International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 02, 2020
ISSN: 1475-7192

# Cyber security Threat Mitigation in Architectures for Industrial IOT

[1]Triveni Mishra, [2]Dr.SaikatGochhait

***ABSTRACT--****The industrial IOT applications are rapidly growing and transforming the traditional industries to smart industries (Industry 4.0) along with the impending consumer IOT adoption. It is therefore necessary to adapt and deploy a reliable cyber security software architecture. Due to the immense security challenges in IIOT, this paper tries to approach the concerns from an end-to-end IIOT solution security perspective. In this paper we discuss the currentarchitectural framework and study how they can address the challenges like scalability, integration problem, data privacy and security and how the framework improves the security in the IIOT environment and reduce cost. With respect to the aspect of cost, we highlight the factors and specific costs in developing an IOT application. This paper also explains the security requirements, practices and types of attacks on the IOT architecture. Here, we highlight the critical problems (threats/attacks/vulnerabilities) and their detection, prevention and mitigation techniques.The authors aim is to prepare a study of existing protocols, frameworks and architectures currently proposed in active research based onvarious parameters as also to review the existing technology and project requirements in IIOT to understand both technology and stakeholder impactover IIOT security.*

***keywords****—Attacks, Cryptography, Industry 4.0, IOT Security, Threats, Vulnerabilities*

## I. INTRODUCTION

The concept of Internet of Things is characterized by diverse technologies that play an important role in innovation across various application domains. Traditionally, the internet was a product where all the data was generated by the people and for the people. Now this internet of people has been transformed into Internet-of-Things (IoT) which connects devices to existing network. It is a platform in which various devices, sensors or machines blend seamlessly to share data generated by them. This interconnection among the devices and people through the network can be called as smart environment. IoT has stepped out of its infant stage with consumers witnessing demand-driven market for IoT devices; most importantly even governments and businesses are understanding the role that IoT plays in ubiquitous connectivity due to its inborn management, monitoring and analytics capabilities.

Manuscript received June 08, 2020; revised July XX, 20XX. This work was

*[1] student of MBA(DTM) at the Symbiosis Institute of Digital and Telecom Management (SIDTM), Lavale, Pune (e-mail: triveni.mishra1921@sidtm.edu.in)*

*[2] Post Doctoral Fellow from University of Extremadura, Spain and a Sr. Assistant Professor at the Symbiosis Insttute of Digital and Telecom Management, Lavale, Pune (e-mail: saikat.gochhait@sidtm.edu.in*

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

Created under the approval of the Academic Integrity Committee of the Symbiosis International University, Lavale, Pune.

It has been seen that by the mid- 1990s, embedded hardware technology was being enhanced by Web servers.High value monitoring of inventory, warning systems, fleet mana-gement and other industrial applications have already been integrated by M2M applications.

Commercial and consumer scenarios in the emerging market are there for which deployment is not simplified, since all vertical systems are divergent, rendering the communications layers inconsistent. Largely horizontal interconnection in API integration is less, achieving less cross-application inter-connection (Chase, J, 2013). This vision of IoT has not been realized fully in a short span of time.As of now, technology protocols and data structures are constrained by their complexity in design as well as security, extensibility, etc.Security is an absolute necessity with the amount of data sent inside the IoT and it is essential to maintain their usability even with significant growth spurt in connected device numbers (Chase, J, 2013).

In this scenario, the security and privacy of the devices, communication channeland the network play a fundamental role in addressing the requirements like data confidentiality, privacy, authentication, console & network access etc. Hence it is important to review the existing architectural framework and study how they can address the challenges like scalability, integration problem, data privacy and security and how the framework improves the security in the IIOT environment and reduce cost. (Khalid, Butt., Jamal & Gochhait,2020).

## II. OT APPLICATIONS

### *A. Smart Homes*

Device Components: Mobile-based Android apps, AI-based voice assistant, Bluetooth module, Arduino-driven controller

Functional Description: For the ordinary user, this helps in the control of electrical home appliances with dedicated modules in the kitchen, washing area, lighting/conditioning and security and so on. An android app on a smart phone can be used to activate either an AI/ NLP based voice assistant which can issue commands to the Arduino controller over Bluetooth to perform simple tasks like switching appliances on/off or toggling other settings.

Usage Scenario: It can be managed by the user's mobile phone, where the Arduino controller's GSM module can even communicate in reply to text messages from the user with the electricity units and total cost consumed by the appliances, thus helping regulate usage. Disabled users like the blind can use AI assistants or the disabled can use the AR-interface.

### *B. Smart Cities & Civic Amenities:*

Device Components: Waste-container sensor, Web/Mobile app-based/Sensor-actuated notification, Gateway/controller for optimization and operational analytics, Waste department truck with app deployed on driver's Smartphone.

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

FunctionalDescription: IoT-driven smart city solutions can be used to manage waste collection either by monitoring waste rates or by offering operational analytics to optimize routes. Each waste container has a sensor which collects the waste state data in that container.If it's below a certain threshold; the waste management system receives a level sensor input, processes it, and sends a notification to the mobile device of a truck driver. The the truck driver empties a complete bin, without allowing any half-full ones.

Usage Scenario: Waste collection operates emptying containers according to fixed operational cycle. This is not an efficient approach since it may lead to the unproductively of waste containers and excessive fuel consumption by trucks used to collect waste.

### *C. Smart Grid & Metering:*

Device Components: A network of smart meters, cost-effective telecom network connectivity, municipal corporation office network-based controller, utilities in company or home IT system.

Functional Description:

Smart connected meters allow data to be transmitted directly over a telecom network to a public utility, delivering accurate meter readings to it. Smart metering allows utility companies to chargeaccurate amounts for each household's water, energy and gas consumption.

Usage Scenario:

A smart meter network helps businesses to gain more insight and see how their consumers are using energy and water.They cantrack demand in real time and redirect resources when required or persuade customers in times of scarcity to use less energy or water.

