ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.5

A Real Time Framework for Monitoring IoT Devices and Overview of Security Challenges

Sreenidhi B.K[1], Shwetha .S Shetty [2]
Assistant Professor[1, 2]
Department of ISE
RNSIT Bengalore, India[1]
MIT Mysore, India[2]

Abstract:
The Internet of Things (IoT) is a trending topic in technology industry, policy and engineering science. A real time framework is very much important for monitoring and diagnosing IoT enabled devices. Any unsecured device that is connected online potentially affects security and the resilience of an internet globally. IoT security is a key for secure development and secure scalable. IoT applications, real time services which connects the real and virtual world between people, objects and system.

Keywords: IoT Working Framework, Considerations, Security Challenges, Security Suggestions

I. INTRODUCTION

IoT- Internet of Things is one of the emerging concepts of socio-technical life. Everyday activities like consumer products purchasing, cars, goods, industrial components, sensors are being merged with internet connectivity. Strong data analytic capabilities that assure to transform the way public works live and play is associated. Meanwhile IoT raises strategic challenges that could stand in the way of realizing potential core benefits. Now a day's public attention towards the hacking of Internet-connected devices, surveillance concerns and privacy fears are major issues dealing with internet. Even though new technical challenges remain and strong policy, legal enforcement and development challenges are emerging. Today large scale daily activities are depending on implementation of IoT devices ensuring many aspects for life [1]. "Smart home" a very good example for internet enabled appliances is an example of IoT environment includes home automation components and energy management devices to strike a smart life. At a reasonable cost, IoT technology can be implemented as advent to beneficial for people with disabilities and elders, offering high level of independence and standard life style. IoT enabled benefits like networked vehicles, sensors embedded in highways and bridges moves closer to smart cities concept. Which intern helps to minimize congestion, energy consumptions, even IoT is deployed in agriculture filed industry to transform the older methods to technically sound modern profitable setups. However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized.

II. DESIGN REQUIREMENTS

Following requirements are identified for an framework that can perform on-line monitoring and Processing of IoT based events in real time.

- **Event Processing:** Device specific events generated by IoT devices have to be processed by this framework and all the events should be effectively managed for better results.
- **Fast Ingestion:** Multitasking system, for a given time the framework should be able to manage huge amount of events and to process them in any conditions.
- **Real-Time Processing:** Online and human led adhoc analysis should be supported in any cause of attacks, as current trends is based on internet handling a real time activities are much important.
- **Visualization:** Graphical display having aggregated and summarized data for human analysis of real -time monitoring is aided for easy analysis and decision making.
- **Flexibility:** All types of event inputs must be supported, so the heterogeneous nature of IoT ecosystem must be easily supported without any issues in between the operation.
- **Ease of Deployment**: Deploying the activities of user into cloud should be easily processed without much headache, required resources, platforms and infrastructure should be automatically supported by the framework.
- **Scalability:** The number of event per second processed by the framework would likely increase with the time,so the framework should be horizontally scalable.
- **Privacy**: Major concern is the security and privacy, that data being reported by the devices is handled very confidentially.

III. DESIGN FRAMEWORK

To address the necessities, the framework is shown in Figure 1. Next we portray the part of every one of the segments of the design [2], and in addition the product items and advances that we imagine could be utilized for every segment.

Devices and sensors: Devices and sensors transfer the events so that others can catch information, usually events are stimulated by the proprietary APIs or by Message Queue Telemetry Transport and connections between gateways and IoT devices are established for event communication.

External sources: It is an optional component, in which system can also collects the events from social media posts and internet based security communities. For example temperature is automatically collected from social networking sites, from this information device would modulate the temperature required for activity.

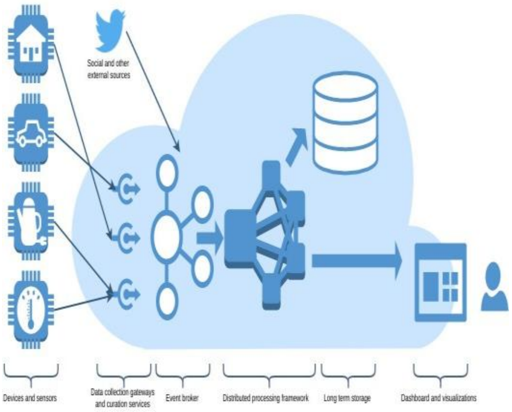

Social and other external sources
Devices and sensors
Data collection gateways and curation services
Event broker
Distributed processing framework
Long term storage
Dashboard and visualizations

Figure .1.Design Framework

Data collection gateways and curation services: The event produced by the IoT gadgets should be cultured and sent to the event agent layer. As such, this layer is comparable to the Extraction layer in conventional Concentrate, the data collections gateway and curation service layer includes gateway with functions (e.g., by using the Apache NiFi or by the Apache Metron probes)

Event broker: Event broker's acts as distributed system with a message queue to publish subscribe interface, an higher volume of events at a very high speed can be ingested. Apache kafka is the best for this layer, because of its ability to manage events with high velocity.

