{BT}$, with KDC
- KDC generates the session key K and distribute it to A and B.
- KDC is trusted to correctly generate the key.

**Fig. 4.** Block Diagram Function for Keydistribution Center

As it was imposed that answer for secret information gathered from different electronic.[22]. The input will be on light of utilizing a marked (SSWC)- Sliding Window Coding in biometric cryptography innovation. " Signed Slide Window Coding standard of working is separating the normal element for sharing the produced M-piece key among gadgets worn on various body parts. This M-piece being produced from light weight commotion signals with high arbitrariness and raw adoption[1]".

Here the Author Commitments for light Low power edge with light weight encryption process for Secure Mobile Crowd Sensing Protocol for haze based application [21] The technique was ECC and extension over Triple Diffie Hellman key process is appropriate for low-power versatile gadgets. The creators focus on planning a secure mist with an edge layer which comprises of modest wearable gadgets with restricted computational assets. Haze functions as a point of interaction to remote server farms continuously. From [22], the plan depends on various leveled engineering made out of one – Key Distribution Focus and a few - Sub Key Distribution Focuses. De-centralized Light weight Group Key Management Architecture for processing and managing over internet of Things. As the primary elements are upgrading the administration, diminishing capacity and computational with communicational overheads in IoT dynamic climate, lastly bring down the Retrying upward on the Key Distribution Center

### ➢ *IoT Modes of Operations*

Internet of things is producing extraordinarily life applications which are affective to improve the personal satisfaction and to help the environment. Normal IoT spaces incorporate intelligence homes, gadgets, modern Web, savvy urban areas, farming, energy commitment, and medical services. The fundamental components in theseapplications are detecting gadgets, Gateways(GW), investigation, and capacity servers. Notwithstanding the previously mentioned spaces are undeniably ordered under IoT title, they have extensively unique engineering and methods of network. For model, the savvy metering application requires somewhat little and convenient uplink traffic from utility meters to the focal server, while brilliant urban areas applications require non-concurrent transmission between immense measures of gadgets and sensors that require higher information rates. Key

the executives is exceptionally impacted by the traits of the IoT administration, including geography, number of designated clients, and, surprisingly, the idea of information. Detecting applications that trade continuous natural data are refreshed regularly what's more, have an extremely short lifetime. Hence, it does not need an elevated degree of safety, so the keys could be traded less continuous or now and again could be hardcoded at the IoT gadget itself. On the other hand, utility metering incorporates touchy client data that influences protection and security, which calls for more grounded security measures, and hence intermittent key age and trade ought to be utilized. In view of the review introduced conspire, we characterize four distinct methods of IoT activity. By mode, we mean how information is traded between IoT gadgets and the cloud. This order intends to assist architects with choosing the ideal security conspire for various applications.

### ➢ **Centralized Mode**

A unified organization is a focal connector with the different hubs through the server. This focal server gets demands from hubs, then, appoints errands to them[29] In this method of activity, the Global Positioning System (GPS) can be utilized for telephone area recognition which is quite possibly the main bits of logical data for savvy application

### ➢ **Principal Mode Highlights:**

- Simple to keep up with, make due, secure, andcontrol

- Diminished costs as redundancies of capacity and it are stayed away from to deal with power
- Single-point network disappointment is asignificant issue

➢ **Centralization of Data Risk:**

- Risk on the security of our data since data is frequently put away on unified servers, leaving more noteworthy potential for hacks and spills.
- Equipment particulars for hubs are severe, may prompt shortcomings with non-standard gadgets and hubs