### *D. Smart Mobility and Transport:*

Device Components: Movement sensors, CCTV Cameras in city metro-rail stations, gateway for loading capacity usage computations, Screens to relay passenger instructions.

FunctionalDescription:By integrating data from ticket sales, movement sensors, and CCTV cameras mounted alongside the track,rail operators can predict the loading of passenger cars on their journeys to and from locations.By analyzing this data, they can predict how each car will fill up with passengers, whereby rail operators encourage passengers to spread along the train to maximize / minimize loading as per fuel cost. The train operators reduce train delays or improve fuel efficiency by optimizing fuel utilization.

UsageScenario:IoT sensor data may help to uncover trends about how people use transportation. This data can be used by public transport operators to improve travel experience, achieve a higher level of performance, health, and punctuality for both the passenger and the service

### *E. Smart Traffic Management System:*

Device Components: Traffic cameras, Network Gateway, City Wide Monitoring System

Functional Description: Traffic cameras connect to a common data gateway which relays information to a city-wide system for managing traffic of the Municipal Corporation.

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

Usage Scenario: Probable traffic congestion due to road repair is reported to the City Municipal Corporation Monitoring System which then predicts peak traffic load and provides alternate movement routes. These can be suggested over the channels like apps on smart devices or over the radio, etc.

### *F. Healthcare, Pharmaceuticals and Life Sciences:*

Device Components: Object- Sensors, Radio frequency antennae, Monitoring Devices

Functional Description:IOT based systems are being used to facilitate asset tracking in hospitals and medical facilities. It is an inexpensive method of monitoring daily activities in a hospital as also unobtrusive and effective.

Usage Scenario: The protection of every hospital or medical facility is the utmost concern. To ensure the full amount of safety the ability to monitor assets inside the building is essential — staff members, patients, and equipment.The scope and size of the situation is much higher in larger facilities that contain numerous buildings, campuses, patients and st aff members, and is not as feasible as in smaller systems.

### *G. Retail& Logistics*

Device Components: RFID tags, mobile-based apps, AI text-assistant, robotic arms as actuators.

Functional Description: Warehouse automation and robotics powered by the shopping patterns online and in-storehave become necessities in the 21st century. RFID is a well-optimized and highly usable part of IoT that can be used to monitor inventories and optimize service costs.

Scenario: IoT allows realtime monitoring of revenue opportunities and tracking missed instore orders, stream lining supply and demand planning. A typical warehouse or distribution center is organized by aisles and shelves based on a fixed blueprint.IOT technology built for this environment requires high mobility and low scalability, but the requirement for the latter is likely to be the opposite in future, the difference being that they will be self-organizing structures (i.e. of varying dimensions).

### *H. Environmental Monitoring*

Device Components: Sensor network (WSN-based), Central cloud analytics engine as controller, display monitor on smart phone or device for environment ministry/departmental officials.

Functional Description: A network of sensors is placed along busy traffic intersections and placement is near plants. These sensors then gather data on the amount of polluting gases such as Sulphur oxide and dioxide, Carbon dioxide and monoxide, methane and so on while the centralized cloud-based platform analyses and visualizes sensor-based monitoring levels.

Usage Scenario:Air quality monitoring is a significant environmental concern. Such a program tracks air quality over ci ty spots so that platform users can display the air quality map and use the data to point out places where air pollut ion is severe and formulate citizen recommendations.

### *I. Smart Manufacturing*

Device Components: A complex sub-system of the manufacturing environment that would include IoT devices, people, applications and mobile apps.

Functional Description: The entire production system will itself have a digital twin as also every sub-system and

individualcomponent.All the smaller twins and all their inputs and outputs must be integrated into the automated twin.Advantagesof this such as operational gains, predictive maintenance and improved product design are allpos sible only with a digital composite twin used to give a higher level of visibility.

Usage Scenario: A composite digital twin can help in building an accurate picture of a business-based use case to highlight process functionality, design flaw, security loophole or an interface concern that is otherwise harder to grasp in a production

environment.Four distinct types of digital twin have been identified overall from a single component to a wh ole business process and are increasingly being used in manufacturing or production industries.(Gochhait, Shou, &Fazalbhoy, 2020).

## III. ARCHITECTURAL MODELS, PROTOCOLS AND THE CISCO-IOT REFERENCE MODEL

IOT architectures have generally begun with the three-layer architecture model or definition of IOT made up of the application, network (access and core) and the perception layer. Such an architecture can have a four-layer secure architecture to support it as defined. (Ahmed, Ali & Ibrahim, Nagwa.,2017). In extension of this, another 4-layer base IOT architecture has been proposed by (Ahmed, Ali & Ibrahim, Nagwa.,2017) with the Data Perception layer, Heterogeneous Network Access layer, Data Management Layer and Intelligent Service Layer. Each layer has its own security requirements, a combination of 5-7 strategies as illustrated therein. There are a number of factors that influence the security management needs within the IOT architectures. It is essential to support the security and privacy in IOT as it is one of the design goals for 'ideal' IOT architectures itself. Amongst the most significant are:

### *A. Impact of heterogeneity to IOT security*

Interoperability is built in feature of IOT as it commits to the underlying concept of IOT or IOE as the internet of 'everything'. This has led to a myriad variety of protocols and wireless communication technologies over which the IIOT functions today. Some of these include the MQTT, AMQP and CoAP communication protocols and the wireless technologies of IEEE 802.11n wi-fi, Bluetooth, Industrial Zigbee and 5G. (Parotkin, Nikolay & Zolotarev, Vyacheslav. , 2018)

### *B. Addressing issues and how they create problems in IOT security*

The adoption and implementation of IOT technologies with IPv6 and 6LowPAN are setting up unique authentication and security requirements essentially stemming from the number of Internet-connected devices now surpassing the earth's human population.

