ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 8, Issue 4, April 2018 Impact Factor 5.132 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

# DEVELOPING SOLUTIONS FOR CHALLENGES AND DESIGNING DEVICES FOR THE INTERNET OF THINGS

**Nutan Sharma[1], Dr. Kalpana Midha[2]**
**Department of Computer Science**
**[1,2]OPJS University, Churu (Rajasthan) – India**

**ABSTRACT**

With the development of technology in modern science, the world has become smaller and easier to us. Today, internet is being used not only on personal computers but also on various smart devices. Smart devices can be considered as interactive electronic devices where they connect with other smart devices through a network to share and interact remotely. Internet of Thing is this kind of invention of modern science which is a computing technology provides anetwork of things and people where human and devices with sensor can communicate each other to perform many different tasks of our day to day life.This paper provides an overview of the Internet of Things (IoT)and its architecture emphasis on well-known problems of IoTandits possible solutions.This paper encountered the discussion of IoT architecture problems and many other challenges including the new malware attack, also proposing some solutions ofscalability, latency, bandwidth, malware attack including RFID and NFC problem. This part will present current and future solutions to the challenges within IoT, and current and future recommendations for securing IoT frameworks. As the solutions are dependent on the accessible resources, a few themes will include different solutions in light of the constraints.

## 1. INTRODUCTION

IoT, along with cloud computing, is a major contributor to the fourth industrial revolution and is inevitably becoming a part of our lives. More and more industries have gradually applied the IoT technology, and an increasing number of enterprises are attempting to gain a footing in the future IoT world.The challenge with IoT is that many enterprises only focus on IoT development without evaluating or learning primary challenges that they are facing. Many of these enterprises do not even have any background in the IT industry or software development but most of them are committed to providing Internet-connected devices. Even enterprises that have software and hardware design experience often mistake IoT as other traditional computing technologies and make terrible mistakes when developing IoT devices.

Again and again, facts prove that this practice is a disaster and will turn out to be a failure, ruin manufacturers' efforts, and ultimately damage the integrity of IoT.This article will put forward four challenges that all manufacturers and developers should consider when they decide to go into the IoT industry.

## 2. SECURITY CONSTRAINTS IN IOT

### 2.1 Authorization

Many less difficult back-end frameworks in the Internet of Things will ordinarily utilize a unique client enter in the header of a demand to authorize a gadget to communicate with the back-end. This will require an enemy to take a few to get back some composure of the way to get to the gadget, and if an encrypted connection is required to communicate, will be a suitable solution. In the event that this solution is to be used, the key is required to be transferred to the gadget, either after the encrypted connection is set up, or during production. Items that can handle a standard HTTP TLS connection will ordinarily utilize this to communicate with the back-end and transfer the key. In spite of the fact that if the item is fit for communicating along these lines, we are more like an essential networked PC, and should utilize consistent account login to the back-end using a mobile application, and receiving a gadget particular get to token identified with the client account.

Authorization ought to in a perfect world be on gadget level, and identified with a client as a different esteem, as we ought to have the capacity to prohibit lost devices without excluding the client account, and grant different permissions to different devices that a similar client owns. As the unique esteem particularly defines a gadget, it doesn't need to be changed during the life of an item, and can be included during production. Be that as it may, as it needs to be identified with the client somehow, a framework for association still needs to be implemented, and will typically is a piece of the key distribution handle.

### 2.2 Authentication

Using authenticated encryption, any changes made by an enemy in transit would be detected as the MAC would not coordinate. For a foe to have the capacity to manipulate data, they would need to have the right key used to generate the MAC. Famous authentication calculations include MD4, SHA-1, SHA-2 and SHA-3/Keccak. An ongoing competition called Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) is currently running to give new authenticated encryption calculations.

## 3. REDUCE BANDWIDTH OVERHEAD

To lessen the bandwidth needed, one wants to transmit data only when needed and keep the parcel little, while as yet keeping the need for retransmissions to the minimum. A few protocols are designed particularly on account of this objective, yet their utilization is often restricted to a particular utilize case, and no one general solution exists.