## 3. Device to Device (D2D) Mode

A Communication process with 2 devices as Device-to-Device (D2D) or which is been initiate are Machine-to-Machine-(M2M) and It is considered as distributed application and correspondence. Allocating the recurrence range or on the other hand same sharing recurrence gives the in the framework with greatest benefits which are utilizing a similar recurrence range are to get to the next level ingeneral throughput, range use, and energy effectiveness. It very well may be a group of houses associated less than 1 internal protocol in a similar organization to lessen calculation and correspondence. "The normal organization utilized in this mode of standard –based wireless technology network with Bluetooth-Low-Energy (BLE) correspondence. Another adding highlight is the direct associations between gadgets in crisis time like fire when the organization of the framework is down" [30]. The manner can be utilized in the most recent request utilizing the age of portable innovation like Long Term Evaluation and high end network technology, from the data in Gigabytes can be moved in proceedings. In this way, it very well may be utilized in the most refreshed applications with top of the line advancements update administrations like web perusing, streaming, virtual entertainment which need a higher information rate moved. The most widely recognized use cases of this mode is Remote Ad- Hoc-Network mode (WANET) as gadgets will get to one another's assets straightforwardly through an essential highlight point remote association[31]. All elements of steering, organization tasks, security, tending to, and key the executives are being finished by the assortment of gadget hubs without the requirement for any focal garcon. is an illustration of use cases article which depends on utilizing "Diffie-Hellman key understanding convention with secret key removed from actual channel qualities utilizing the computational hardness of discrete calculations which depend on haphazardness and uniqueness of remote blurring channel properties". Sadly, the utilization of discrete calculations for secret key extraction caused to bring down in key age rate what's more, higher correspondence above. This prompts the need to utilize the Diffie-Hellman with versatile gadgets which manages GHz level processor recurrence to higher the computationallimit. Considering at long last that the principal utilization of this convention is the combination with the current Wi-Fi direct convention.

➢ **sensor to Gate way Mode**

Gate Way is a significant key component in some IoT methods of activity to work with the general associations among sources and objections (gadget to gadget or gadget to cloud) as displayed in Figure. 5.

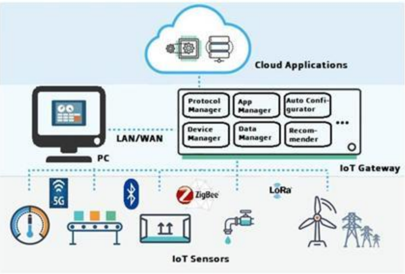


**Fig: 5** Gateway Community IOT Sensors

IoT Gateway developed to perform many undertakings from information separating to perception to complex examination by its equipment with the product stage. IoT Passage association undertakings are expressed underneath:

- Working with correspondence with associated gadgets with the non-webassociation.
- Information, pre-handling, onglomeration, separating, and advancement then, at that point, putting away, buffering, streaming, representation and examination.
- Oversee client access by gadget arrangement the board.
- Oversee network security elements and framework diagnostics.

The Open Automation Software (OAS) stage performs information conglomeration andsystems administration capacities. It can work atthe information source also as in the cloud. OAS stage is viewed as a adaptable answer for most

IoT and IIoT execution like displayed in Fig. 6.

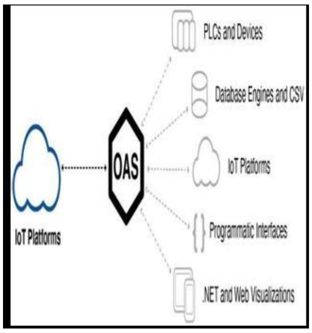


**Fig 6:** Open Automation Software Platform in IOT

Fig. 7. Illustrates the GW design layers of Internet of things GW is comparable in obligation to some layers like checking, preprocessing, capacity furthermore, security layers. GW plays as a point of interaction block between brilliant gadgets and the cloud information focus or server [34].

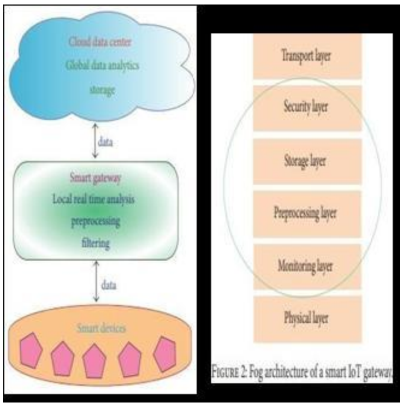


**Fig. 7.** Illustrates smart way of communication

"The normal use cases of this mode is Smart- Metering (SM) applications where the power Utilization of home machines is being sent from a gathering chief to SM by two cases [32]":

**First:** For the situation of few machines, don't bother the gathering yet direct correspondence among pioneers and gadgets to gather power utilization information by means of balanced.

