A Survey on securing communication between IoT application and private cloud with hybrid algorithm

[1]Kunj S Patel, [2] Ms.Vineeta Tiwari, [3]Ms Ruchika Vyas
[1]M.Tech student, [2] Principal Technical Officer, [3] Project Engineer
ITSNS Department
Gujarat Technological University, Ahmedabad, India

Abstract: IoT is connected with real world and cyberspace via CLOUD (physical substance) that embedded devices loaded with sensors which collects information from the surroundings, and process it & relay it to remote area for further process via different layer of IoT. Because of cloud characteristics peoples are attracted towards the utilize the power of cloud computing. To store the IoT data and process the Data cloud is integrated with IoT devices. Communication between cloud and IOT is totally in networking channel so here the security of the communication channel and data security is very important from various attacks on each layer. To provide security from that attack various encryption method is used.

Keywords: IoT Security, Cloud with IoT Security.

I. INTRODUCTION

The time of distributed computing and IoT convey new plan to utilize the savvy gadgets in our every day life. IOT is absolutely remote and RFID through remote system and innovation to accomplish transmission and handling. Security is identified with label data (RFID), remote correspondences data security, arrange transmission of data security, protection and security data handling security.so it is essential to study and research on outline and expanding a security issue in IOT. IOT dole out the physical gadgets which are settled with web, hardware, programming, sensors, actuators, and system network. It is a mix of specialized design, ip based correspondence, and advances are advance the trading of shrewd question benefits over uncertain channels, along these lines security and protection is the principle issue of associated client is the prime issue. There are some security hazards in the two consumers and business in IOT, so information encryption can be utilized to decrease security risks. Giving a reasonable encryption calculation can assume a powerful part in diminishing the security dangers. This sort of encryption can be an open key cryptography which fast in encryption security and less memory necessity are its specifications.[6]

II. BACKGROUND SURVEY

A. IoT

A system of web associated objects ready to gather and trade information utilizing implanted sensors. Fundamentally this is the plausibility of basically connecting any contraption with an on and off change to the web. This incorporates everything from cell phones, espresso producers, clothes washers, earphones, lights, wearable gadgets and nearly whatever else you can consider. This also applies to sections of machines for example a stream engine of a plane or the center of an oil settle. As I specified, in the event that it has an on and off switch at that point chances are it can be a piece of the IoT. The relationship will be between human individuals, human things, and things-things.

I. IoT layer Architecture & Protocol

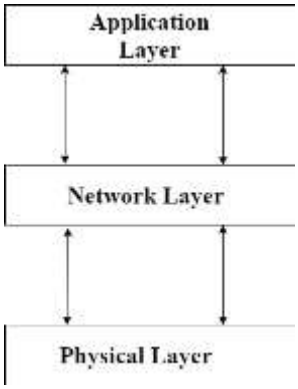

Figure 1 IOT Layer Architecture

Table 1 IOT Protocol

Application Layer	HTTP,COAP,EBHTTP,LTP,SNMP,IPFix ,DNS,NTP,SSH,DLMS,COSEM,DNP,M ODBUS
Network/Communication Layer	IPv6/IPv4,RPL,TCP/UDP,UIP,SLIP6Lo WPAN
Physical /MAC Layer	IEEE802.11 series,803.15 series,802.3, 802.16,WirelessHART, Z-WAVE,UWB,PLC,KNX

II. IoT Application

Smart Home:- Smart Home obviously emerges, positioning As most surprising IoT application on every last deliberate channel.[7]

Wearable:- wearable have encountered a touchy request in business sectors everywhere throughout the earth. Wearable gadgets are presented with sensors and programming which accumulate data and information about the customers. This information is later pre-prepared to separate fundamental bits of information about client.[7]

Smart city:- smart city crosses a wide collection of utilization cases from action organization to water movement to misuse organization urban security and natural checking.[7]

Smart grids:- Smart grids is a special one. A future smart network guarantees to utilize data about the practices of power providers and buyers in a mechanized manner to enhance the productivity, unwavering quality, and financial matters of power.[8]

Industrial internet:- Industrial web is the advanced buzz in the advanced division furthermore named as modern internet of things (IoT). It is enabling modern building with sensors, programming huge data examination to make splendid machines.[7]

Connected health:- Associated health remains the resting goliath of the IoT applications. The possibility of a related human administrations system and splendid restorative contraptions bears immense potential not just for associations in like way for the thriving of individuals as a rule.[8]

Smart farming:- Because of the remoteness of cultivating operations and the huge number of domesticated animals that could be observed the IoT could upset the way agriculturists work.[7]

III. **IoT Security Issues & Attack**

Data Encryption:- Internet of things applications assemble tremendous measures of data. Data recuperation and getting ready is fundamental bit of the whole IoT condition. A vast bit of this data is up close and personal and should be guaranteed through encryption.

Data Authentication:- After powerful encryption of data chances of contraption itself being hacked still exist. If there is no genuine approach to develop the authenticity of the data being granted to and from an IoT device, security is bartered.

Malicious Code injection:- The attacker deals a middle point by physically injecting it with malicious code that would give him access to the IoT structure.