### 3.1 Mesh Networks

Within mesh networks, we want to course data rapidly to the recipient node(s) while keeping trace to a minimum. A few different strategies for transmission in a mesh network are recommended in the examination community, however some proposed solutions will only work for particular sorts of mesh networks. Securing the networked devices within a mesh network can be handled with varying level of overhead. To secure all connections within a crush network, one ought to in a perfect world secure the immediate link between every gadget, except again this will be dependent on what mesh technology is utilized.

Intrusion detection is an integral piece of each mesh network. The capacity to prohibit individual nodes in a network ought to be conceivable within a reasonable amount of time. In a mesh network, intrusion through a fringe gateway between the nearby mesh and the external Internet ought to be detected on the gateway, while intrusion into the neighborhood mesh ought to in a perfect world be detected by the mesh nodes themselves. This is not generally conceivable, as an enemy can get hold of the keys to the network, and masquerade as a new trusted node connected to the network. In these cases, excluding nodes in the network ought to be conceivable when the rupture is found through an alerting or monitoring framework.

Monitoring the condition of the nodes as to their integrity will generate additional parcels in the network. Yet, as devices ordinarily transmit additional data, for example, battery state and network express, this does not increase the heap on the network significantly. One will often utilize a pulse to identify whether devices are as yet alive and/or present in the network. In these cases, one would need to utilize the central monitoring administration to identify abnormalities in the network. If all devices are controlled by one entity (for the most part the case in industrial or explore settings), inclusion of new devices can be manually controlled. This is not an adaptable solution for the eventual fate of the Internet of things as the number of devices can rapidly achieve an unmanageable amount.

### 3.2 Optimized Protocols

Using the web stack (TCP/IP HTTP REST APIs) is still exceptionally common in IoT, either between the entire frameworks, or as a piece of it (center communicating with a back-end server). Using this common method of communication gives more "elements" and less demanding interoperability than the specific protocols; however in the meantime they require more resources, and has an immense overhead.

A few protocols have been proposed to take care of the bandwidth overhead issue in IoT frameworks. In recent years we have seen the emergence of protocols, for example, Bluetooth LE (Smart), IPv6LoWPAN, MQTT, CoAP, DDS, AMQP, STOMP, and many more. These protocols endeavor to keep bundle sizes to the absolute minimum, while as yet providing solid communication. This is accomplished by removing any header and payload that is not entirely needed for communication in IoT. When the attention is entirely on reducing the parcel estimate, security mechanisms are not generally a need. Along these lines, one ought to assess whether the hypothetical reduction in bandwidth translates to quantifiable abatement in bundle estimate when security is added to the protocol. MQ Telemetry Transport (MQTT) is a protocol that uses the endorser distributer technique for transmitting data. All data is sent from a gadget to a message broker point-to-point, where the broker broadcasts this message to all devices that subscribes to the predetermined theme. By utilizing this technique, in principle, the only required elements of the bundle is the subject, message sort and message (QoS level, Duplication Flag and Retain fields are included for included unwavering quality). With the strict concentrate on reducing bundles, there is positively no emphasis on security in the MQTT protocol.