Distributed processing framework: It can be used to query days from event broker to execute capabilities such as apache storm used to query data from event broker, framework can execute continuous analysis process to find attack with some anomalous nature.

Long term storage: For an long term storage strategies like hadoop distributed file system (HDFS) where some data or all the data must be stored.

Dashboard and visualizations: Web based interface provides needful visualization and active information. This can be built by Microsoft's powerBI or Tableau or by any open source.

IV. IoT SECURITY CHALLENGE

Main principle includes ensuring the resilience, security, reliability and internet applications stability [3][4] . Being an internet user obvious to expect high degree of the trust that internet and its applications, associated devices linked to it are very much secure enough to do all kinds of activities we want to do online based in relation to risk tolerance associated with those set of activities. The internet of Things is the same in this regard and security in IoT is generally connected to the ability of users to put stock in their condition. On the off chance that individuals don't trust their associated gadgets and their data are sensibly secure from abuse or mischief, the subsequent disintegration of trust makes reluctance to use the Internet. Indeed, ensuring the security in IoT devices and services must be considered as top priority for the sector. Potential security vulnerabilities grows as in a daily life with increasingly connecting devices to internet. Cyber attacks are most common in poorly designed devices which expose user's data to theft by leaving the information streams inadequately secure. Cyber attacks allows malicious authorities to re- program a devices to cause malfunction, due to this can create security vulnerabilities. IoT devices manufacturing faces challenges in competitive cost and technical constraint for an adequate design.

$$\text{Cyber security Risk}=\frac{\textit{Threat level} \cdot \textit{probality of attack} \cdot \textit{points of exposure}}{\textit{cybersecurity measures implemente}}$$

Major difference between the internet of things to traditional internet method is that the number of possible threats are increasing due to the following reasons[6].

➢ **More points of exposure**: With an increasing number of connected devices, systems, applications, end users subjected to more points of exposure

➢ **probability of attacks** : IoT devices themselves becomes new attack vectors

➢ **Increased impact of attacks:** With more connected devices in many applications (i.e., number of different use cases in which are all built on different standard frameworks, interacting with different systems and have different goals), specific to critical infrastructure applications where there is an increased impact of attacks (i.e., physical world damage can be possible loss of life), which increases the threat level.

➢ **New threats from across the stack**: A complex technology stack means new threats are likely to be across the stack, which must be counteracted by cyber security by an experienced security professionals.

Increase in number and nature of associated IoT devices could increase the chances of attack. When it coupled with an highly interconnected nature of IoT devices, then every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally, not just locally. For instance, an unsecured television or washing machine that is infected with a malware can send harmful spam emails to worldwide recipients using device owner internet connection. As technology growing it is bit difficult to buy an devices that are not internet connected. Day by day we are depending on IoT devices for basic essential services and we expect those devices to be more secure. With an increasingly depend on these devices for essential services . security of IoT devices and services is a major point of discussion , should be treated as an critical issue.