**Second**: in the event of an enormous numbers, the entirety home machines fill in as a gathering where the Specialist organization (SP) refreshes that gathering in a WBAN climate. Creators of

[32] understand security in SM bunch conditions in light of key trade with bunch validation in a dynamic way. Its fundamental objective is gathering information from sensors then, at that point, sending it to SP which fills in as a door like displayed in Fig. 8. This SM bunch correspondence is superior to balancedcorrespondence in decreasing correspondence above. The plan in [32] acknowledges security byapplying

The following three stages:

1. Enlisting Phase
2. Bunch verification Phase
3. Meeting Key circulation stage

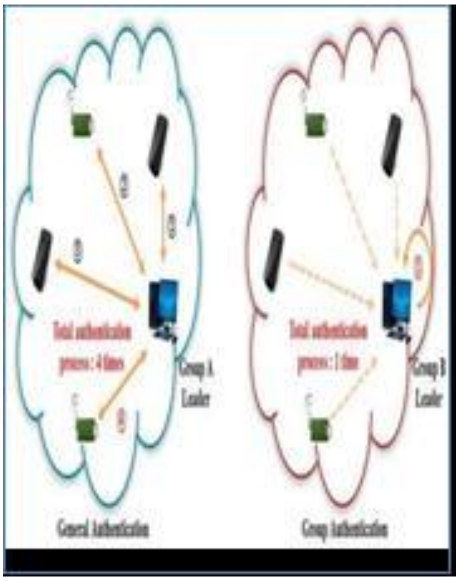


**Fig 8:** Separation of single and Group approval Communication

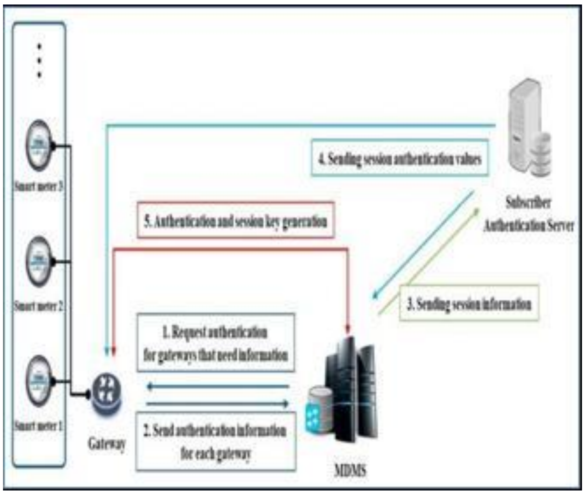

Smart meter 3
Smart meter 2
Smart meter 1
Gateway
4. Sending session authentication values
5. Authentication and session key generation
Subscriber
Authentication Server
3. Sending session information
1. Request authentication
for gateways that need information
2. Send authentication information
for each gateway
MDMS

**Fig. 9.** Smart Meter and Gate way AuthenticationPhase with Meter Data Management System

- **Collaborative Mode:**

The new group detecting applications are considered as normal use cases in cooperative mode [33]. This mode opens great advancement in high level IoT genuine applications by its sensors or gadgets on implanted frameworks or potentially versatile gadgets, for example, cell phones, workstations, tablet PCs furthermore, wearable gadgets and so forth. Instances of these genuine applications are the savvy stopping framework and savvy medical services framework utilizing the portable with a secret key from the service organization for entirety understanding assortments. The cooperative model improves the processing abilities of the mind boggling and colossal information handling by consolidating handling abilities and detecting in view of the Portable Cloud Computing (MCC) worldview. Cooperative method of activity is considered as a way to deal with beat the incorporated mode Disadvantage which prompts correspondence framework delays. This idleness disadvantage has an incredible negative aftereffect in unique sight and sound information for example, applications in light of video and picture securing gadgets[36,37] This method of activity is being applied in different organization layers and their registering stages included. The fundamental approach of applying this mode is coming to the streamlining utilization of computational assets of an IoT climate.

It represents one of the cooperative mode use cases called Secure Mobile Crowd detecting Convention (SMCP) for haze based applications". The plot depends on two kinds of lightweight encryption strategies which are Extended Triple Diffie-Hellman Key understanding (X3DHKA) which is applied in Android and IOS applications for low power cell phones. The subsequent kind is the Elliptic Curve Cryptography (ECC). The primary parts of this plan are:

- The Edge Device(ED) : it has the primary undertaking of catching crude information like done in wearablegadgets.
- The Fog Devices (FD): with huge registering power the board of alternate quantities of EDs. It fills in as

constant connection point between EDs also, remote cloud server farms.

