International Journal of Research in Advent Technology, Vol.7, No.6S, June 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Survey on Securing IoT Architecture through Modern Techniques

Nithyashree C M, Dr. Sandeep Varma N

Abstract—Internet of Things can be defined as connection of millions of devices through network. As the number of devices are rapidly increasing, it raised the issues like scalability, flexibility, security and efficiency among IoT system. thus, the efforts should be put to design the IoT architecture to overcome the challenges. In this paper, the brief introduction to IoT is given, followed by the challenges faced by IoT system. The secure IoT architecture using modern technologies like NFV(Network Function Virtualization) and ICN(Information Centric Networking) are explained.in the end the comparison of different techniques used for IoT system is illustrated.

IndexTerms— Internet of Things, Network Function Virtualization(NFV), Information Centric Networking(ICN).

I. INTRODUCTION

The Internet of Things (IoT) is an idea that includes systems administration of gadgets at endpoint and physical devices[1] to increment accommodation as well as effectiveness of regular day to day life. The IoT system incorporates ground breaking applications, for example, brilliant homes, structures, urban areas, retail, transportation, and open wellbeing. Advantages of IoT incorporates use of asset use effectively, limit the human exertion, it spares time.

The Internet of things (IoT) is theprolongation of Internet connectivity to physical devices and everyday objects. The electronic devices, other hardware such as actuators and sensors which contains embedded technology can communicate over the internet and also can be remotely controlled and monitored. Due to combination of technologies like embedded system, sensors and real-time analytics, internet of things has come into picture.

In 1998, the term internet of things was coined.it refers to interconnection of devices by the internet. As of late, the idea of IoT has turned out to be most basic in different applications, for example, medicinal services checking, keen farming, brilliant lattice, shrewd retail, keen assembling, savvy home the board, etc. Applications, heterogeneous entree, data handling, and detecting, are considered as the significant segments that can be as a component of IoT framework [1]. In expansion towards that, there are security and protection by means of imperative parts in the IoT system. The glitches are progressively increasing in terms of security in IoT.

The paper reconnoiters challenges related to the Internet of Things along with a review of various techniques used to secure IOT Architecture and system and future work in this innovative area.

The content of this paper is given as pursues: The difficulties of the Internet of Things are advised in Section II. Segment III gives writing audit. The different techniques utilized for IoT System to defeat these difficulties and give security, versatility and protection to Internet of Things (IOT) framework are given in Section IV. Segment V gives the examination of the considerable number of procedures which are advised in Section IV. At last, the paper end and future headings are exhibited in Section VI.

II. CHALLENGES OF IOT

Privacy

Privacy plays important role in users accessing and processing data in IoT. Due to large number of connecting devices, service and common communication which is shared by people, privacy has key role in security principles. The critical privacy problem is confidentiality of user's data for having the communication ability.

To overcome the data privacy challenges, we must incorporate efficient security features for IoT applications [2]. The IoT privacy issues includes:

- Huge Data:The volume of data which is generating from IoT devices is irresistible. If the data generation continues to increase in this phase, it results in creating more entry points for the hackers and is threat to private information.

Security

Security is major concerns for protecting the devices, data and networks from the hackers. This can be resolved by designing the technologies and policies to preserve the data integrity and to look after the unauthorized access of information[2].

The chances of exploiting the security vulnerabilities has amplified due to increase in number of connected devices. The security of IoT deals with protecting

Manuscript revised May 13, 2019 and published on June 5, 2019
Nithyashree C M, *Mtech Student, Dept of Information Science & Engineering, BMS college of Engineering, Bangalore, India*
Dr. Sandeep Varma N, *Assistant Professor, Dept of Information Science & Engineering, BMS college of Engineering, Bangalore, India*

doi: 10.32622/ijrat.76S201918

the connected devices and network of the system. It has a problem of a greater number of unsecured devices which communicate through the internet. As expanding the number of associated devices, the opportunity to exploit security vulnerabilities is likewise increment, as in modest or low standard structured devices, because of inadequate information streams the odds of information burglary is expanded through which individual's health and safety can be unsafe.

