WHITE PAPER

IOT CONNECTED WORLD : SECURITY AND PRIVACY

- Shri Krishan, Vishal Sharma & Pawan Dubey

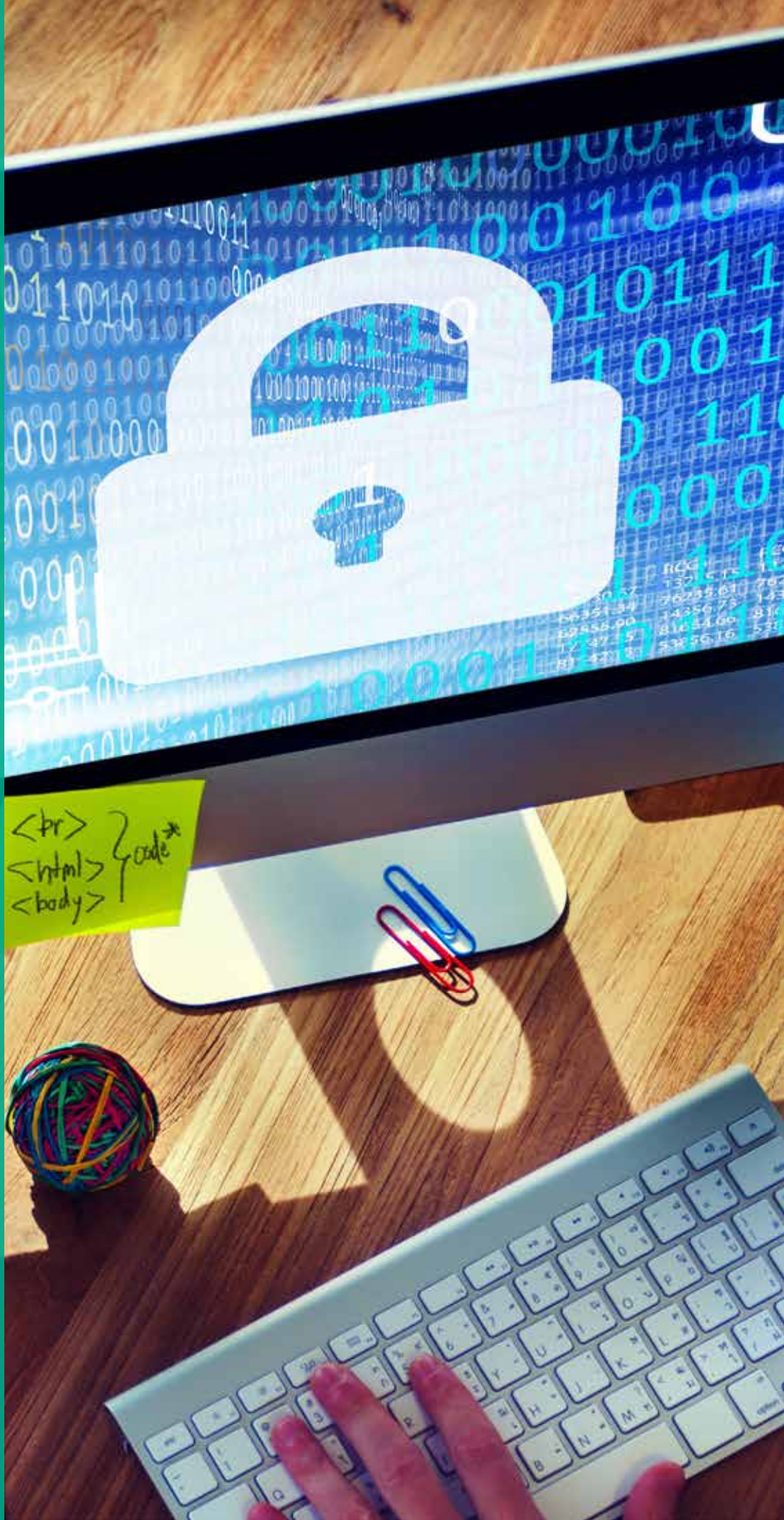
Infosys®
Navigate your next

Executive Summary

We are in a world where potentially everything is becoming digital, mobile and connected via the internet. These latest waves of technological changes will bring unprecedented opportunities, along with new risks, to business and society. It will combine the global reach of the Internet with a new ability to directly control the physical world, including the machines, devices and infrastructure that define the modern landscape. Security in IoT is fundamentally linked to the ability of users to trust their environment. If consumers don't believe their connected devices and their information are absolutely secure from misuse or discrimination, the resulting attrition of trust causes disinclination towards the adoption and use of the internet.

While we move towards the realm of a connected world- connected living, it has now become necessary to conceptualize IoT security and privacy as a spectrum of device vulnerability. The spectrum ranges from totally unprotected devices with no security features to highly secure systems with multiple layers of security features.

This paper addresses the impact of Internet of Things (IoT) on telecom business, challenges and opportunities associated with Information Security. The overall security and resilience of IoT is a function of how security risks are assessed and managed. Service providers and OEMs must consider security as key