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

### *C. The complexity of IOT architecture due to convergence of technology*

Hybrid, integrated architectures for IOT have been proposed in order to overcome inherent IOT concerns of simplifying the information acquisition, information analysis, decision making, and action implementation process(Ahmed, Ali & Ibrahim, Nagwa.,2017). Also, this integration will provide visibility of the network resources and management of access based on user, group, device, and application that eventually enables the ability to exchange data between users and devices. These include the SDN-based IOT architecture, context-aware MVNO (Mobile Virtual Network Operators) architecture and the Cloud- and Fog- computing based architectures. (Ahmed, Ali & Ibrahim, Nagwa.,2017)

In 2014, Cisco proposed a 7-layer IOT Reference Model to elaborate upon the existing need and functional requirements that need to be supported by IOT and predicted the exponential growth in IOT devices by 2020 (Cisco, 2014) In this paper, we have attempted to map the Cisco Model to Security Requirements, across layers, keeping existing Security Requirements in mind, while also adding some of our own. A complete summary of our findings is present in the section "ATTACKS IN IOT TECHNOLOGY AND COUNTERSTRATEGIES AS PER SECTOR" below.

## IV. FACTORS IMPACTING THE COST OF AN IOT APPLICATION

There are numerous factors that can affect the cost of developing an IoT application. It begins with the target audience and the kind of products or services that need to be delivered; further what type of hardware that is to be used to target along with the features and the functionalities that they offer.(Dev Technosys, 2018, May 22)

All these resources cost money; plus, the time invested in designing the application is also an add-on to the cost, any development time and number of hours spent on the project by a developer decides the cost of development.(Dev Technosys, 2018, May 22)

Complexity of the project plays a decisive part in determining the cost. The application with basic functionality, features and standard UI requires little customization and time for development.However, the complex IoT application may require access to large databases, vendor integration & realtimesyncing with technologies like social media, geo location ,multi-device synchronization, multi-user access,multi-platform interoperability, code length, scope creep and so on.

In the Post-Production stage of the application there is a maintenance cost associated with it. The application needs to be up and running all the time. It also needs to be updated with relevant features and bug fixes.

### *A. Techniques for Cost Estimation in an IOT Project*

Broadly there are two approaches for reaching the total IOT project cost. Cost estimation involves the estimation of resources required for development and implementation of a project across its different stages. It is a process of calculation that needs to take into account the project's scope, timeline, budget and resources.

These approaches are the:

1. ***Analogous estimates*** are a technique that use past project cost estimates to determine the cost of a current similar project. An example of this estimation technique is in the application of Monte Carlo Simulation Modelling Techniques that estimates the complete life cycle cost while keeping the quantitative project risk and external factors into consideration to model the costs incurred over time.

2. ***Parametric estimates***is a more accurate for estimating cost as compared to the analogous technique. It is more accurate hence better applied in case of integrated system such as industrial or enterprise IOT.A parametric estimate is determined by identifying the number of units required for the project(Ivan Valeryevich Evdokimov *et al* 2019) followed by the unit cost. The measurement must be scalable in order to be accurate as the system's scalability ensures that the parametric modelling is valid even at higher number of units. Techniques involved in this are the Constructive Cost Model (COCOMO), The Use Case Points Method (UCP) based on the use of UML; and the Three-point estimation technique, which is a PERT (Program Evaluation and Review Technique) modification to remove uncertainties in assessment. Equation (1) gives the Three-point estimation formula where O, M and p represent 3 cost points and E is the estimate derived from them

$$E= (O+4M+P)/6 \quad (1)$$

*B. Steps of Cost Estimation using QFD- based Design by cost*

1. ***Determining the Cost structure***

As we know, cost of production from the basic accounting principles or approach can be a combination of direct costs and/or indirect costs (overheads). The material cost and labour cost are direct costs. We can say that in an IOT project, the material cost can vary as per the quality of material procured and the area where the manufacturing is set-up and the difficulty or ease of acquiring the product (where in the supply chain the product is procured- manufactured or vendor-procured). Indirect costs include the Variable and fixed factory overheads which are calculated. For a custom or limited manufacturing set-up, the fixed cost is a constant ratio of the sum of material cost, labour cost and the variable manufacturing cost. The variable factory overheads are determined from the indirect materials (including power consumed) and the indirect labour costs.

*2.*Design ***by Cost (CE by QFD)***

The basic features of the QFD technique include the QFD Matrix which is created at the design stage. The design solution is translated into cost estimation QFD by creating a comparison matrix with 2 dimensions. The correlation values are entered into each cell of this matrix for the correlation between the functional attribute and the customer needs it satisfies. A similar correlation matrix can be created for the Business Drivers and the functional attributes that corresponds to it. In each case there are weights assigned to each Customer Need (w) or Business Driver (w`) as the case is. The mathematical relationship between the functional weight and the matrix values for an IOT product with 10 customer needs and 10 Business Drivers can be given as (Refer 2):

$$W(F1) = \Sigma 10i=1 \ (wirij+w'ir'ij) \quad (2)$$

Here, w and r are the weight of Customer Need and the correlation with function respectively and w' and r' for the Business Driver and functional attribute(s) respectively.

*3. **A Technical Comparison of Features***

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

Competitive products can be compared to the product being prepared and its features assigned to it. Functions characteristics can be rated on a scale of 10, from level 1 to level 10 (excellent). Hence a cumulative function score can be recorded as the equation (Refer 3):

$$Fj= W(Fj.Lj) \quad (3)$$

*4.* ***Consolidatinginto a single approach***

Fj is determined and the cost factor helps in estimation of system cost. Let us see how the cost factor (kj) can be estimated. In an IOT system with m competitive products and n function attributes, Cost of competitive products- (mu(c), Var(c)) is obtained via system cost analysis. Here we consider the cost of competitive products to be a distribution with Gaussian properties. Function attribute score (Fj) is as F11, F12, F13…and so on. In matrix form (Refer4):

$$[F][muk]=[mu(c)] \quad (4)$$

Subsequently, mu(k) can be calculated by least square method under m>=n condition as (using matrix transpose) (Refer 5):

$$[muk]=[[F]T.[F]]-1. [F]T[mu(c)] \quad (5)$$

The variance of cost factors can be similarly calculated (Tsai, Chang, 2004).

