Machine to Machine Metamorphosis to the IOT

Pavan Manjunath [1], Dr. Pritam Gajkumar Shah [2]
[1]*Ph.D. Scholar in Computer Science, Jain University, Bangalore*
[2]*Ph.D. Department of Computer Science, Jain University, Bangalore*

***Abstract*— The Internet of Things (IoT) is going to be the next group of Internet revolution linking more and more devices on Internet network or encouraging domain for next-generation communication systems. The data transferred by the machines or set device over the internet should be safely secured, and the data should be transmitted only to the intended system, then delivering the data to any another users or devices. The Machine-To-Machines and Internet of Things (IoT) communications are used in the wide-areas of applications such as transportation, smart grids, interactive education, e-healthcare, home area networks, agriculture sector. This paper will focus the Machine-To-Machines and Internet of Things (IoT) and the subset of Industrial Internet of Things (IoT) ecosystem and also focuses on vulnerabilities and security prone issues, these paper will provide insight guidance and reference for future research works.**

***Keywords*— Machine-To-Machines; Internet of Things(IoT); Industrial Internet of Things (IIoT); IoT architectures; Vulnerabilities; Security**

I. INTRODUCTION

The Machine-to-devices communication is a form of data communication that includes one or more devices that do not certainly needs any human intervention in the process of communication [1]. The data which is transferred could be fixed wire or wireless [2]. The Machine-to-Machine (M2M) is widely used in the telecom industries [3] and also can be used to more proficiently monitor the situation of public infrastructures, such as water treatment facilities or bridges [4].

The Internet of Things refers to a collection of physical entities or set of object that each object is assigned IP address for internet connectivity, and the communication that happens between these entities or objects and other Internet-enabled devices and computer or mobile systems [5]. The Internet of Things (IoT) has delivered a gifted break to build controlling of industrial systems and the small set of devices multiple systems and applications and a larger set of Industrial Internet of Things (IoT) applications have been developed and deployed in recent days [6]. For example, the remote healthcare monitoring environment can assistance in the supervision of the expenses and easing the lack of healthcare personnel [7].

Industry Internet of Things (IIoT) can be categorized as a subcategory of the bigger Internet of Things (IoT). Internet of Things (IoT) includes Industry Internet of Things (IIoT) additional to it includes things such as hand watch, health device monitor, smart ovens or smart consumer products. Industry Internet of Things(IIoT) emphases specifically on larger industrial applications such as manufacturing industries or agriculture, and oil and gas, logistics, mining and metals, energy, aviation. For an example, of the Industry Internet of Things(IIoT) is predictive maintenance in the manufacturing industries, where it can be predictive before or the possibility, if the machine is getting broken, by such a predictive methods it can save millions of dollars in lost productivity[8].The manufacturing industries are undergoing a digital transformation. All types of set of machinery are being fixed with sensors, and intelligent controls to generate data from this machines and then send it over the Internet, and making the devices or machines much smarter it's the Industrial Internet of Things (IIoT). A massive quantity of useful data is confined with in the factory-floor machines. If captured, the data could be useful to advance the operations, reduce costs, and make for a safer workplace and data can be further analyzed using the Big Data analytics tools [9].

The difference between Machine-to-Machine(M2M) and Internet of Things(IoT), The Machine-to-Machine(M2M) is like one end point connecting to other end point or connecting 2 points, and the Internet of Things(IoT) is like a network, and consists of multiple systems and can trigger lots of interaction via a smart contract program[10].

The old traditional Machine-to-Machine (M2M) solutions were mostly designed to monitor few hundreds to thousands of remote assets, but in the case of the Internet of Things (IoT), it manages millions of billions of connected devices [11].

The Machine-to-Machine (M2M) usually addresses 'vertical' applications, developed as a single purpose 'silos', Internet of Things(IoT) is developing to a 'horizontal' model in which devices and applications share functionality and data and it can support multiple use cases, through a shared platform eco-system infrastructure[11].

The security and vulnerabilities risk related to Machine-to-Machine (M2M) applications are relatively partial, as only endpoints often communicate over point-to-point a virtual private network connections. With the enormous deployment of vulnerable Internet of Things (IoT) multiple devices and connected mobiles, the computer, and the increasing volumes of un-encrypted data exchanged over un-protected networks like the public network will attracts more hackers, and it's a big issues concern which needs to be resolved[11].

The Internet of Things(IoT) has got evaluation how telecoms do business the Comarch Internet of Things(IoT) connectivity Management formerly recognized as "Comarch Machine-to-Machine M2M" Platform, Comarch Internet of Things(IoT)

Connectivity Management facilitates the putting into practice of Internet of Things(IoT) service provider business strategies[12].