Denial of service:- An attacker can execute DoS or appropriated refusal of advantage DDoS attacks on the impacted IoT organize through the application layer, affecting all customers in the framework.

Phishing Attack:- The attacker gets to private data by satirizing the confirmation certifications of a customer, as a general rule through debased messages or phishing destinations.

MITM:- Right when two customers of an IoT structure A and B, exchange keys in the midst of a test response circumstance, so as to set up a safe correspondence Channel an adversary positions himself among them on the correspondence line. The adversary by then catches the signs that A and B send to each other and attempt to interfere by playing out a key exchange with A and B freely. The adversary will then have the capacity to unscramble/scramble any data beginning from A and B with the keys that he confers to them two. Both A and B will ambience that they are visiting with each other.

Brute Force Attack:- Brute force is an experimentation strategy used by application projects to interpret scrambled information for example passwords or information encryption Standard (DES) keys, through comprehensive exertion as restricted to utilizing scholarly methodologies.

B. CLOUD

cloud a model for empowering inescapable accommodating on ask for arrange access to a run of the mill pool of configurable figuring assets that can be instantly provisioned What's more, released with inconsequential organization achievement or pro association affiliation. Because of cloud characteristics like on-demand self-service, Broad Network access, resource pooling, rapid elasticity, measured services so that peoples are attracted around the cloud innovation. Cloud provide a various services in form of service model like IAAS (Infrastructure-as-a-Service), PAAS (Platform-as-a-Service), and SAAS (Software-as-a-service). All cloud are not same so there are four different deployment model of cloud like Private cloud, Public cloud , Hybrid cloud , Community cloud.

III .METHODOLOGY

In, 2017 authors in article of [6] have presented hybrid approach using AES symmetric block cipher & NTRU Encryption algorithm. Here fundamental motivation behind encryption is smart home framework can safely communicate with IOT devices.

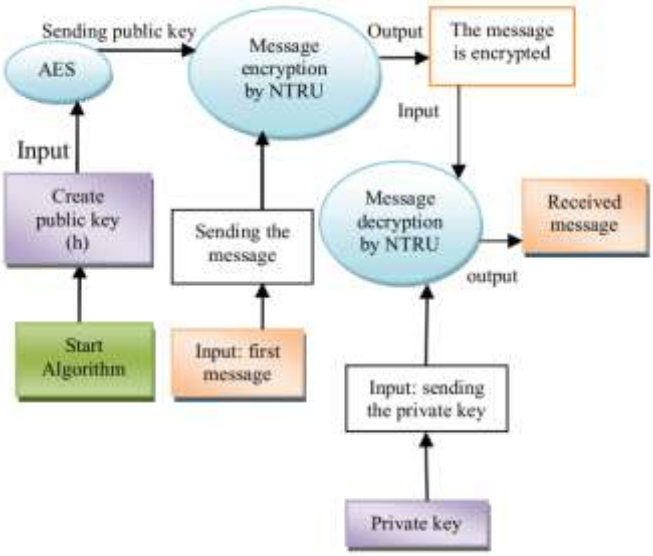

Figure 2. HAN Encryption Algorithm Step.

In, 2016 authors in article of [5] have presented secure data transaction over system or LAN. Here they used Kerberos along with PGP to overcome issue of nonrepudiation.

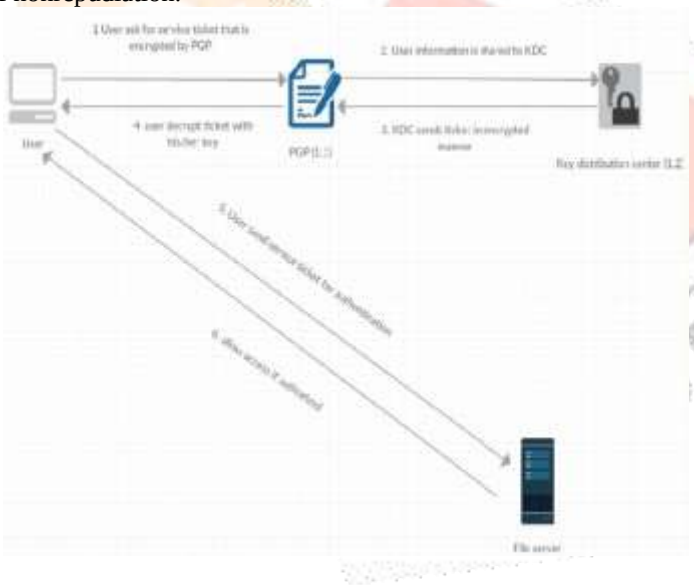

Figure 3. Proposed Model

In, 2017 authors in article [4] have exhibited a one-time file encryption protocol for IoT devices here they implement IBE (ID Based Encryption system) using the computational advantage of ECC (elliptic curve cryptography) with the small key length and is equivalent to secure RSA.and also used DH(diffie-hellman) protocol for session key establishment between entities.

In, 2017 authors in article [3] have implemented security system for distribution of key between user and cloud service provider. Here they implement DH key trade for IoT nodes in cloud Network to secure again internal and external traffic, protect against MITM attack, DOS attack etc.