*C. Project Commencement and Continuity Criteria*

Despite the existence of such methods, the cost cannot be accurately calculated; there is always an uncertainty factor involved. To reduce this project uncertainty of overrun or financial risk, the following criteria need to be adhered for the project:

***RequirementsAnalysis***

Defining project requirements and check whether all of them are high in feasibility and appropriateness especially from functional aspects(Tsai, Chang, 2004). It is advisable to anticipate pessimistic scenarios of total cost when defining the project requirements as it is impossible to formally cut-out any possible scenario of overrun. Each project phase has a different requirement and accordingly a different budget strategy allocated to it.

**TABLE-I:** BUDGETARY ALLOCATION FOR AN ICT PROJECT

| Percentage Ratio (%) | Stage | Description |
|---|---|---|
| 20 | Specification | Project Requirements |
| 25 | Design | Development and Verification |
| 20 | Development | Code Writing and Execution |
| 35 | Integration & Testing | Combination of elements and testing in multiple ways. |

| | | |
|---|---|---|
| | Maintenance | --Customer's expense-- |

In the context of IOT, the requirements at the design stage include:

- Database provisioning
- Network provisioning
- Connectivity Provisioning (LPWAN, LTE etc.)
- Device (Sensor, actuator, controller) provisioning
- Security Provisioning (User authentication, firewalls, location confidentiality, device authorization)

At development stage, which is mostly covered by software development requirements, the total LOC, the different modules, the integration of modules and the unit, integrated and other testing methods and the cost of human and computing resources come into play. At each level of requirements, the costing of every individual supplier/ manufacturer considered effects the total project cost. These requirements have been identified in research previously as under, where the Budgetary allocation based on the cost estimate and requirement analysis can be as in Table-I(Tsai, Chang, 2004).

***Specification of appropriate tasks***

The customer always needs to know the task plan to correctly allocate expenditures. At this stage the importanttasks are separated from the conditional ones and exclusions made in order to reduce costs harmlessly for the project. Restrictions to the project must be declared and agreed in writing. Any later additions can shoot up costs in the project.

***Detailed project documentation***

Documentation costs often escape the costing requirements due to inefficient project management and hence it needs to be considered.

***Requisite qualifications for skilled workers***

As a rule, to obtain an objective estimate and forecast the associated expenses it is necessary to consider a situation where initially the employees' skill levels are lower than those required while a minimum level of accomplishment to execute tasks and maintain quality is required.

***Project prototypes***

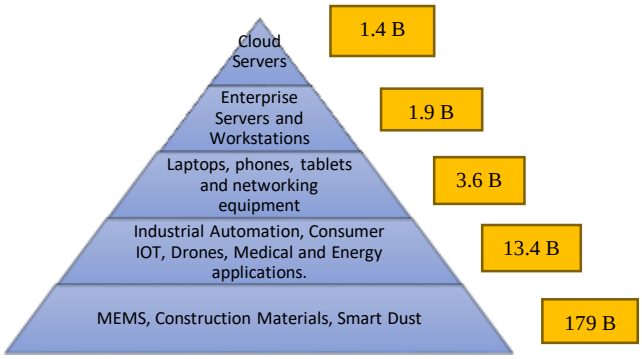
In an iterative project lifecycle this gives the stakeholders an opportunity to visualize project development live by prototypes which require some amount of end-user functional testing prior to go-live.

***Appropriate choice of technology***

The chosen approach to a solution is a key reason for cost overruns. To minimize financial risk in the above, additional costs for learning new technologies, included in total cost are often made.

*D.Layers in IOT and 'Security-to-Cost' trade-offs in an IOT Application*

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 




Source: springer.com

**Figure 1**: The Estimated Number of IOT Devices, by layer.

Overheads from security functionality for layer 1– 3systems is usually estimated to be 10-15percent of total system cost, which is a low overhead because these systems are generally capable of supportin g a common collection of security features, algorithms, or operations.However, in cases where theedge layerexists in constrained environments, computing power remains limited. (Cheruvu S., Kumar A., Smith N., Wheeler D.M.,2020) Highly constrained environments are found in healthcare applications where the device size could range from layer-3 to layer-5. To add to this, smart city applications in mobility, environment and waste management also demand solutions to the lower end of the physical scale as the surface area/unit is less. Removal of unused functionalityof the embedded systemof an application for fitting into constraints sometimes results in the preservation of security functionality vis-à-vis the non-security functionality. This leads to the question of the viability of profits in such environments, profits which are not always as a result ofapplication functionality alone. Often these trade-off decisions lead to counter-productive justification for weaker security in the devices and architectures.

In the Cost of Cybercrime report, a study published by Accenture Security in 2018, the annual average of cybercrime cost had increased by approximately 2 million $ in a year and there was a recorded 11% increase in the number of security breaches over the same period. The highest average cost/sector had been recorded in the Banking and Financial Services industry, which is one of the most risk-ridden sectors towards cybercrime. To further develop a case for Cyber-security in industrial IOT in the age of smart cities, the frequency and cost of incidence of cybercrime, in the national capital of India, Delhi, have been highlighted below. It is observable that the graphical trends show an overall average increase from 2016 to 2018 annually in case of boththe metrics.

With respect to the costs incurred due to cybercrime, they can be internal or external. The internal costs depend on the actual activity cycle occurring internally, i.e. the D-2-R cycle (Discovery, Investigation, Containment, Recovery). These cost mechanisms depend on the regulatory framework and the strategic importance of security as a priority in the organization. The external cost is the cost of damage incurred due to the incident itself which is much harder to determine the impact of due to factors like non-discern ability and/or incorrect estimation of the extent of information loss (information is an asset to the enterprise), business disruption (failures and stoppages can extend theTAT's), equipment damage (software assets are a cost to company), and resulting revenue loss.(Bissel, La Salle, Dal Chin., 2018).