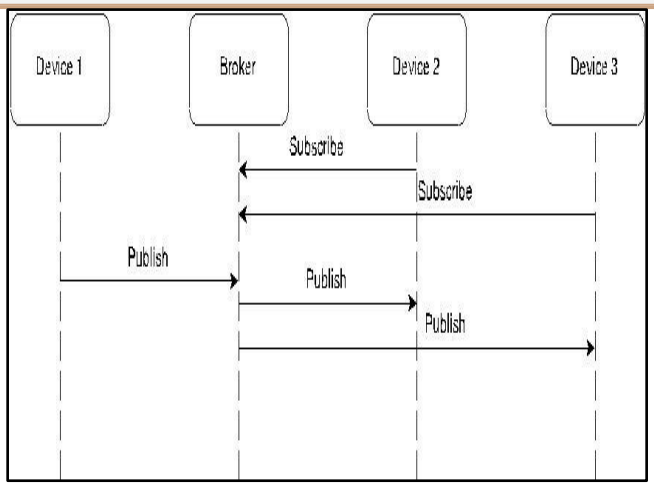


**Figure 1: Illustration of the publisher / subscriber method used by MQTT toreduce bandwidth overhead**

A newer protocol that considers both parcel overhead and security is CoAP. It utilizes User Datagram Protocol (UDP) on the transport layer to diminish the overhead made by Transmission Control Protocol (TCP). Even however it is conceivable to run CoAP with no type of security, it was designed with the intention of using DTLS to secure the connection [ZSB14]. This would bring down the obstruction for developers to utilize secure connections by facilitating for the utilization of DTLS within the conveyed software. In actuality, this has shown not to be the situation. In a plugtest report from 2013, it is acknowledged that there were excessively couple of implementations that help DTLS, making it impossible to get any significant data from tests. Even however the standard encourages security from the earliest starting point, it is the genuine implementations that in the end should include secure communication techniques. The implementations that exist have shown that more than 1/3 of the bundle will be taken up by DTLS, in this way reducing the accessible space in every parcel significantly [Juc12] [HB12].

## 4. ROBOTIZED CRACKING INSTRUMENTS

### 4.1 Application Layer Encryption

There is an unmistakable correlation between the main processing force and how data encryption is handled in devices. When the main processor has low processing capacities, the gadget will probably either utilize hardware-quickened encryption given by the microcontroller, or implement no encryption by any stretch of the imagination. This is often the case with low-control devices that should run disconnected from the electrical network for a long time. A case of this is the Fitbit wellbeing monitor analyzed before which utilize an ARM Cortex-M3 with quickened 128 piece AES.

Many devices that are not constrained by processing limit or power requirements will use any encryption technique that fits the gadget or administration in question as they are not required to utilize any implicit encryption to conserve resources. These devices are often smarter devices and may even use an

undeniable operating framework, where developers can choose what security ought to be implemented without being (strongly) managed by the chip specification.

**4.2 Public Key Infrastructure**

Increased utilization of Public Key Infrastructure will take into account better control of devices within a network. On the off chance that a gadget is traded off, one can invalidate the certificate of the gadget from the network in a mechanized or manual fashion effortlessly. The plausibility of introducing PKI into the Internet of Things is an intensely talked about theme, and while not generally in utilize today; it is considered a feasible solution for the Internet of Things.

The main issue with implementing PKC in the Internet of Things is that the constrained devices would utilize excessively resources to approve the key of another gadget, contrasted with using a pre-shared key. Using ECC in PKI will bring down the processing requirements and in this manner the power requirements while providing more noteworthy cryptographic strength contrasted with RSA. With the cost reduction of the main cryptographic operations of ECC (scalar point multiplication) in the later years, the validation procedure is becoming negligible contrasted with the security gains by using PKC. To gain additional control of a PKI, one can utilize online validation using the wireless network and central CA, rather than preloading the CA's certificate on all devices.

**4.3 Post-Production Management**

Including authentication will enable the gadget to dismiss any changed firmware with potential indirect accesses. Many more seasoned items will commonly include a USB port through which new firmware can be added to the gadget (TVs, speakers, set-top boxes, and so forth.), requiring express human interaction to initiate the refresh. For this situation, the refresh is downloaded using a desktop PC with every cryptographic function required to ensure the refresh is the right one.

Newer items tend to initiate refreshes over the wireless network. For this situation the refresh is either initiated by the client, or initiated naturally from the developers. Client initiated updates will normally include using a mobile phone to initiate the download, or pressing a button on a UI. Frameworks using the mobile phone as an initiator will often utilize the phone to authenticate, authorize and download the new refresh before transferring the refresh to the gadget over the nearby network. Even however it is certain that there is some type of authorization and authentication, it is pointless if the gadget is utilized as a part of a common and/or open network setting.