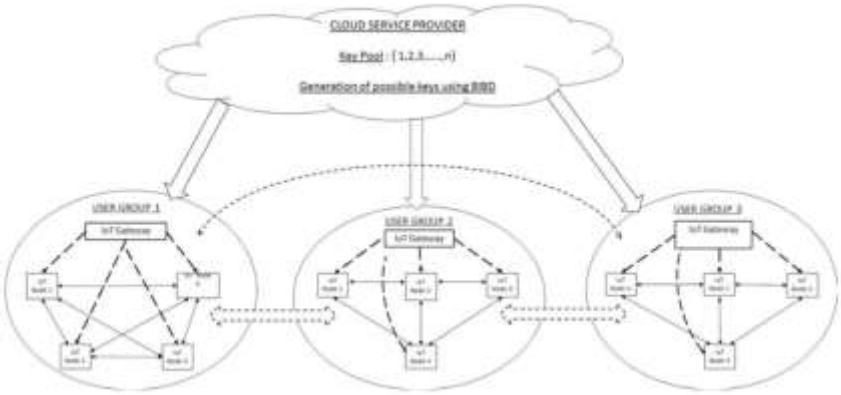

Figure 4. Proposed model of secure key Distribution

In, 2013 authors in article of [2] presented hybrid encryption algorithm using DES & RSA Encryption in Bluetooth connections.

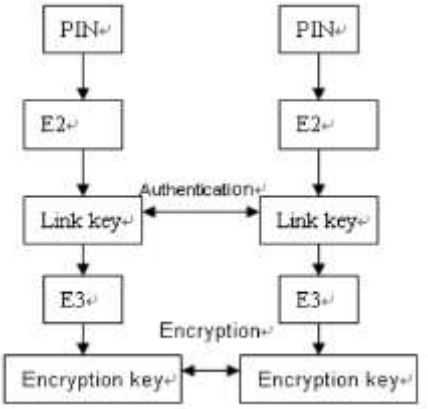

Figure 5. Process of Bluetooth Encryption

In, 2016 authors in article of [1] present identity-based Confirmation scheme for heterogeneous IoT system. And give some basics introduction about IoT and SDN. Here they used ECC cryptography algorithm for certification.

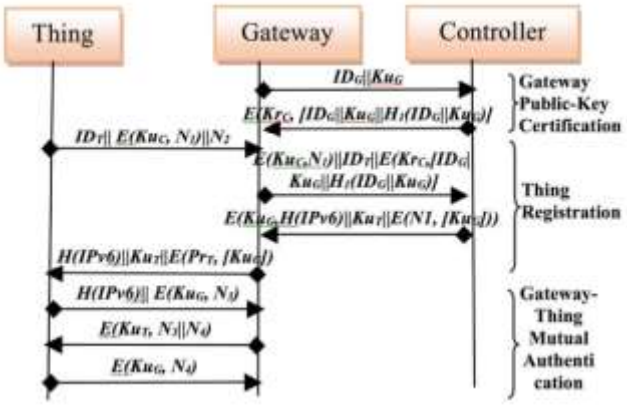

Figure 6. Protocol Message Flow

IV. CONCLUSIONS

In this Paper we have study the basics of IoT and Cloud Computing. Also we have study the suggested system to secure the communication channel between user to IoT node through Cloud System.so here we conclude that various symmetric and asymmetric encryption algorithms can be used to more secure the communication to prevent the various type of attacks.

REFERENCES

[1] Ola Salman Sarah Abdallah Imad H. Elhajj Ali Chehab Ayman Kayssi," Identity-Based Authentication Scheme for the Internet of Things", 2016, IEEE Symposium on Computers and Communication (ISCC).

[2] Wuling Ren, Zhiqian Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", 2010 , Second International Conference on Modeling, Simulation and Visualization Methods.

[3] Soumya Ranjan Moharana, Vijay Kumar Jha, Anurag Satpathy, Sourav Kanti Addya, Ashok Kumar Turuk, Banshidhar Majhi, "Secure Key-distribution in IoT Cloud Networks" , 2017 , 3rd International Conference on Sensing, Signal Processing and Security (ICSSS).

[4] Biao Wei, Guohong Liao, Weijie Li , Zheng Gong , "A Practical One-time File Encryption Protocol for IoT Devices" , 2017 , IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)

[5] Moin A. Khorajiya , Gardas Naresh Kumar , "A Security based Architecture using Kerberos and PGP" , 2016 , ACM.

[6] Afsoon Yousefi , Seyed Mahdi Jameii , "Improving the Security of Internet of Things using Encryption Algorithms" , 2017 , IOT and Application (ICIOT), International Conference on.

[7] iot-analytics.com, knud lasse lueth, "**The 10 most popular Internet of Things applications right now**", 2015. [Online]. Available: **https://iot-analytics.com/10-internet-of-things-applications/** [Accessed: 21-November -2017]

[8] analyticsvidhya.com , Swati Kashyap , "**10 Real World Applications of Internet of Things (IoT) – Explained in Videos**" , 2016.[Online]. Available:**https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/** [Accessed: 20-November-2017]