Various IoT systems will have group of similar or adjacent similar devices. This consistency grows the potential effect of any single security shortcoming by the absolute quantity of devices that all have similar highlights[3].

Scalability

Scalability is the capacity of a device to adjust to the changes in the environment and meet the changing needs. It is important feature of any system which has the capability to grip the growing amount of work.

As the number of devices which are connected to the IoT systems are increasing, scalability has become the major threat. The devices should have the ability to adjust to the environment of the system. There should be a specialized solution to make people to understand the issues in working with the software and legacy systems.

Connectivity

The biggest challenge of IoT is connecting numerous numbers of devices, and it will affect the current communication structure and technologies underlying it. Some systems use centralized, server/client approach to authorize, validate and connect nodes in network.

The centralized model is effective for present IoT frameworks, in which a great many gadgets are included. Be that as it may, when these number increments to join a huge number of gadgets, this framework will be moved toward becoming bottleneck. Such frameworks will require tremendous speculations and costs in keeping up cloud servers that can deal with such a lot of data trade, and whole frameworks can go down if the server ends up inaccessible.

The IoT system can be depend on decentralized network to take care of above-mentioned issues. This can be possibly achieved by moving IoT architecture towards the edge, with the help of fog computing systems in which cloud servers can take responsibility of data collection and analytics and smart devices such as IoT hubs take care of mission-critical operations.

III. LITERATURE SURVEY

This section provides a review of literature on different techniques used to secure IOT system.

Igor Miladinovic and Sigrid Schefer-Wenzl has proposed a NFV enabled IoT architecture for scalability of IOT Architecture. As a southbound interface for IoT application's they adopted web services based on representational state transfer (REST) web architecture[4].

Robert E. Hiromoto, Michael Haney and Aleksandar Vakanski has given a Secure Architecture for IoT with Supply Chain Risk Management. The system which is proposed will reduce vulnerabilities of malicious supply chain risks by using technologies like machine learning (ML), cryptographic hardware monitoring (CHM) and distributed system coordination (DSC) techniques to alleviate the consequences of unforeseen (including general component failure) threats[5].

Pradip Kumar Sharma, Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park has designed a Distributed Blockchains-Based Secure SDN Architecture for IoT Networks i.e. DistBlockNet. This combines the advantages of two emerging technologies: SDN and blockchains technology[6].

Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco and Alberto Coen-Porisini described detailed IOT Architecture using ICN(Information Centric Networking) for securing purpose[7].

Dr. S. Smys and S. Sridhar proposed an Intelligent Security Framework for IoT Devices. The proposed architecture actualizes Asymmetric Key Encryption to share session key between the hubs and afterward utilizes this session key for message exchange This shields the framework from Distributed Denial of Service Attacks and Quantum calculation attacks[8].

Amiya Kumar Sahu, Suraj Sharma, Deepak Puthal, Abhishek Pandey and Rathin Shit considered a smart home based on IoT architecture where the IoT smart Hub(ISH) communicate with the cloud in one hand, and home appliances and smart devices on the other. This design ensures security in the smart home scenario[9].

Effy Raja Naru, Dr. Hemraj Saini, Mukesh Sharma has provided an excellent insight into the lightweight techniques used for secure data transmission in IOT[10]..

IV. TECHNIQUES

IoT architecture based on Network Function Virtualization

In many ways we can incorporate NFV and SDN In an IOT architecture and these approaches helps in reducing IoT traffic, cost savings and helps in faster service innovation. The architecture [4] address the benefits of security, specified its less complex to apply and preserves the security measures on a centralized system rather than on single devices. The other advantages of these architecture are scalability and maintainability of the system.

Fig 1, represents architecture which is proposed. The sensors and actuators communicate with IoT gateway. The IoT gateway are not responsible for any application logic rather runs on a simple hardware. The purpose of gateway rendering between IP protocol towards its northbound interface and divers' protocol which are necessary for IoT device towards its southbound interface. Ensuring the NFV concepts, the application logic is available in data center and

doi: 10.32622/ijrat.76S201918

keeps running on standard equipment, regular for all applications for differing network functions. As needs be, the IoT application is comprehended as a network function and centralized in a data center.