Devices that initiate refreshes specifically on the gadget ought to authorize and authenticate the report on the gadget itself Devices like TVs may have an account on the manufacturers benefit, and enable TLS connections to the refresh server. This is obviously limited to the more able devices. Using the LWM2M protocol mentioned is a decent candidate yet requires moderately resource-intensive and ideally utilize UDP and CoAP at the moment. In the event that the gadget can bolster SSL/TLS, many off the rack protocols can be utilized. On the off chance that the gadget is extremely constrained, connecting the

gadget to a PC using a dongle, or connecting physical storage medium to the gadget will be secure alternatives.

**4.4 Privacy**

Protection is a difficult subject within IoT. On one hand, we want to have the capacity to recognize all devices uniquely; however in the meantime; the client of the gadget often does not wish to be recognized. Wireless networks, for example, Wi-Fi or Bluetooth utilize unique identifiers (addresses) for each network interface, which is communicated in each transmission to or from the gadget. These unique identifiers was shown in the analysis of the EyeFi card, where the network interface broadcasts a MAC address with every bundle, in the Fitbit where the gadget address was unique could track a person's movement, and in the HomeEasy framework where the ID of the transmitter is communicated with each signal.

When one wants to send data particularly to one collector, this identifier is utilized as a deliver for the beneficiary to have the capacity to identify the sender and the other way around. In broadcasts guided at anyone who wants to listen, be that as it may, these addresses are not generally needed and excluding or randomizing these can give security to the client. This component is as of now incorporated into the Bluetooth LE standard when broadcasting advertisement outlines (in spite of the fact that not commonly implemented), and are utilized by a few vendors for Wi-Fi tests (e.g. Apple's iPhone).

Where this element does not forbid the utilization of the item, it ought to be implemented. In any case, in many circumstances, the uniqueness of the gadget ID is the general purpose of the gadget. A case of this is Bluetooth "sack/key/remote-trackers". The likelihood of randomizing the deliver to maintain a strategic distance from security concerns is not plausibility, as uniquely tracking the gadget is the selling highlight of a Bluetooth tracker.

**4.5 Focus on Security across All Products and Services**

The truth of security considerations is that individuals tend to make the wrong assumptions, and does not see all the potential harm that can be made. In the event that you where to ask a person what is more important to secure; their front entryway, light, TV, stereo or Wi-Fi, individuals are in general fear someone getting in through their front entryway.

As a designer of new IoT items one will then concentrate on securing what oneself see as the most important. Looking at existing solutions for securing the front entryway of homes, for example, the August Smart Lock [Aug] and the KwiksetKevo [Kwi], there is an unmistakable concentrate on how secure the items are on their website pages. Obviously bolts are inherently a security-gadget, so it is not surprising that their attention is on security. Be that as it may, in general, an entryway bolt won't give much security when a home has glaring indirect accesses, for example, exacting secondary passages, or glass windows. This is the reason safes has been utilized all through centuries to secure profitable things. On the other hand, security center in IoT devices in the house is nearly non-existent; even however they often contain get to tokens or credentials to client's accounts.

Even however this is an unreasonably self-assured illustration; it indicates why security considerations are hard. Even however an engineer does not consider the gadget "important" enough to secure, this won't be the situation in actuality. And even however one development group has chosen that the framework truly needs no security mechanisms, future additions to the item may make new requirements that one cannot anticipate in the main version of the item. Security should along these lines dependably be considered a necessity, even however it doesn't appear to be necessary from current requirements.

### 4.6 Data Storage

When designing an IoT gadget for the future, one ought to consider the likelihood of physically losing a gadget. Securing the devices 100 % will never be sensible. Therefore the amount of data put away locally on the gadget ought to be considered in relation to the importance of the data remaining hidden from a foe. Data put away on every gadget ought to preferably be the absolute minimum that is needed. Unless the data is entirely required for neighborhood analysis, or is not yet shared somewhere else, there is no need to have it put away on the gadget. As the Internet of Things is storing personal data from consumers, security is, and will be, a reasonable concentration amongst consumers. Reducing the amount of nearby data ought to be organized, contrasted with somewhat reducing the energy efficency of the gadget. When nearby computing is performed on a gadget, crude data ought not be kept after the data has been analyzed.