- Cloud Data Center (CDC): regulates the new enrollment of the framework with its edge and haze gadgets as indicated by the comparing applications.

➢ ***Main elements of IoT Connectivity***

Information rate, Coverage, and energy effectiveness are the three key specialized measures expected in IoT modes of tasks. The accompanying depictions of these boundaries are given.

## 4. Information Rate (On Up/Downlink)

IoT application information rates range from a couple hundred pieces each second (bps) for metering to a few Megabits each second (Mbps) for uplink video and are advanced to information bundles with the rising intricacy of IoT applications for downlink abilities. Wi-Fi and cell networks have high information rates with their short range data transfer capacity or with complex waveforms and versatile balance. While most LPWA innovations have lower information rates due to applying hearty tweak conspires yet at the same time with lower energy utilization run on microcontrollers with restricteddatatransmission.

➢ ***Coverage:***

To associate gadgets, all IoT applications require solid inclusion, while others simply require inclusion in unambiguous inside areas, for example, mentioned in unified savvy home applications mode and D2D mode; be that as it may, others request critical inclusion in far off regions, for example, in GW and cooperative modes. Inclusion can be applied by different cell advancements which can be ordered into open air and indoor. Outside

for example, utilizing 3G or 4G which are viewed as a genuine illustration of a Wide Area arrangements. There is likewise the Low Power Wide Area (LPWA) with its similarity with IoT power imperatives. Indoor which isdescribed by short-range correspondence utilizes Wi-Fiand Zigbee innovations.

➢ ***Energy effectiveness:***

The energy effectiveness of an association innovation significantly affects the lifetime of upkeep pattern of IoT gadgets that depend on battery or energy collecting, and it is impacted by the utilization of the application primary boundaries like availability innovation's reach, geography, intricacy, the length and recurrence of message transmission. At last, we can say that all the previously mentioned

IoT factors influence the availability methods of activities relying upon applications. In brilliant meters, for instance, there is a requirement for high energy effectiveness and information rates. SM requires a dynamic difference in exchange key to keeping up with the protection which could cause acknowledged resilience postpone in SM. Be that as it may, for the instance of vehicle application, there is a more serious requirement for speedy reactions, portability and, situating more than energy proficiency.

## Conclusio

IoT is a significant keen web innovation for actual item associations. It has independent control highlights andsimple admittance to object without any human communication in various application fields. Security is viewed as the principal advancement estimating device forIoT as it is one of the major IoT challenges. Theunwavering quality and security of IoT items rely upon powerful end-to end ways to deal with safeguard purchasers and their information. The fundamental papercommitments are: first, characterizing the IoT availability method of tasks upon the incorporated and decentralized Classifications. Second, presents different IoT key the board security studied articles with its principal vivacious engine key components which are critical age and conveyance. Third, assigns these referenced security overviewed articles under the appropriate method of tasks crossing with key age and conveyance in a matrix map connect table. This planning table between the fundamental two proposed article aspects which are IoT methods of activities and security components helps architects in choosing the ideal security strategy that gives the best split the difference between the expected security level also, each IoT mode imperative.

## References

[1] J. Sathish Kumar , Dhiren R. Patel ,” A Survey on Internet of Things: Security and Privacy Issues”, International Journal of Computer Applications (0975 – 8887), Volume 90 – No 11, March 2014.

[2] Somayya Madakam, R. Ramaswamy, Siddharth Tripathi,” Internet of Things (IoT): A Literature Review”, Journal of Computer and Communications, India, Volume 3, Pages 164- 173, January 2015.

[3] Chris Folk, MITRE, Dan C.Hurley, “The security implications of the Internet of Things”,AFCEA International Cyber Committee, February 2015.

[4] Inayat Ali*1, Sonia Sabir1, Zahid Ullah, “Internet of Things Security, Device Authentication and Access Control: A Review”, (IJCSIS) International Journal of Computer Science and Information Security,Pakistan , Vol 14, No 8, August 2016.

[5] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva,” Security for the Internet of Things: A

Survey of Existing Protocols and Open Research Issues", IEEE communication University (ICU), page no. 305- 732,Korea,2000

[6] Ramaswamy Chandramouli , Michaela Iorga , Santosh Chokhani," Cryptographic Key Management Issues & Challenges in Cloud Services', National Institute of Standards and Technology Interagency or Internal Report 7956 (NISTIR) , September 2013.