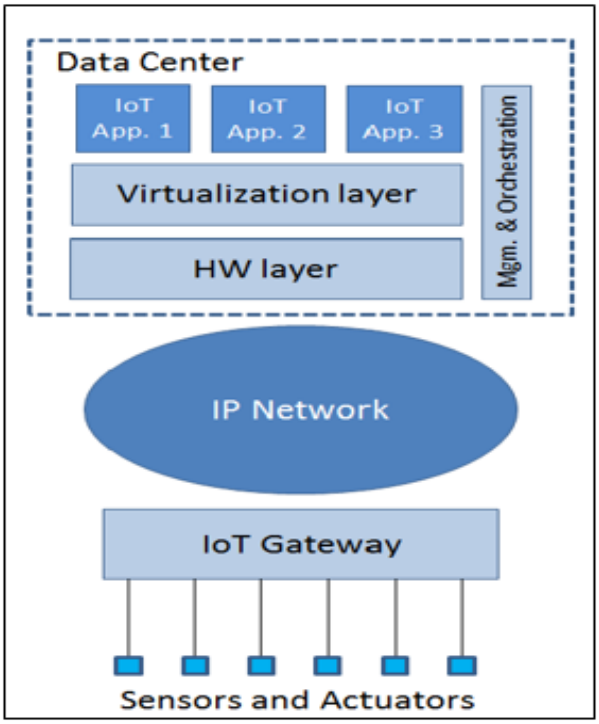

Fig 1. NFV based IOT Architecture

The different layers of the data center's functions are given below:

- HARDWARE LAYER consists of COTS hardware components, together with network interfaces, storage and CPUs. This serves as elastic as well as scalable hardware platform for network functions and to all IoT applications.
- VIRTUALIZATION LAYER is an abstraction layer[4]. It delivers virtual machines for Iot applications using the physical hardware resources.
- MANAGEMENT AND ORCHESTRATION LAYER is helpful for coordination of the IoT application and resources, along with lifecycle management of IoT applications.

Northbound Interface of the IoT Gateway:

The exchange of monitoring and information control are the function of the interface between IoT gateway and Application logic.It needs to be:

- Simple, to permit low complexity of IoT gateways
- Scalable, to withstand a large amount of end devices and IoT gateways.
- Fast, to maintain the latency between IoT gateways and application logic for better user experience with the system
- Flexible, to support different needs of IoT applications Adaptations

In this design, Representational state transfer (REST) or on the other hand Restful Web Services[11] is utilized as interface between the application and IoT entryway. The key favorable position of REST API in the engineering is there is no compelling reason to deal with any states in door.

The architecture's flow of is given as follows. Based on the sensor types, it takes the most recent incentive from sensor or effectively checks the present estimation of the sensor and send it to the application at whatever point mentioned. Depending on the received data, the command to the IoT gateway is send by application and in turns controls the actuators.

The interaction between the Iot application and gateway is shown in fig 2,the application will request for the value of sensor from the IoT gateway with ID 4108.the IoT gateway after collecting the value from the sensor it will respond the request by sending 200 OK. After receiving the value, the application decides to alter some actuators based on logic. If room temperature is high, the request will go to IoT gateway to reduce it and by modifying the temperature it will send 200 OK response.

Further future work of this concept is taken care by illustrating its applicability by two scenarios namely non-time-critical and time-critical[12].