enabler for adoption of IoT, rather than just an afterthought or enforced cost. This paper outlines key mechanisms proposed to overcome the impact of security and privacy challenges in today's telecom business and technology oriented business platforms.



Contents

Introduction - Internet of Things

Internet of things (IoT) refers to the ability of everyday objects to connect to internet and exchange information. IoT network provides an interconnected environment where objects have a digital presence and can communicate with other objects and people. In an IoT ecosystem, anyone present anywhere and at any time can use service/application to control things e.g. connected home: home owner can open smart door locks for an unauthorized person after checking on a smart video camera over the internet.

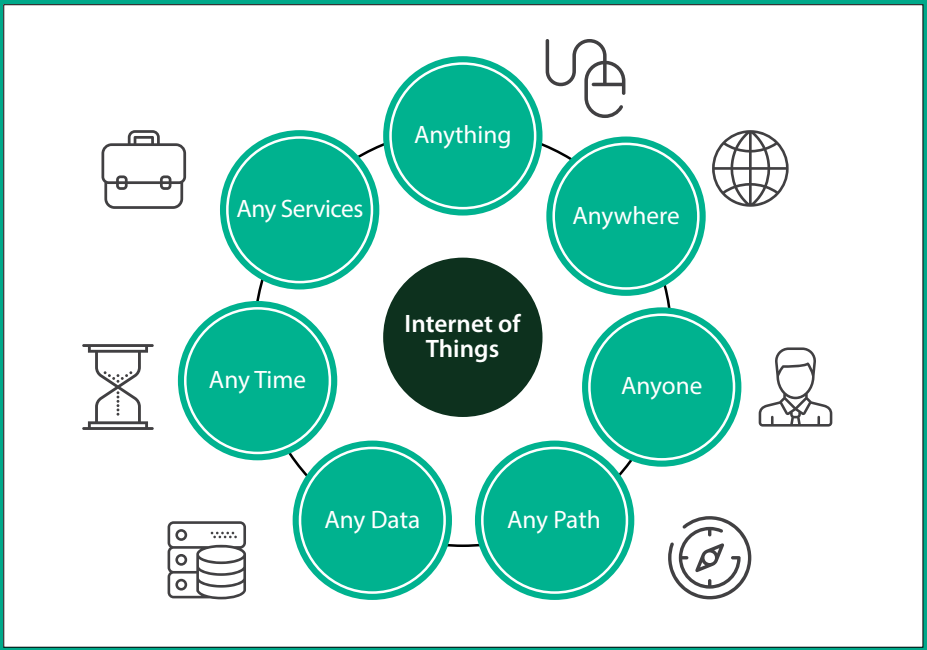


Figure 1: IOT ecosystem

IoT represents a revolutionary transformation in IT and digital world that has the potential to touch everyone's life. We can already feel changes to the day to day activities such as smart connected homes, smart cities, tagging cattle in agriculture fields, efficient energy management, remotely real-time patients monitoring, integrated supply chain, smart wearable devices, parking sensors and many more. The growth and adoption of IoT is moving at a very fast rate. Its adoption is driven by multiple forces involving rise in connected devices, evolution of wireless protocols, low cost micro-processors, huge volumes of data and increase in inclination towards cloud based application software.