[7] Manikandan G1, Sakthi U2, "A Comprehensive Survey on Various key Management Schemes in WSN",Second International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2018) IEEE Xplore Part Number:CFP18OZV ART, ISBN:978-1-5386-1442-6, India, 2018.

[8] Christof Paar et al., Understanding Cryptography © Springer-Verlag Berlin Heidelberg 2010, Pages 331-357

[9] Chapter 13,Key Establishment George Margelis , Xenofon Fafoutis, George Oikonomou , Robert Piechocki , Theo Tryfonas , Paul Thomas, "Efficient DCT-based secret key generation for the Internet of Things ", Ad Hoc Networks 92 (2019) 101744 , Denmark, August 2018.

[10] Janusz Furtak, "Cryptographic Keys Generating and Renewing system for IoT Network Nodes-A Concept", Sensors 2020, 20, 5012; doi:10.3390/s20175012 ,Poland , Septemper 2020

[11] Boyeon Song and Kwangjo Kim, "Comparison of Existing Key Establishment Protocols", Information and Communications University (ICU), page no. 305-732, Korea, 2000.

[12] Wen-Chung Tsai, Tzu-Hsuan Tsai, Guang Hao Xiao, Te-Jen Wang, Yu-Ruei Lian, Song□Hao Huang," An Automatic Key-update Mechanism for M2M Communication and IoT Security Enhancement", 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Tiawan , 2020.

[13] Mohammad Wazid 1 , Ashok Kumar Das 2 , Sachin Shetty 3 , Joel J. P. C. Rodrigues 4,5 and Youngho Park," LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge Based IoT Deployment", Sensors 2019, 19, 5539;doi:10.3390/s19245539,2019.

[14] Mohamed H. Eldefrawy, Nuno Pereira and Mikael Gidlund," Key Distribution Protocol for Industrial Internet of Things without Implicit Certificates", Citation information: DOI 10.1109/JIOT.2018.2865212, IEEE Internet of Things Journal,2018.

[15] Bashar Alohali*, Kashif Kifayat, Qi Shi, William Hurst," A Survey on Cryptography Key Management Schemes for Smart Grid" Journal of Computer Sciences and Applications, 2015, Vol.3, No. 3A,27-39 , UnitedKingdom,2015.

[16] Chandrasegar Thirumalai, Himanshu Kar," Memory Efficient Multi Key (MEMK) Generation Scheme for Secure Transportation of Sensitive Data over Cloud and IoT Devices", International Conference on Innovations in Power and Advanced Computing Technologies [i-PACT2017],India , 2017

[17] I.V. Chugunkov1, O.Уu. Novikova, V.A. Perevozchikov, S.S. Troitskiy," The Development and Researching of Lightweight Pseudorandom Number Generators", IEEE , Russian, 2016.

[18] Fangmin Sun, Weilin Zang, Haohua Huang, Ildar Farkhatdinov and Ye Li," Accelerometer-Based Key Generation and Distribution Method for Wearable IoT Devices", Citation information: DOI 10.1109/JIOT.2020.3014646, IEEE Internet of Things Journal,2021.

[19] Federico Concone, Giuseppe Lo Re and Marco Morana," SMCP: a Secure Mobile Crowdsensing Protocol for fog-based applications", Concone et al. Hum. Cent. Comput. Inf. Sci. (2020) 10:28, Italy, 2020.

[20] Maissa Dammak1, Sidi Mohammed Senouci1, Mohamed Ayoub Messous1, Mohamed Houcine Elhdhili2, Christophe Gransart3, "Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments", IEEE Transactions on Network and Service Management, June 2020.

[21] Akbar Morshed Aski1 · Hamid Haj Seyyed Javadi2 , Gholam Hassan Shirdel3," A Full Connectable and High Scalable Key Pre-distribution Scheme Based on Combinatorial Designs for Resource-Constrained Devices in IoT Network", Wireless Personal Communications, Iran, MAY 2020.

**[22]** Daemin Shini,2, Keon Yuni,Jiyoon Kini,Philip Virgil Astillo1,Jeong-Nyeo Kim3,And Ilsun You1,"A Security Protocol for Route Optimization in DMM- Based Smart Home IoT Networks", special section on security and privacy in emerging decentralized communication environments, South Korea , 2019.