# V. SECURITY REQUIREMENTS IN IOT TECHNOLOGY

Here we will demonstrate which security precept is affected by the vulnerabilities and challenges that exist in the IOT space today. As it is known, vulnerabilities can existin any layer/device level which can act as an attack vector/ surface- it can be the device, its software, network or the data under threat, whether in IOT based consumer devices or as a part of industrial large-scale IOT applications. These vulnerabilities are important to study as while they may not be intended as part of the manufacturer's standard protocols and designs, these inherent weaknesses do creep into the system as a result of the trade-offs mentioned (in previous section).

### *A. Data Confidentiality*

When dealing with data confidentiality two important aspects needs to be considered i.e. Access control & authorization mechanism of which vulnerabilities and challenges include Eavesdropping and Authentication & identity management mechanism of which the vulnerabilities and challenges include Impersonation and Identity Spoofing. Encryption Schemes of encrypting the data are useful to mitigate them. It is necessary to protect both the device/network and the user's data as well.So, the technology-to-cost impact ratio is high.

### *B. Physical Security*

The attacker can target the physical characteristics of the IoT device to partially or totally destroy/alter it, aiming to send error ridden messages to the network.V&C include physical tampering and device manipulation/destruction/alteration for transmitting erroneous messages or totally skipping packets. Technology-to-cost impact ratio is low; it may not be a high-priority unless the IOT system is placed in a remarkably red-area or zone of potential harm or lack-of-safety. As such minimal security measures are necessarily at place at enterprise level, but protective measures are needed as IOT transforms to a highly open and public asset base.

### *C. Privacy*

Data sharing and collection as well as management is a sensitive subject with respect to privacy.V&C include Data tampering for unauthorized purposes.

### *D. Authentication*

An unauthorized third party can easily access corresponding IoT services and devices if the authentication function for users is absent, mis-configured or weakly controlled.Authentication involves identification and authentication of devices or users or sources of information so that data is verified as being generated from a trusted source when devices are interacting with each other.

### *E. Console Access*

IoT device manufacturers may leave a physical access path for device troubleshooting activities in device consoles. However, if this access path left for such normal purposes is identified by an attacker, the access path may be exploited in the form of an attack path.

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

***F. Software-as-ServiceIntegrity***

Cyber-attack statistics show thatroot kits, ransom ware, bots, financial malware, logic bombs, virus, worms and Trojans are the most malicious attacks that exist. These can be added by the programmer at the time of source code development or in the scripting. Gray-ware,includes adware and diallers, cannot be considered as malicious, but it can negatively affect the device's performance by acting without bona-fide interest on the user's device or data. An example of Gray-ware is outdated or unused 'white' software such as Google Talk or Google's toolbar which sits on top of existing software. Mad-ware(a type of adware),uses targeted and aggressive advertising messages or pop-upsto collect information from a user's device or by storing malicious cookies in a device accessing certain unsecure web pages[7]. There also exist mobile- software based Trojans which can steal and copy mobile information from one device by sending an SMS to an app on another device. The attackers can target the IoT devices with compromising or malicious code or software infection, since they usually are not tamper-resistant, and then physically compromising them. IOT devices can be attacked by malware, compromising access, data or even the functioning of the sensing or actuating or controlling equipment via various access points. Unpatched APIs and Un-secure updates are also capable of adversely impacting this layer's integrity and security.

***G. Security of Network Communications:***

***Network Authentication***- Challenge-response mechanisms include P-2-P Encryption to ensure the confidentiality of the transmitted Data and/or Cryptographic Hash functions (CHFs)to maintain the integrity of the transmitted data. Also, there needs to be a device authentication mechanism on the network layer to secure access to confidential device data.

***RoutingSecurity-***

Routing security is key to the adoption and use of sensor networks in IOT for different applications and it is found that most of the routing protocols used are unreliable. Routing protection should be maintained by providing multiple paths for data routing which enhances the system's ability to detect an error and continue to work despite system failure.Hence, routing security is important from availability as well as confidentiality purview. Also, encryption and authentication mechanisms increase the security, i.e. integrity level of routing data. System built- in restrictions comprise of Multiple Paths, Routing Table encryption, Route Tablehashing and so on.

***Internet access via service/ Port-level Access***-The opening of unnecessary or vulnerable service ports may lead to illegitimate access to network/device. In particular, IoT devices that use the Telnet service for direct access to an embedded OS must have secured access via appropriate network barriers is necessary.

***Avoiding persistent threat due to on-going access*** -APT is a sophisticated and persistent network level threat targeting high-value information assets in business and government (national defence) to steal data. It is a three-step vulnerability exploitation and can only be secured via a multi-layer approach of cyber defence.

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

### *H. Device and Data Privacy*

***Data Integrity-***

Integrity ensures that the data exchanged between various IoT devices during the transmission stage is not altere d by any unauthorized device or individual. The validity of the data obtained on the other end is verified through cryptographic hash functions. In the event of evidence of data interference, m echanisms for error correction may be implemented to mitigate the problem.

***Data privacy***–Legal access to the sensor nodes and device and user data in it ensured by using authentication mechanisms and point-to- point encryption techniques.

### *I. Resource Management*

It involves the self-intelligence or self-management in the IOT architecture. A large number of IoT nodes can be deployed to support a single application. Thus, having to manage Fault, Configuration, Accounting, Performance andSecurity (FCAPS) capabilities is necessary and is at the heart of the manageability of IOT. The common types of manageability include centralized and distributed control. (Ahmed, Ali & Ibrahim, Nagwa.,2017)

***Availability-***

Availability ensures the data or resources are available whenever required by the devices or users so that the baseline SLAs/QoS of IoT is definitely achieved. It is measured in terms of throughput, similar to network throughput but in wireless sensor networks.