As per analysis from Cisco [1] and Morgan Stanley [2], by 2020, more than 50 billion devices will be connected through IoT globally. Figure 2 below show the global IoT forecasts by various analysts. The IoT global market forecast will be between $3.9 and $11.1 trillion by 2025 as per McKinsey [3] latest report.

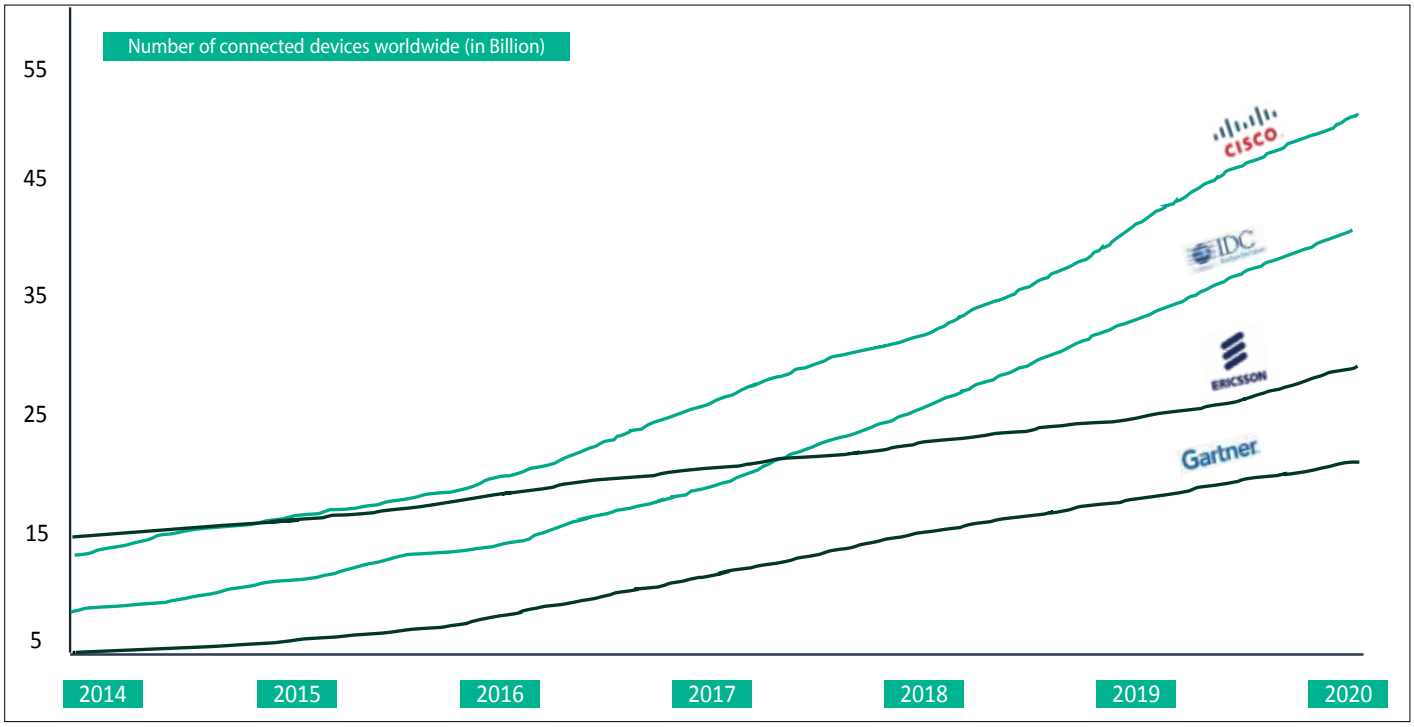


Figure 2: Global IoT device forecasts, IoT Analytics 2014.

