Analysis of Fog Computing for IOT Security

Manju Kumari, Lecturer
Govt. Polytechnic College, Bikaner
manjusunia08@gmail.com

Deepika Gupta, AP
Engineering College Bikaner
deepika.gupta1218@gmail.com

Naresh Mathur, AP
Sobhasaria Group of institutions, Sikar
nareshmathurer@gmail.com

Abstract
Distributed processing efficiency provided by fog computing, IoT needs an autonomic security approach. It is because IoT devices are deployed in both the managed and the unmanaged environments. The devices in unmanaged environment are more vulnerable to cyber-attacks. The new IoT produces large amounts of data from millions of connected devices which needs low latency analytics. Fog computing will fulfill this need. Fog nodes provide an abstraction layer that masks the heterogeneity between devices and offers a consistent, virtualization programmable interface.

Keywords: IOT, computation, cloud etc.

I. INTRODCUTION

The Internet of Things (IoT) is an arising worldview zeroing in on the between association of things or devices to one another and to the clients. Over the long haul, the vast majority of associations in IoT are moving from 'Human to Thing' to 'Thing to Thing'. This innovation is foreseen to turn into a fundamental achievement in the development of smart homes to bring accommodation and proficiency into our lives and our homes. In any case, by bringing this IoT innovation into our homes there will be significant ramifications for security in these advancements. Associating each keen articles inside the home to the internet and to one another results in new security and protection issues, e.g., classification, realness, and trustworthiness of information detected and traded by objects.

These advancements are a lot of powerless against various security attacks that make an IoT-based brilliant home unstable to live in and thusly it is important to assess the security dangers to pass judgment on the circumstance of the keen homes. For any innovation to be effective and accomplish inescapable use, it needs to acquire the trust of clients by giving adequate security and protection confirmation. As in all areas, keeping up security will be a basic test to survive. As homes are progressively modernized and loaded up with devices, potential PC security assaults and their effect on occupants should be explored.

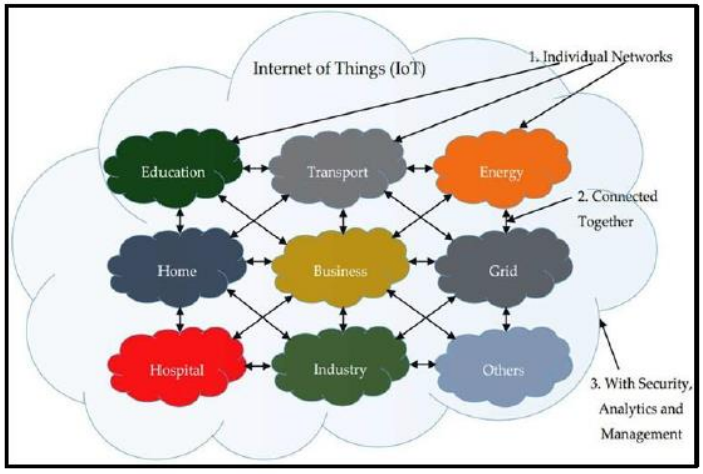

Fig 1. IoT can be seen as a Network of Networks

II. FOG COMPUTING

Fog Computing is a paradigm for shifting data and resources from the cloud to the edge of the network. The data collection, storage and resources are managed by distributed computing on the edge of network computers (Bonomi 2012). The new IoT produces large amounts of data from millions of connected devices which needs low latency analytics. Fog computing will fulfill this need. Fog nodes provide an abstraction layer that masks the heterogeneity between devices and offers a consistent, virtualization programmable interface. In order to manage services and resources among fog nodes, Fog Computing needs organization. Fog computing offers additional support for IoT devices, as well as reduced latency and lower bandwidth usage. Fog nodes can be tracked to inform IoT end user localization. It can be deployed globally to support wide scale IoT implementations with a high availability and scalability. Fog computing has IoT system mobility support protocols. It also deals with the problems of fragmentation of IoT by interoperability and stability of IoT applications.

The IoT fog-based framework architecture is deemed to have three components: end system, fog and cloud. The terminal interface level includes IoT sensing equipment from basic sensors to all types of devices connecting to the Internet. The primary objective of this level is to collect and fog data from its environment. In the systems of the network, such as access points, gateways, and routers, Fog Layer is built on distributed computing. The cloud level collects information from the fog nodes and manages data globally. It also offers final submission of data based on the IoT implementation requirement.