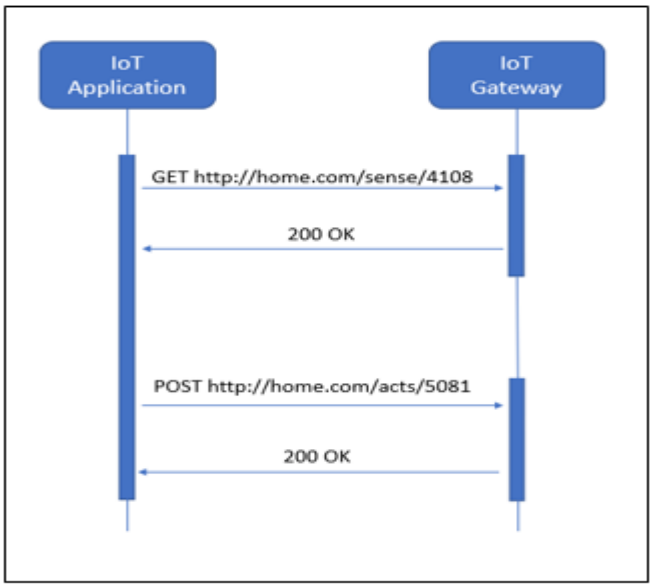

Fig 2. Interaction between Iot Gateway and Application.

IoT architecture based on Information Centric Networking (ICN)

Information-centric networking (ICN) is an approach to change the Internet structure away from a host-centric standard based on continuous connectivity and the end-to-end principle, to a network architecture in which the principal point is "named information".

The key features of Information-Centric Networking (ICN) are: (a) the recognizing the network units(contents, devices and services) by name as a substitute of their IP address. (b)a system to route which includes both names and addresses.(c) security of content etc. Such

doi: 10.32622/ijrat.76S201918

capabilities and functions help in the mobility support, scalability, multicasting and the caching of the contents[7].

IoT -ICN ARCHITECTURE

The unified IoT platform utilizing an ICN centric methodology is proposed as a middleware technology[13].In this engineering, ICN functionalities are run particularly from IoT administrations. This is useful in overseeing IoT information revelation and conveyance. The basic capacities to be upheld by the essential ICN foundation are: (a)device and system administration revelation, through an efficient substance distribute/buy in the board. (b)service dependent on naming, which recommends the capacity to give one of a kind characters, for example, name to the gadget assets, guaranteeing the diligence just as in presence of security issues and mobility[7]. (c) to condense content access latencies, techniques like context processing and storage caching are used.

The architecture includes five components:

- EMBEDDED SYSTEMS help in sensing and actuating the data and forwarding the data to the aggregator.
- AGGREGATOR, which has two important function: (a). To link the communication between the resource-constrained nodes which are part of network and the other aggregators. (b).In local network, aggregators help in integrating the sensing and actuating services.
- LOCAL SERVICE GATEWAY (LSG), helps in communication between local IoT system and global, managing the local name assignment and applying policies of data access for the local IoT devices.
- ICN-IOT SERVER, which take cares of lookup services and the subscriptions. As this server is involved in the regulate of the name and exchange of certificate between publishers and subscribers, it is not signified as a blockage for the content provision.

SERVICES/CONSUMERS, these are application interfaces which interacts with the ICN-IoT Server

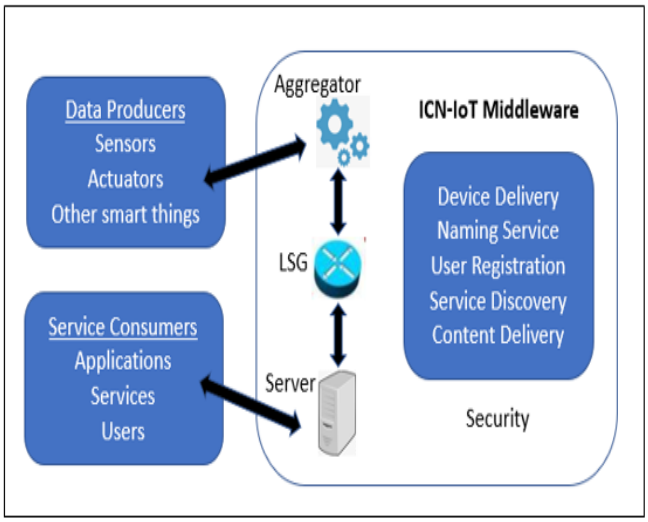

Fig 3. IOT -ICN Architecture

The main objective is the distributed network nodes should take care of the data discovery, processing and delivery by keeping it to close proximity. The aggregators and the LSGs ought to have self-design capacities and ready to convey local services, yet in addition scaling to expansive IoT services. The incorporation functionalities additionally have a noteworthy job in this. Fig. 3[7], demonstrates a pattern of the proposed ICN-IoT middleware, alongside its associations and capacities