IoT Architecture

IoT enablers are a) Hardware (smart devices) b) Communication layer c) Cloud (application hosting, rule engine and database etc.) and d) application layer. Figure 3 represents IoT architecture for a connected home as an example.

Connected physical devices such as embedded devices, sensors, smart meters, actuators, hub, centralized console, gateways generate and exchange required data to enable connected things. Data is communicated and transported to network using communication technologies like Wi-Fi, NFC, RFID, Barcode, Bluetooth, zig bee, Z-wave, LTE, 3G, 4G, Global navigation system, LAN, WAN.

1. Device to Device: This model is commonly used in solutions such as home automation, which uses small data packets of information with relatively low data rate. Residential IoT devices such as light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command).

2. Device to Cloud: Devices connect directly to an Internet cloud service e.g. to an application service provider to exchange data. This approach make use of Ethernet or Wi-Fi connections to establish a connection between the device and the IP network that connects to the cloud service.

3. Device to Gateway: IoT device connects through a gateway as a channel to reach cloud service. In simple terms, application software on a local gateway device acts as an intermediary between the device and the cloud services to provide security and other functionality such as protocol translation. In many cases, the local gateway device is a smartphone running an application to communicate with these devices and relay data to a cloud service.

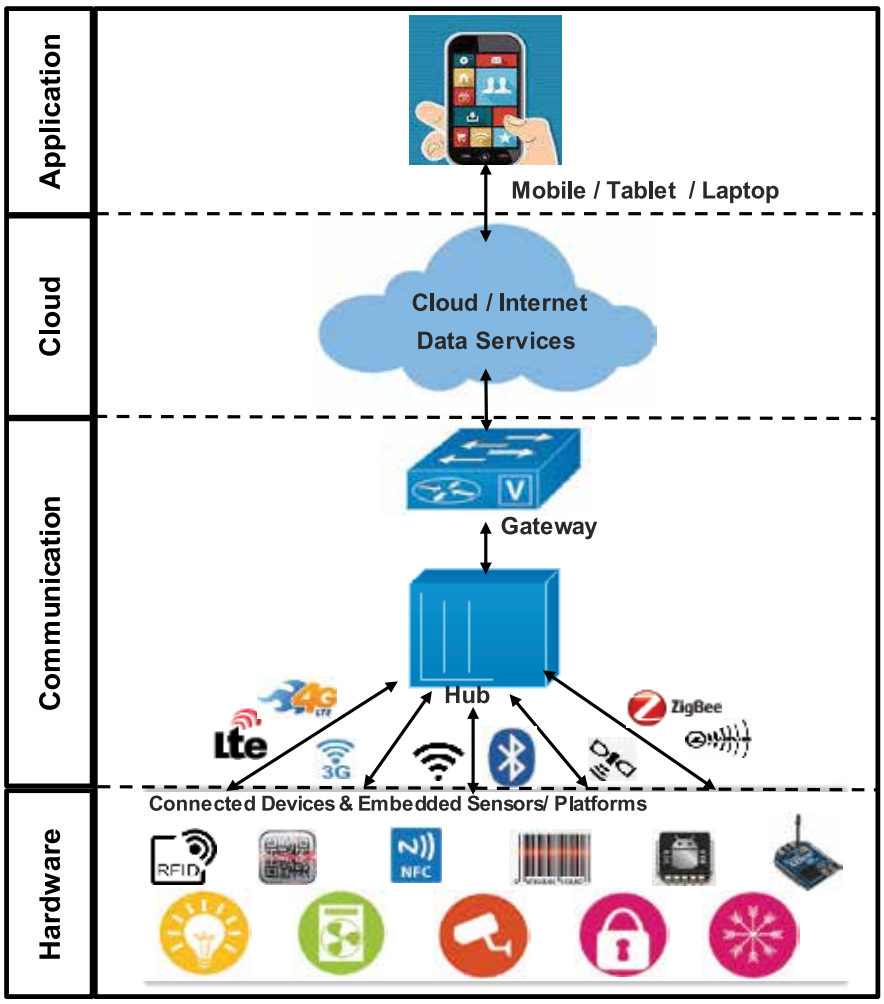


Figure 3: IoT architecture

Data generated by hardware devices and processed by software, is consumed by applications available on smartphones, PC, tablet or other devices through mobile or web apps. This is where IoT services turns the data into real value for end user (B2B or B2C).