II. MACHINE-TO-MACHINE(M2M) ARCHITECTURE

The Machine-to-Machine (M2M) technology allow both wireless and wired systems to communicate with another set of devices. The Machine-to-Machine (M2M), does not use the IP address, as the Internet of Things (IoT) use the IP address to communicate between the devices and for collecting of data The Machine-to-Machine (M2M) allows point-to-point communication, most of the devices uses the wired networks or cellular and devices and does not depends on the on the Internet connection, there is very less options to integrated with the other application. It is based on the tight coupling between communication interfaces and applications; it also lacks open source Machine-to-Machine (M2M) development environment [13].

An Machine-to-Machine (M2M) solution usually consists of devices such as sensors and actuators The Gateway is used to handles the server communication and handles assets, these include wireless connectivity such as WiMAX and WiFi and wired, the Machine-to-Machine (M2M) acts as intermediate between end-user applications or enterprise applications as shown in the below figure 1[13].

III. INTERNET OF THINGS(IOT) ARCHITECTURE

A key blockage in using Internet of Things (IoT) devices for applications such as smart healthcare and smart cities is in scaling the architecture to thousands to millions of Internet of Things (IoT) devices. The applications normally use a subscribe architecture eco-system. A broker gathers data from the Internet of Things (IoT) devices or the publishers and transmits the data to the appropriate devices or subscribers, such as monitoring and notifying systems[14].

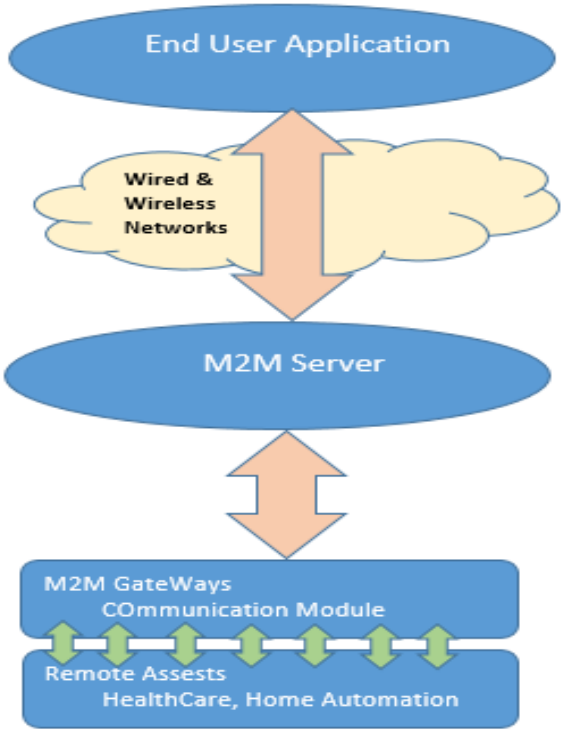

Figure 1: The block diagram of the integration of Machine-to-Machine (M2M) to end-user applications.

As shown in figure 2, the perception layer usually consists of wireless sensors and RFID and wearable device, the data is collected via sensors and transmitted over the network layer using Gateways and the data gathered is saved in the common storage area and it can be used for analysis or use by other application [15].

The Industry Internet of Things (IIoT) is the subpart of known as the Internet of Things (IoT). The Internet of Things (IoT) is a network of devices, sensors, and objects that gather and share huge amounts of data. The collected data is sent to a data ware house or central Cloud-based service where it is accumulated with other data, and then the data is shared with end users. The Internet of Things (IoT) will upsurge the automation in the education system, health care, in many industries [16].

The application of the Industry Internet of Things (IIoT) to the manufacturing industry is called the Industrial Internet or Industry (IIoT).The Industrial Internet or Industry (IIoT) will transform manufacturing by allowing the procurement and availability at greater speeds.

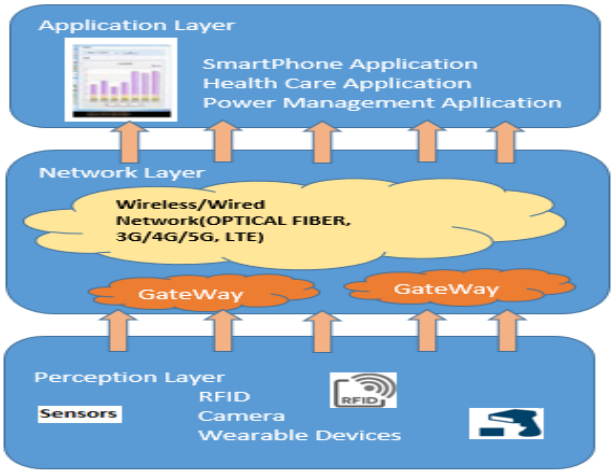

Figure 2: The block diagram of the integration of Machine-to-Machine (M2M) to end-user applications.