III. FOG COMPUTING FOR IOT SECURITY

Fog computing bridges the gap between cloud and end devices by allowing storage, distributed computation, communication and networking functionality nearer to the end devices in IoT environment. In addition to the advantages of reduced bandwidth consumption and latency, fog computing supports cyber security of IoT. Since fog nodes work in the cloud-to-things continuum, they provide additional security to IoT. The distributed multi-tiered architecture of fog computing supports IoT security in the following ways Fog computing enables better security by providing computation, storage and networking closer to end devices.

Computation: In fog computing, the computation and control are performed at the fog nodes closer to the end devices instead of remote data centers at the cloud. All the traffic to and from cloud to end devices need to pass through fog nodes. Hence the fog nodes can quickly detect and mitigate the attacks.

Storage: Similar to computation, data from the end devices can also be stored and retrieved from the distributed fog nodes closer to user premise supports high availability, security and privacy.

Networking: In fog computing, communication between the end devices can be performed nearer to the end user therefore, privacy is protected and chances of eavesdropping are highly reduced.

 Fog computing protects the resource constrained IoT devices which cannot execute complex security protocols and algorithms. The distributed multi-layered architecture of fog computing provides multiple levels of security to the end devices enabling defense in depth.

 Fog computing allows the storage of security credentials and software updates for the end devices.

 Fog computing enables a trusted security status monitoring by using its distributed architecture.

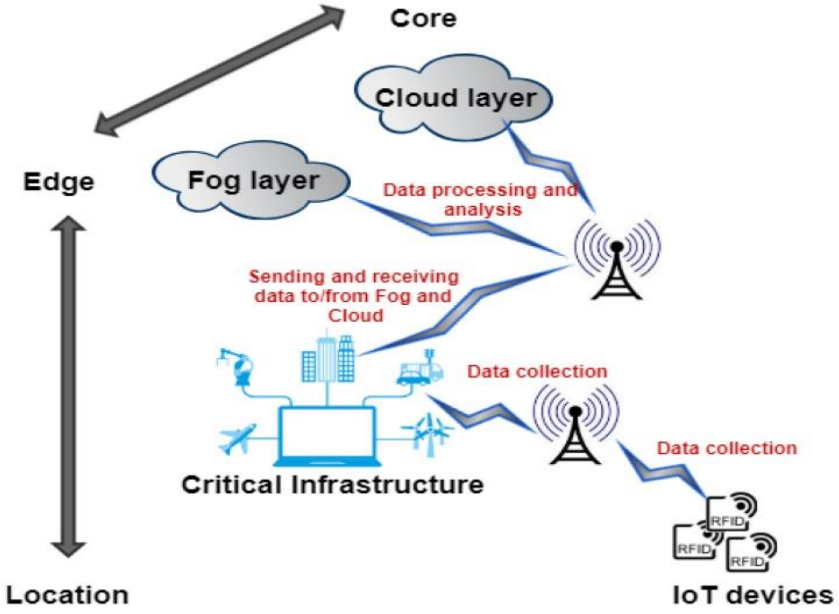

Fig 2: Fog computing for IOT

IV. CONCLUSION

IoT-based smart home unstable to live in and thusly it is important to assess the security dangers to pass judgment on the circumstance of the keen homes. For any innovation to be effective and accomplish inescapable use, it needs to acquire the trust of clients by giving adequate security and protection confirmation. As in all areas, keeping up security will be a basic test to survive. As homes are progressively modernized and loaded up with devices, potential PC security assaults and their effect on occupants should be explored. The self-protect functionality of autonomic computing can be adapted by security methodology in IoT to forecast, detect and defend cyber-attacks with less or no human intervention.

REFERENCE

[1]Yinghui Huang, Guanyu Li,"Descriptive Models for Internet of Things", International Conference on Intelligent Control and Information Processing, August, 2010 - Dalian, China.

[2] Daqiang Zhang, Laurence T. Yang, Hongyu Huang, "Searching in Internet of Things: Vision and Challenges", Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications, 2011.

[3] Yinghui Huang, Guanyu Li "A Semantic Analysis for Internet of Things" , International Conference on Intelligent Computation Technology and Automation , 2010.

[4] Lu Tan, Neng Wang, "Future Internet: The Internet of Things", 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) , 2010.

[5] Louis Coetzee, Johan Eksteen , "The Internet of Things – Promise for the Future? An Introduction ", IST-Africa 2011 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, ISBN: 978-1- 905824-24-3, 2011.

[6] Guicheng Shen, Bingwu Liu,"The visions, technologies, applications and security issues of Internet of Things", IEEE, 2011.

[7] Qian Zhu, Ruicong Wang, Qi Chen, Yan Liu and Weijun Qin*y, "*IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010 .