Common IoT Protocols

Many protocols have been defined and developed at various layers of the International Organization for Standardization (ISO) stack to enable the operation of IoT devices. The key thing to be aware that these protocols are designed with energy preservation in mind, along with low computing and memory requirements. The IPv6 Internet is one of the most important enablers of the IoT as it is not possible to add billions of devices to the IPv4 Internet.

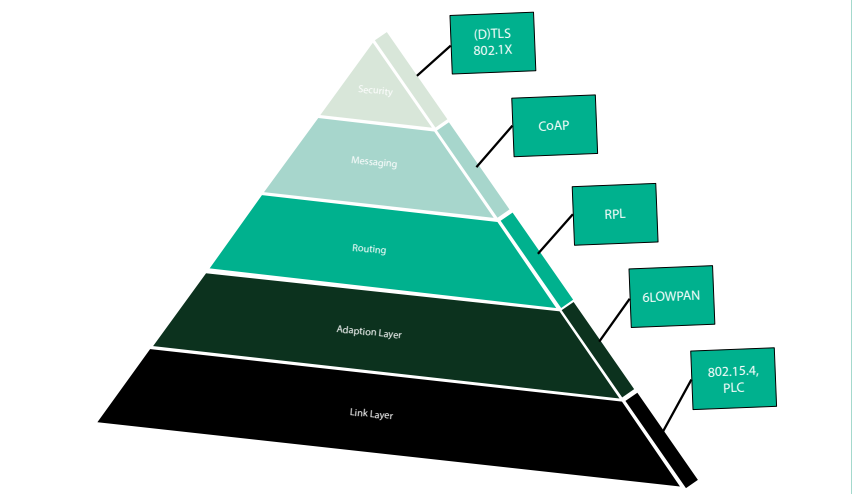


Figure 4: Common IoT protocols

Researchers and early adopters have been further encouraged by advancements in wireless technologies, including radio and satellite.

Thinking Security and Privacy

In today's world, when the technology become more omnipresent and integrated into our day to day lives, security consideration expanded to personal privacy, financial transactions and cyber theft which includes attacks such as identity forging, hacking, phishing, data theft, Operating system attack, key logging attack, denial of service (DoS) attacks etc. Any compromises on security of IoT devices and services can serve as potential entry points for unauthorized access and expose user data to theft. Cyber criminals are targeting organizations or individuals through new techniques such as distributed denial of service (DDoS), cross platform malware (CPM), industry control system (ICS) attacks etc. Their attacks are becoming more sophisticated and difficult to control.