The Industry Internet of Things (IIoT) can greatly efficiency, connectivity, time savings, and cost savings for the organizations. [16]

Industry Internet of Things (IIoT) is connecting devices and machines, and moving their data to a data warehouse or in the cloud system, and then data is analyzed to predict and avoid downtime[17]. The Industry Internet of Things (IIoT) is a subpart of the Internet of Things(IoT) and industry, as shown in figure 3.

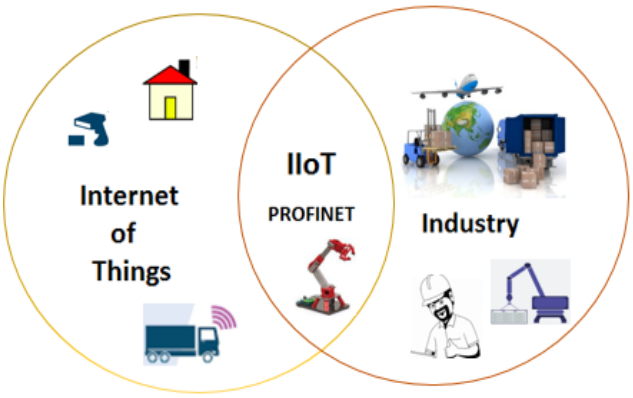

Figure 3: The diagram showcase the Industry Internet of Things(IIoT) is part of the Internet of Things(IoT)

IV. INTERNET OF THINGS(IoT) SECURITY AND VULNERABILITIES

As there is higher growth for the Internet of Things (IoT) and Industry Internet of Things (IIoT) in the up-coming years as industries grow and demand increase, the industries and governments organization will need to overcome the number of imperative issues. The first and foremost impact is data privacy and security, which are now increasing, and resulted in more increased vulnerabilities to attacks, data breaches driven by increased connectivity, espionage and data sharing [18].

Current developments and latest technologies upgradation, such as "Industrie 4.0" and Internet of Things (IoT), ensures that innovative business models and very good user experiences through solid connectivity and proper usage of the next generation of embedded systems. These systems produce, process, and interchange immense quantities of privacy-sensitive data, which invents them eye-catching targets of attacks. Cyberattacks on the Internet of Things (IoT) systems are very serious since they may effect physical destruction and even the lives threats to the human lives [19].

The considerable scales of latest DDoS attacks in 2016 October on DYN's servers that brought down many widespread online services in the United States, which gave the attackers can control up more than 150,000 unsecure Internet of Things (IoT) systems as malicious endpoints [20].

To resolve these security issues, there should be a proper security eco-system to safe-guard the Internet of Things (IoT) devices, let us take an example from the from existing Internet of Things (IoT) security eco-system build by the company Internet of Things (IoT)-Analytics and Internet of Things (IoT) Security company name called "Ardexa" to implementing of Internet of Things (IoT) double-check to build a very secure Internet of Things (IoT) eco-system [20].

In the Internet of Things (IoT) security architecture will focus on the four different layers, the first layer is Device, second layer is Communications, the third layer is Cloud, and the final layer is Lifecycle Management [20].

As shown in figure 5 the Internet of Things (IoT) security architecture and solution will focus on the four different layers, the first layer is Device, the secure device layer is termed as hardware level of the Internet of Things (IoT) solution that is physical things or the objects, some of the manufactures are introducing the chip security in the usage of "Trusted Platform Modules" that will acts as the trust by protecting the sensitive information and not to let loose of the encryption keys outside the chip and "secure booting" make sure that only verified software will run on the systems, the second layer is Communications layer denotes as connectivity networks layer of the Internet of Things (IoT) solution, in these layer data should be securely transmitted and received securely and in the communication layer the data should be safely encrypted and transferred to appropriate users and it should firewalls and intrusion prevention system, The third layer is Cloud, the secure cloud layers denotes the software backend of the Internet of Things (IoT) solution, the cloud system is treated as delivering secure and efficient cloud services by default, all the sensitive information should be stored in cloud with data must be encrypted and the digital certificates can play the key roles for authentications and identification and the final layer is Lifecycle Management layer, this layers indicates that there should be continuous processes of keep on upgrading of the security for the Internet of Things (IoT) and ensuring the security stages are in place from device manufactures and there should be active monitoring plays the vital role to keep track, detect and certain suspicions activity and also ensure the secure remote control is required when maintaining millions to billions of the Internet of Things (IoT) [20].