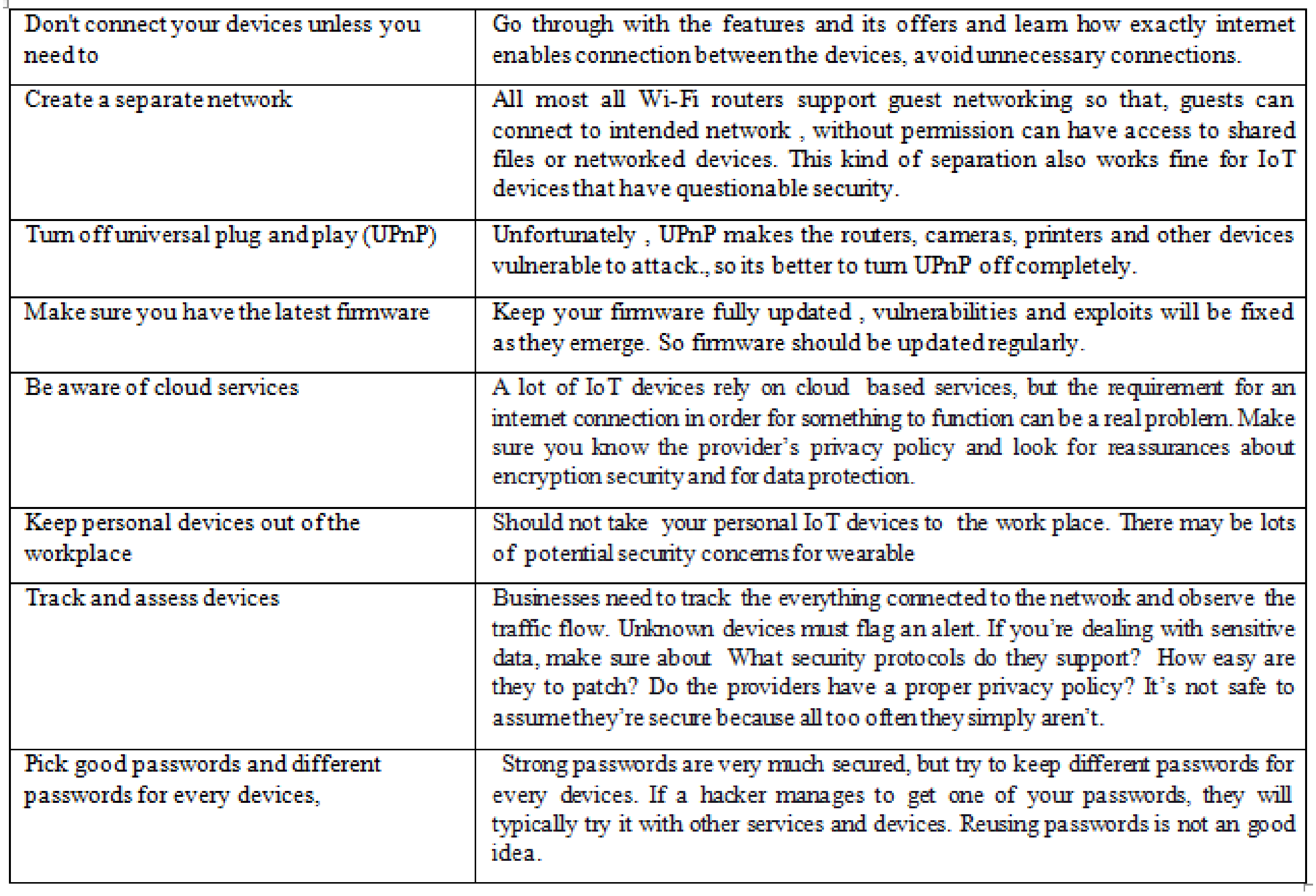
V. SPECTRUM OF SECURITY CONSIDERATIONS

When thinking about Internet of Things devices, comprehend that security of these devices isn't outright. IoT gadget security isn't a paired recommendation of secure or shaky. Rather, it is helpful to conceptualize IoT security as a spectrum of device vulnerability. The range ranges from absolutely unprotected gadgets with no security highlights to exceedingly secure frameworks with various layers of security highlights [5]. The general security and strength of the internet of Things is a component of how security dangers are evaluated and overseen. Security of a device is an element of the hazard that a gadget will be traded off, the harm such bargain will cause and the time and assets required to accomplish a specific level of assurance. On the off chance that a client can't endure a high level of security hazard as on account of the administrator of an activity control framework or individual with an embedded, Internet enabled medicinal gadget. As an issue of guideline, designers of brilliant objects for the internet of Things have a commitment in guaranteeing that those devices don't uncover either their own clients or others to potential mischief .As an issue of business and economics, vendors have an intention to reducing their cost, complexity and market time. For an instance, IoT devices associated with larger volume, mid margin components that already represent a cost added to that of the product in which they are embedded are becoming quite common adding more memory and a faster processor to implement security measures could easily make that product commercially uncompetitive.