Encryption on privately put away data can be utilized, i.e. securing the key in an encryption chip, at the end of the day; the key should be put away on the gadget, and along these lines only includes some resistance for enemies that needs to remove the way to unscramble the data.

### 4.7 Increased Computational Speed

We can only expect that the speed of processors and microcontrollers will increase in the coming years, in any event in relation to control consumption. This will make it conceivable to implement stronger cryptographic calculations, without increasing force consumption. The exceptional constraints existing in the Internet of Things means that computational power will be significantly lower than that of desktop PCs for years to come. Yet, as long as strong cryptographic calculations are utilized, this computational hole will be minuscule contrasted with the computational power difference between brute forcing an encryption calculation, and encrypting data using the encryption calculation.

### 4.8 Interoperability

The standards bunches have until now made a larger number of issues than real solutions the interoperability issue. The nearest we have gone to an interoperable standard is administrations like IFTTT (IF This Then That) and Twitter, which is bolstered by most devices available, in spite of the fact that with varying level of ease of use. There are some exclusive corporate solutions, for example, Apple's HomeKit and HealthKit that tries to motivate vendors to help a common standard for control and storage of data. Their HomeKit1 solution presently can't seem to be launched, and substantial players in

wellbeing monitoring solutions, for example, Fitbit, has freely announced [Fit14] that they won't bolster the HealthKit standard. This issue is unfortunately a question of economics and competition more than technology as an arrangement of common security protocols is definitely a probability, and has just been made in the different consortiums. Hence, the genuine solution to this issue lays beyond the extension this theory, despite the fact that it will affect the eventual fate of security in IoT frameworks in a major manner.

## 5. CONCLUSION

Many challenges exist in the process of developing IoT products. This article lists some major challenges. If these challenges do not get properly considered, you may walk into a deep channel without a torch. Under this circumstance, you may have to feel your way forward with hands and pray that you will not step into any trap. In fact, challenges encountered in IoT development may be even more complicated and comprehensive. If you find other challenges for IoT development, you are welcome to share your ideas with us. While these are some of the major challenges that appear while IoT application development, it is imperative for development companies to adapt and adopt technological advancements to drive IoT developments. Having said this, it is essential for a developer to be aware of the challenges and get ready to work on them to successfully establish themselves in the market.

## REFERENCES

[1]. T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, et al. (2012) – ", RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks". Available: https://tools.ietf.org/html/rfc6550

[2]. L. Anhtuan, J. Loo, A. Lasebae, A. Vinel, C. Yue, and M. Chai,(2013) - "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks," Sensors Journal, IEEE, vol. 13, pp. 3685-3692, 2013.

[3]. B. Wu, J. Chen, J. Wu, and M. Cardei, (2007) - "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless Network Security, Y. Xiao, X. S. Shen, and D.-Z. Du, Eds., ed: Springer Science, pp. 110 -132.

[4]. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer,(2005) - "An Authenticated Routing Protocol for Secure Ad Hoc Networks," IEEE Journal on Selected Areas in Communication, special issue on Wireless Ad hoc Networks, vol. 23, pp. 598-610, March.

[5]. T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson,(2014) - "A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)," .

[6]. A. Dvir, T. Holczer, and L. Buttyan, (2011) - "VeRA-version number and rank authentication in rpl," in Mobile Adhoc and Sensor Systems (MASS), IEEE 8th International Conference on, 2011, pp. 709-714.

[7]. K. Weekly and K. Pister,(2012) - "Evaluating sinkhole defense techniques in RPL networks," in Network Protocols (ICNP), 2012 20th IEEE International Conference on, pp. 1-6.

[8]. J. P. Wang, S. Bin, Y. Yu, and X. X. Niu (2013) - "Distributed Trust Management Mechanism for the Internet of Things," Applied Mechanics and Materials, vol. 347-350, pp. 2463-2467, Aug.