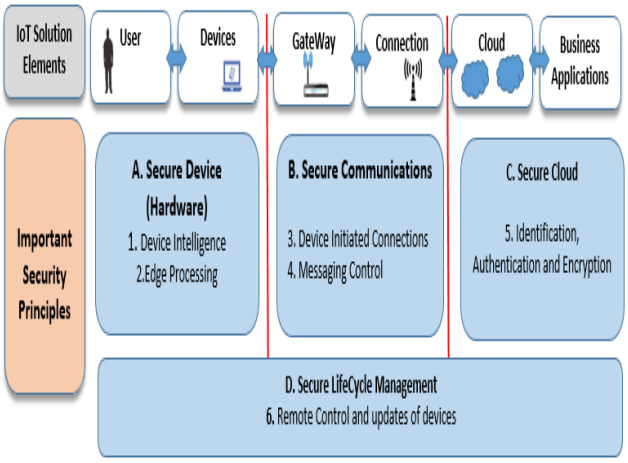

Figure 4: The four layer Internet of Things (IoT) security architecture

V. CONCLUSION

This paper has provided an inclusive overview of Machine-To-Devices, Internet of Things (IoT), and Industry Internet of Things (IIoT),and how most of the industries are leaning towards Internet of Things (IoT) from Machine-To-Machine (M2M) eco-systems and also focuses on the general over view of Machine-To-Machine(M2M) architecture communication system model, as well as the Internet of Things (IoT) architecture and Industrial Internet of Things (IoT) eco-system, and final how the Internet of Things (IoT) can be safely secured from the attackers, using an appropriate Internet of Things (IoT) security eco-system.

REFERENCES

[1] White Paper on “Machine-to-Machine Communication (M2M)”

[2] Telecom ABC-M,M2M

[3] WIPRO,Applying Thought,MACHINE TO MACHINE,The Technology of the Future

[4] HowStuffWorks/Tech/Computer/ComputerHardware/Networking,How Machine-to-Machine Communication Works,BY TIM CROSBY

[5] Main/TERMI,IoT-Internet of Things,By Forrest Stroud,

[6] L.D.Xu,W.HeandS.Li,"Internet of Things in Industries: A Survey," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243, Nov. 2014.doi: 10.1109/TII.2014.2300753

[7] J.Zheng,D.Simplot-Ryl,C.Bisdikian and H.T.Mouftah,"The internet of things [Guest Editorial],"in IEEE Communications Magazine, vol. 49, no. 11, pp. 30-31, November 2011

[8] The Industrial Internet of Things - What's the Difference Between IoT and IIoT?, Calum Mclelland,Dec 22, 2016

[9] HOME/TECH TOPICS/SMART TECHNOLOGY,How the Industrial Internet of Things Is Changing the Face of Manufacturing,

New networks could reduce maintenance costs and make workplaces safer,By KATHY PRETZ 23 February 2018,

[10] What is the difference between the "Internet of Things" (IoT) and "Machine to Machine" (M2M)?,Lucas Wang, Founder of HWTrek, platform that brings hardware to life (IoT/wearables/etc),Updated Dec 1, 2016

[11] The road from M2M to IoT is paved with big data,by Marc Jadoul,Feb 16 2017

[12] Comarch Telecommunications Solutions IoT Connectivity Management,IoT Connectivity Management,

[13] eclipse,HOME/ECLIPSE/WIKI/IoT/M2MIWG/M2MIWG/charter draft,IoT

[14] S.Sen and A.Balasubramanian,"A highly resilient and scalable broker architecture for IoT applications," 2018 10th International Conference on Communication Systems & Networks (COMSNETS),Bengaluru,India,2018,pp.336341.doi:10.1109/COMSNETS.2018.8328216

[15] AUGMENTED REALITY SERVICES IMPLEMENTED WITHIN SMART CITIES, BASED ON AN INTERNET OF THINGS INFRASTRUCTURE,CONCEPTS AND CHALLENGES:AN OVERVIEWArticle (PDF Available)·March 2018

[16] The Industrial Internet of Things (IIoT)

[17] 7 STEPS TO IIOT,Posted February 21st, 2017 by Carl Henning & filed under IIoT.

[18] Industrial Internet of Things:Unleashing the Potential of Connected Products and Services,January 2015,

[19] A.R.Sadeghi, C. Wachsmann and M. Waidner,"Security and privacy challenges in industrial Internet of Things," 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2015, pp. 1-6.doi: 10.1145/2744769.2747942.

[20] Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers,November 29,2016, Padraig Scully