***Robustness***–This means that any node is able to tolerate issues in its execution such as errors, in input without any degradation in its performance.

***Resiliency***–It involves the comparison of computational metrics such as TTF, MTBF and so on for ensuring the restoration of services to normalcy after an abend in the IOT application functioning.

| SECURITY REQUIREMENT | C.S. GOAL OF IMPACT | | | LAYER | SECTOR/APPLICATION | MITIGATION |
|---|---|---|---|---|---|---|
| | CIA | PRIVACY | TRUST | | | |
| Physical Security/**Tamper Resistance** | X | | | ALL | 2,3,4,5,6,9 | Physical Barriers, Alarms, Security personnel, ACLs. |
| Secure Booting | X,I | | X | P.D. | 3,5,6,7 | NH, WH CHF |
| Device Authentication | X,I | X | X | P.D. | 3,5,6,7,9 | KMS, passwords |
| Data Integrity | X,I | | | Edge | 1,2...,9 | CRC, Checksum, Parity Bit, CHF |
| Data Confidentiality | X,C | | | Edge, D.A. | 3,4,5,6,7 | Blowfish, RSA** |
| Anonymity | | X | | P.D., Edge | 2,4,5,8 | K-anonymity |
| Privacy Framework | | X | | Connectivity | 1,3,4,5,6 | Auth. mechanisms and P2P encryption |
| Secure Routing and Forwarding | | X | | Connectivity, Edge | 1,2...,9 | Encryption & Authentication (R.T.), multipath protocols, hashing |
| Data Security | X* | | | D.A.,D.S., App | 3,4,5,6,7 | Auth.-Passwords/biometrics/multi-layer etc., encryption, CHF( integrity mechanisms) |
| Access Control, IAM | X | X | | ALL | 3,5,6,7,9 | ACLs |
| Intrusion Detection | | X | | ALL | 1,3,4,5,6 | Alarms, stop-locks |
| Robustness and Resilience | X | | | Edge,Connectivity,Appli cation, Collaboration | 3,4,5,6,8 | Firewalls***, Anti-malware |
| Secure Network Access | | X | | Connectivity | 1,2...,9 | CHF,Auth. mechanisms and P2P encryption |
| Network Segmentation | | X | | Connectivity | 3,5,6,8 | Micro-segmentation and/or channelisation |
| Secure Storage | X,I | X | X | Data Storage (D.S.) | 3,4,5,6,7 | Encrypted access and retrieval, RBAC -based storage |
| Encryption | X | | | Connectivity, Edge, D.S. | 3,4,5,6,7 | Cryptographic techniques (Lightweight cryptographic protocols) |
| Management Framework | | | X | ALL | ALL | Protocols, policies, regulations, mechanisms for low power reliability, QoS, processing behaviour, reputation |
| Trust Framework | | | X | ALL | ALL | Uniqueness and non-repudiation- Blockchain-based solution. |
| Audit Control | X | X | X | ALL | ALL | Risk Scanning, Compliance monitoring, built-in logging (traceability) |
| Risk Assessment & Maintenance | | X | | ALL | ALL | Systems scanning, patches & updates, security improvements |
| | | | | | | |
| ** AES cannot be used due to high power consumption | | | | | | |
| * All of C,I and A | | | | | | |
| ***Packet filtration, DOS prevention, Password-cracking prevention | | | | | | |

**Figure 2:** Summary of mitigation for security requirements

# VI. ATTACKS IN IOT TECHNOLOGY AND COUNTERSTRATEGIES

There are different variables to consider in securing IOT like the device limitations, the network infrastructure and its capabilities and so onas outlined extensively in literatureby (Perez, 2019).In the table prepared by us, is our summary of the attacks due to IOT system vulnerabilities discussed earlier that are commonly observable in IOT. This table is essential to understand the underlying impact of attacks and how they must be managed to reduce the impact on the

manageability of resources and to aid in the development of complex and dynamic adaptive security mechanisms such as the automated risk analysis system (Varga, Pal & Plósz, Sándor & Soos, Gabor & Hegedus, Csaba.,2017). or the intelligentcollaborative security model(Curtis, Hywel.,2018). for IIOT across-industry and applications.

This table displays the surface of attack for all the most frequent of attacks possible on IOT systems. A total of 40 attacks have been mapped to the architectural layers which they impact the most. This defines where the detective (surface) and the mitigate (layer of impact) and the preventative controlling of these attacks must be built into the IOT system. Also, the impact upon the goals is necessary as the driver for a countermeasure to be installed into place and necessary for accuracy of vulnerability and risk assessment.

It also helps to determine (now qualitatively) the actionable impact of any security model vis-à-vis the level of threat or exposure to any particular IOT system.

This is the first such summary of attacks w.r.t the Cisco- IOT Reference Model that we have seen in recent literature.

We have verified our summarization against numerous research papers and white papers currently published or printed in credible journals and publications. In all, IOT will prove to be compelling resource to protect, making security the critical and foundational element that the network is built on which leads to a simplified implementation of security, to ensure efficient threat

Management.