VI. UNIQUE SECURITY CHALLENGES OF IOT DEVICES AND SUGGESTIONS

IoT devices like, sensors, consumer item are made to be at an massive scale so orders of magnitude beyond that of the old internet connected devices. So, potential quantity of links between these gadgets is unprecedented. In a dynamic fashion, many of the devices can establish link of communication with others unpredictably. So the existing methods, tools mechanism associated with IoT security needs an new considerations. Many IoT deployments will consist of collections of identical or near identical devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics. For example, a communication protocol vulnerability of one company's brand of Internet-enabled light bulbs might extend to every make and model of device that uses that same protocol or which shares key design or manufacturing characteristics. Deploying IoT consists of group of similar or nearest devices. By this homogeneity associates the potential impact of any individual security vulnerability from the sheer number of devices that all have same characteristics in nature. Many Internet of Things devices will be deployed with an anticipated service life many years longer than is typically associated with high-tech equipment. It's difficult to reconfigure or update them. Further, these devices might be deployed in circumstances that make it difficult or impossible to reconfigure or upgrade them, these devices might outlive the company that created them, leaving orphaned devices with no means of long-term support. These scenarios illustrate that security mechanisms that are adequate at deployment might not be adequate for the full lifespan of the device as security threats evolve. As such, this may create vulnerabilities that could persist for a long time. This is in contrast to the paradigm of traditional computer systems that are normally upgraded with operating system software updates throughout the life of the computer to address security threats. The long-term support and management of IoT devices is a significant security challenge. Operation of IoT devices are not visible or user may don't know the internal operation of the devices creating an security problem when an user thinks that IoT device is performing a certain function. In reality it may perform unwanted operations or may be collecting more data than it has to be intended. device functions could change without knowledge when an new update is launched, so users are subjected to any changes that manufacturer makes to the devices. Sometimes physical security is impossible to achieve , but still deploying an IoT devices will be at risk. Attackers can easily get direct physical access to installed IoT devices. To ensure an security, antitamper features should be enforced and design innovations has to be updated to meet the security . Early models of Internet of Things feels IoT will be an product of large private or public technology enterprises, but in the future "Build Your own Internet of Things" (BYIoT) might become more commonplace as exemplified by the growing Arduino and Raspberry Pi [3]developer communities. These may or may not apply industry best practice security standards. As more and more Internet enabled devices increses find their way into our smart homes and businesses field, it's very important to remember that they represent an security risk. The Internet of Things (IoT) is growing rapidly and in the rush for convenience [7], our privacy and safety is often an afterthought. Leaving them with an unsecured is the digitally equivalent to leaving the back door unlocked. here are some possible suggestion listed in the table 1.

Table.1. Security Suggestion



Don't connect your devices unless you need to	Go through with the features and its offers and learn how exactly internet enables connection between the devices, avoid unnecessary connections.
Create a separate network	All most all Wi-Fi routers support guest networking so that, guests can connect to intended network , without permission can have access to shared files or networked devices. This kind of separation also works fine for IoT devices that have questionable security.
Turn off universal plug and play (UPnP)	Unfortunately , UPnP makes the routers, cameras, printers and other devices vulnerable to attack., so its better to turn UPnP off completely.
Make sure you have the latest firmware	Keep your firmware fully updated , vulnerabilities and exploits will be fixed as they emerge. So firmware should be updated regularly.
Be aware of cloud services	A lot of IoT devices rely on cloud based services, but the requirement for an internet connection in order for something to function can be a real problem. Make sure you know the provider's privacy policy and look for reassurances about encryption security and for data protection.
Keep personal devices out of the workplace	Should not take your personal IoT devices to the work place. There may be lots of potential security concerns for wearable
Track and assess devices	Businesses need to track the everything connected to the network and observe the traffic flow. Unknown devices must flag an alert. If you're dealing with sensitive data, make sure about What security protocols do they support? How easy are they to patch? Do the providers have a proper privacy policy? It's not safe to assume they're secure because all too often they simply aren't.
Pick good passwords and different passwords for every devices,	Strong passwords are very much secured, but try to keep different passwords for every devices. If a hacker manages to get one of your passwords, they will typically try it with other services and devices. Reusing passwords is not an good idea.

VII. CONCLUSION

Thus hereby we conclude that the design framework which is analyzed in this paper is efficient against security challenges that iot devices facing . key IoT issue areas are examined to explore some of the most pressing challenges. IoT devices tend to differ from traditional computers and computing devices in important ways that challenge security

VIII. REFERENCES

[1]. M Bashir And A.Gill , "Towards An Iot Bigdata Analytics Framework: Smartbuilding Systems, ", 2016, Ieee International Conference.

[2]. RafaelI.Bonilla and CristinaL.Abad “Towards real time framework for monitoring IoT devices for attack detection ", 2017 IEEE.

[3]. Karen Rose, Scott Eldridge, Lyman Chapin, " The Internet of Things: An Overview ", 2015, the Internet Society (ISOC).

[4]. J Pescatoreand G Shpantzer, “securing the internet of things survey", SANS institute, 2014.

[5]. K.Zhao and Ge, “a survey on the internet of things security", international conference on computational intelligence and security 2013.

[6].https://dzone.com/articles/5-things-to-know-about-iot-security

[7].https://www.csoonline.com/article/3085607/internet-of-things/8-tips-to-secure-those-iot-devices.html