V. COMPARISON OF DIFFERENT TECHNIQUES

The Different techniques are used to design a secure iot architecture to overcome challenges. Table 1,gives the comparison of techniques and their benefits

Table 1. Comparison between Related Work

Authors	Technology used	Benefits
Igor Miladinovic and Sigrid Schefer-Wenzl[4]	Network Function Virtualization (NFV)	Scalability, Maintainability, Security
Robert E. Hiromoto, Michael Haney, Aleksandar Vakanski[5]	machine learning (ML), cryptographic hardware monitoring (CHM), and distributed system coordination (DSC) techniques	Security, Reduce Vulnerabilities
Pradip Kumar Sharma, Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park[6]	SDN and blockchains technology	flexibility, efficiency, availability, security, and scalability
Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco and Alberto Coen-Porisini[7]	ICN(Information Centric Networking)	Privacy and security
S. Sridhar, S. Smys[8]	light weight Asymmetric cryptography	privacy and confidentiality

VI. CONCLUSION

The Internet of Things has become important part in our day to day life.it acquired domains like Retail, health, agriculture, industry etc. the widespread distribution is controlled by some limitation and challenges yet. The IoT architecture should be designed to withstand the challenges and to overcome the limitations. This can be done by using the modern technologies like NFV,ICN etc. As the future work, the blockchain technology and machine learning methods can be used to design the secure IoT architecture.

REFERENCES

[1] L. Prathibha and K. Fatima, "Exploring Security and Authentication Issues in Internet of Things," *2018 SecondInternational Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2018, pp. 673-678.

[2] M. S. Virat, B. S M, B. Aishwarya, D. B N and M. R. Kounte, "Security and Privacy Challenges in Internet of Things," *2018 2nd International Conference on Trends inElectronics and Informatics (ICOEI)*, Tirunelveli, 2018, pp.454-460.

[3] E. P. Yadav, E. A. Mittal and D. H. Yadav, "IoT: Challenges and Issues in Indian Perspective," *2018 3rdInternational Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Bhimtal, 2018, pp. 1-5.

doi: 10.32622/ijrat.76S201918

[4] Igor Miladinovic and Sigrid Schefer-Wenzl, "A Highly Scalable IoT Architecture through Network Function Virtualization," *Open Journal of Internet of Things (OJIOT)*, Volume 3, Issue 1, 2017

[5] R. E. Hiromoto, M. Haney and A. Vakanski, "A secure architecture for IoT with supply chain risk management," *20179th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Bucharest, 2017, pp. 431-435.

[6] P. K. Sharma, S. Singh, Y. Jeong and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," in *IEEE CommunicationsMagazine*, vol. 55, no. 9, pp. 78-85, Sept. 2017.

[7] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "A secure ICN-IoT architecture," *2017 IEEE InternationalConference on Communications Workshops (ICC Workshops)*,Paris, 2017, pp. 259-264.

[8] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," *2017 International Conference on InventiveSystems and Control (ICISC)*, Coimbatore, 2017, pp. 1-5.

[9] A. K. Sahu, S. Sharma, D. Puthal, A. Pandey and R. Shit, "Secure Authentication Protocol for IoT Architecture," *2017International Conference on Information Technology (ICIT)*,Bhubaneswar, 2017, pp. 220-224.

[10] E. R. Naru, H. Saini and M. Sharma, "A recent review on lightweight cryptography in IoT," *2017 InternationalConference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017, pp. 887-890.

[11] R. T. Fielding, "REST: Architectural Styles and the Design of Network-based Software Architectures,"*Doctoraldissertation, University of California, Irvine, 2000. [Online]*

.

doi: 10.32622/ijrat.76S201918