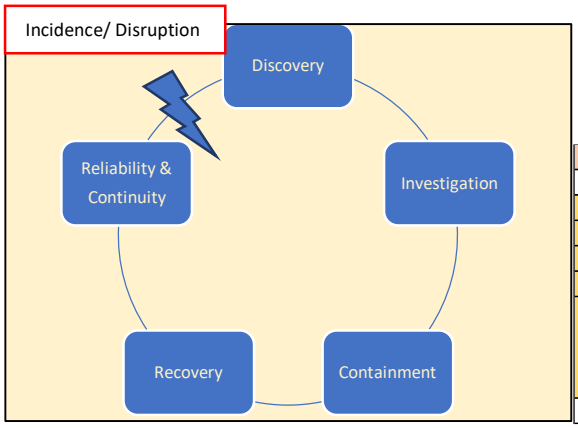
### *A. Regarding the Detection, Avoidance, Mitigation and Prevention of Cyber Attacks on IOT devices*

In the table in Fig.2, we highlight the mitigation strategies per the security requirement, going forward with our approach of maximizing the achievement of security goals. This table is a summary of the 16 high-priority requirements in an IOT system. We highlight these because they are required with one or more of all the applications; we have considered that exhibit the characteristics of Industrial IOT solutions. They also encompass our ‘security recommendations’ for what type of security modules an implementation of the solutions can carry as a benchmark. This is highly relevant because these solutions are being commonly adopted and implemented in India as well as globally.In Fig.4, the final findings, we summarize some of the recent emerging areas of security arising out of the complexity of the IOT environment, heterogeneity, stakeholder multiplicity, etc. highlighted in the section on “Architectural Models, Protocols and the Cisco-IOT Reference Model”. These have been highlighted here and can be discussed from a broader to a narrower, single point-

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

of-reference discussion on the implications of these requirements.

At present, we can see that largely these issues are being only touched upon briefly in the areas ofcloud security, third party risk and compliance, asset management, secure remote access, IOT-as-a Service (Varga, Pal & Plósz, Sándor & Soos, Gabor & Hegedus, Csaba.,2017). and so on. The real threats, vulnerabilities and the existenceof attack surfaces unknown currently remain to be assessedand studied.




| SECURITY REQUIREMENT | C.S. GOAL OF IMPACT | | |
|---|---|---|---|
| | CIA | PRIVACY | TRUST |
| Service Automation Security | X | | |
| Data Processing/Edge Security | X,A,C | X | |
| Securing Third-Party Services | X,A,C | X | |
| Cloud Computing Operational Security | X,A,I | X | X |
| Client Application Security- | | | |
| Internet-based (Web) | X,C,A | | |
| Communication Channel (V.P.N) | X,C,I,A | | |
| System Integrity | | | X |
| | | | |

**Figure 3:** End-to-end Cyber security Threat Mitigation in IIOTFig.4: Summary of Emergent security requirements in IOT

In addition, in Fig.8, there are 4 requirements that have come up in our systematic review that we specifically highlight for heightened security of certain use cases which bring the system closer to 'ideally secure', as these are preventative strategies or enablers that cut across all layers as well as applications. From the perspective of the CIA triad the restoration of system to normal risk is covered in level-3 below and this approach can be useful in maintaining some of the requirements in Fig.7, 'Emergent Security Requirements in IIOT' :

Continuity of systems via Management Framework- With 97% breaches in 74% of surveyed enterprises lasting more than 24 hours, a robust management framework which incorporates the benchmarked standards in QoS, processing behaviour, system reputation, power-optimization and such contingency planning and takes into account many of the fail-safes to manage the risk of threat and the threat itself in the occurrence of an incident are necessary.

Discovery in systems via Risk Assessment and Maintenance- Accenture's 'Innovate for Cyber Resilience' Report of 2020 highlights that 74% enterprises that are non-leaders could only detect 54% of the breaches their systems suffered. These activities will help threat detection rates climb in organizations as this is important for timely action and will in-turn affect the threat response of the IOT system to be appropriate, accurate and efficient and hence minimize damage.

Investigation, Containment and Recovery of systems via Audit Control – This is a crucial step towards securing the IOT environment as it is a preventative measure towards insider threats critical in secure networks used for surveillance and reconnaissance, data security must be ensured in physical, electronic and storage pathways and sites, limiting of access would be achieved via key-based and RBAC based authentication and access control schemes(J. Liu, Y. Xiao and C. L. P. Chen, 2012) as well as, latest regulatory compliance must be built-in and

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 

achieved either manually or otherwise. There are also tools available for threat and vulnerability scanning, monitoring and system trace-backs, that can be applied periodically for 360-degree security in IOT systems.

Reliability of Systems via Trust Framework – In a distributed and heterogeneous environment, trust or a kind of SCRM becomes imperative. According to the work on Trust-Chain, IOT application or service level trust can be managed via a Blockchain-based approach(Yu, B., Wright, J., Nepal, S., Zhu, L., Liu, J., & Ranjan, R.,2018). This is as a result of participating entities in the IOT ecosystem requiring a trust and application level authentication mechanism, to ensure reliability in the IOT supply-chain. Such a type of system trust framework has been visited frequently in IOT research. Largely, it can be seen that the trust matrices can vary as per sector or solution and they ensure a great deal of data supervision and device lifecycle management as well. The security and reliability through many techniques like E-LITHE, GTRS, TBBS and DTMS can be ensured within and between datagram, i.e. at the Transport layer (Ud Din, Ikram &Guizani, Mohsen & Kim, Byung-Seo& Hassan, Suhaidi& Khan, Khurram.,2018).

## VII. CONCLUSION

Regulation would affect the security of IOT platforms to the largest extent up to almost 85% of everything, as layer 5 (Fig.2) represents the largest attack surface. That suggests there will be many more major cyber infrastructure attack scenarios going forward. Hence, while the physical area of each device's surface is reducing to micro- or even nano- scale, the numbers are sufficient to impact cyber security of IIOT to a large extent, making the safety of devices in connectivity a priority in the times to come. Mitigation of new attacks will be countered by additional security capabilities being applied to layer 4 and layer 5 objects Aside of this, there is a need to understand security from the cost aspect and to realize the advantage of that approach in the fact that a well-implemented security apparatus within the IOT architecture can lead to immense cost-savings for an organization due to enablement of accepted security standards and frameworks in IOT security through rapid enforcement. Additionally, if our approach to IIOT application design and development is implementing principles typically found within generally accepted system for governance and compliance such as the ISO, ITIL, NIST, OWASP, or even the more recent COSO and COBIT, manageable risk mitigation might be achievable.Principally, Internet of things must include capabilities such as segmentation, authentication and encr yption combined with routine maintenance and administrative efficiency due to the realtime nature of communic ation and highly exposed internet attack surfaces, and so on, which need to be secured effectively.We should als o start designing the IoT architecture with security in mind within targeted IoT devices based on the minimum se curity requirements. Control measures can be deployed to provide safety layers but it should also secure the envir onment where security holes or vulnerabilities ex

## REFERENCES

1. Ahmed, Ali & Ibrahim, Nagwa. (2017). “Modern IoT Architectures Review: A Security Perspective,” 8th Annual International Conference on ICT: Big Data, Cloud and Security (ICT-BDCS 2017). DOI:
2. 10.5176/2251-2136_ICT-BDCS17.30. https://www.researchgate.net/publication/320044307_Modern_IoT_Architectures_Review_A_Security_Perspective
3. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 180-187, doi: 10.1109/ISCC.2015.7405513.
4. Bissel, La Salle, Dal Chin. (2020). Innovate for Cyber Resilience. AccentureSecurity Study. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
5. Bissel, La Salle, Dal Chin. (2018). The Cost of Cybercrime. Accenture Study. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
6. Chase, J. (2013). The evolution of the internet of things. Texas Instruments white paper. http://www.ti.com/lit/ml/swrb028/swrb028.pdf
7. Cheruvu S., Kumar A., Smith N., Wheeler D.M. (2020) IoT Frameworks and Complexity. In: Demystifying Internet of Things Security. Apress, Berkeley, CA.https://doi.org/10.1007/978-1-4842-2896-8_2
8. Curtis, Hywel. (2018). Why you need Automated Security for the Internet of Things.Venafi.
9. https://www.venafi.com/blog/why-you-need-automated-security-internet-things-iot.
10. Dev Technosys (2018, May 22). How Much Does it Costs to Develop IoT Application?Business of Apps. https://www.businessofapps.com/news/how-much-does-it-costs-to-develop-iot-application/
11. Filho (2020). Vulnerabilities and security issues of IoT devices. Sikur Lab whitepaper. DOI:10.13140/RG.2.2.14211.86562.
12. Gochhait, S., Shou, D. T., &Fazalbhoy, S. (2020). Cloud Computing Applications and Techniques for E-Commerce. IGI Global. http://doi:10.4018/978-1-7998-1294-4
13. Islam, S.M., Kwak, D., Kabir, M.H., Hossain, M., & Kwak, K. (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, 678-708.
14. Ivan Valeryevich Evdokimov et al 2019 J. Phys.: Conf. Ser. **1176** 042083
15. A Cost Estimation Approach for IOT projects.
16. https://iopscience.iop.org/article/10.1088/1742-6596/1176/4/042083
17. Liu, Y. Xiao and C. L. P. Chen, "Authentication and Access Control in the Internet of Things," 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, 2012, pp. 588-592, DOI: 10.1109/ICDCSW.2012.23.
18. Kaushik, Keshav & Dahiya, Susheela. (2018). Security and Privacy in IoT based E-Business and Retail. 78-81. 10.1109/SYSMART.2018.8746961
19. Khalid, A., Butt, S. A., Jamal, T., &Gochhait, S. (2020). Agile Scrum Issues at Large-Scale Distributed Projects: Scrum Project Development At Large. International Journal of Software Innovation (IJSI), 8(2), 85-94. doi:10.4018/IJSI.2020040106.

20. Milosevic, Jelena & Sklavos, Nicolas & Koutsikou, Konstantina. (2016). Malware in IoT Software and Hardware. Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE'16)
21. https://www.researchgate.net/publication/317011595_Malware_in_IoT_Software_and_Hardware.
22. Parotkin, Nikolay &Zolotarev, Vyacheslav. (2018). Information Security of IoT Wireless Segment. 1-7. 10.1109/GloSIC.2018.8570144
23. Radanliev, P., De Roure, C.., Cannady, S., Montalvo, R.M., Nicolescu, R., Huth, M., 2018. Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance, in: Living in the Internet of Things: Cybersecurity of the IoT - 2018. Institution of Engineering and Technology, London. https://doi.org/10.1049/cp.2018.0003
24. Rak M., Casola V., De Benedictis A., Villano U. (2019) Automated Risk Analysis for IoT Systems. In: Xhafa F., Leu FY., Ficco M., Yang CT. (eds) Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 24. Springer.
25. Robles, Daisy & Robles, Rosslin. (2019). State of Internet of Things (IoT) Security Attacks, Vulnerabilities and Solutions. 3. 255-263.https://www.researchgate.net/publication/334224658_State_of_Internet_of_Things_IoT_Security_Attacks_Vulnerabilities_and_Solutions/citations
26. R. Sharma, N. Pandey and S. K. Khatri, "Analysis of IoT security at network layer,"2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, 2017, pp. 585-590
27. The Internet of Things Reference Model (2014). Cisco whitepaper.http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.
28. Tsai, Chang (2004). Function-based cost estimation integrating quality function deployment to support system design. International Journal of Advanced Manufacturing Technology 23(7):514-522. DOI: 23. 514-522. 10.1007/s00170-003-1564-7.
29. Ud Din, Ikram &Guizani, Mohsen & Kim, Byung-Seo& Hassan, Suhaidi& Khan, Khurram. (2018). Trust Management Techniques for the Internet of Things: A Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2880838.
30. Varga, Pal &Plósz, Sándor&Soos, Gabor &Hegedus, Csaba. (2017). Security Threats and Issues in Automation IoT. 10.1109/WFCS.2017.7991968.
31. Yu, B., Wright, J., Nepal, S., Zhu, L., Liu, J., & Ranjan, R. (2018). IoTChain: establishing trust in the Internet of Things ecosystem using Blockchain. IEEE Cloud Computing, 5(4), 12-23
32. https://doi.org/10.1109/MCC.2018.043221010

**Received: 02 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 05 Feb 2020** 