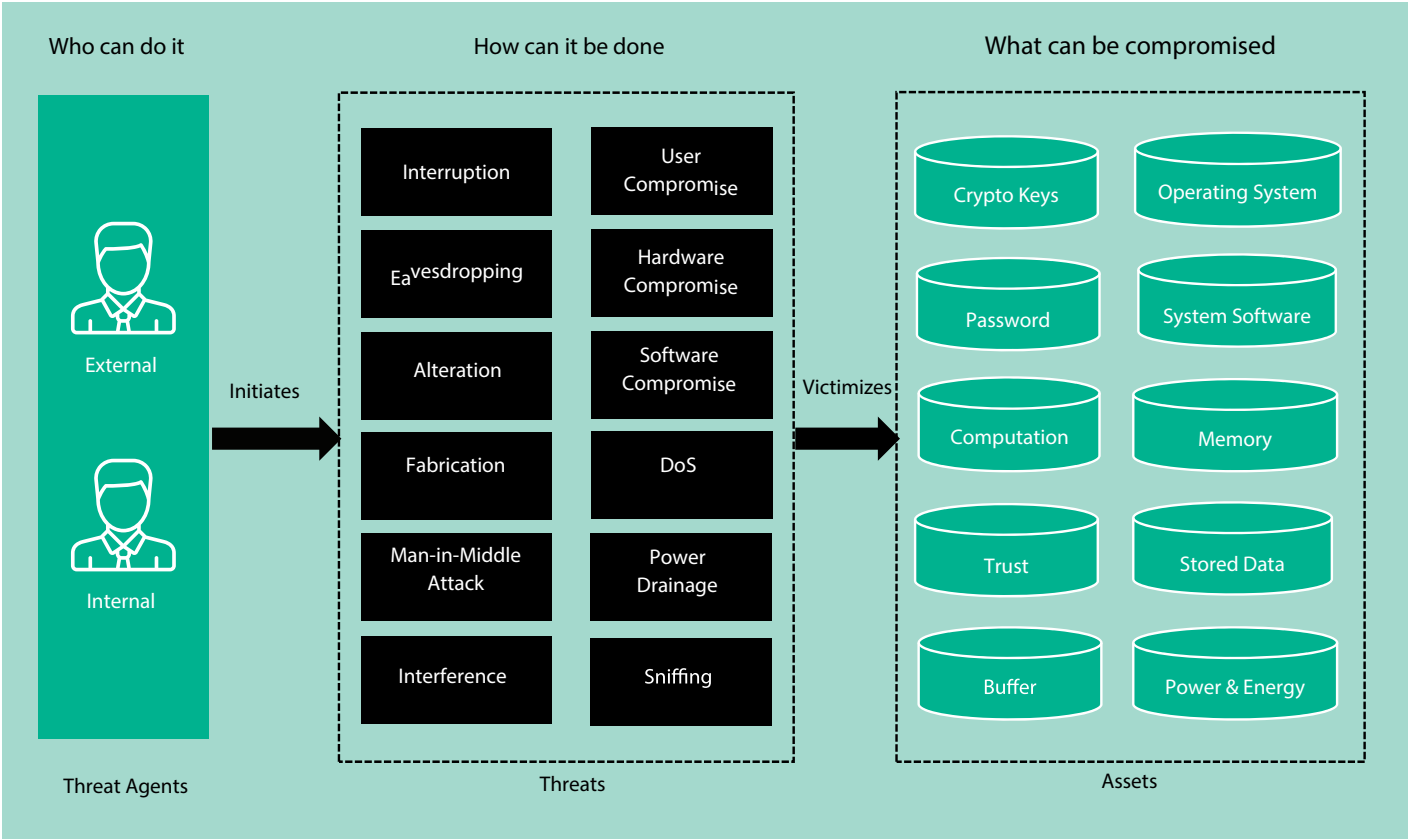


Figure 5: IoT security/privacy intrusion flow

There are five key IoT areas to examine some of the most pressing challenges and questions related to the technology. These include security; privacy; interoperability and standards; legal, regulatory, and rights; and emerging economies and development. In this paper, we will be primarily addressing security and privacy challenges and some key mechanism proposed to overcome the impact of these challenges on today's telecom business and technology oriented business platforms.

IoT Security/Privacy Questions

A number of areas of concerns have been raised regarding security and privacy challenges posed by Internet of Things ecosystem. Many of these questions existed prior to the growth of IoT, but they increase in significance due to the scale of deployment of IoT devices and connected world initiatives. Some prominent questions include:

Security	Privacy
Design Principles • What are the guiding principles for device manufactures to handle security threats? • Can devices to handle threats automatically? **Design cost Vs Security** • How to make right choice considering cost Vs benefit analysis **Metrics and Benchmarking** • Defined guidelines to benchmark and measure the effectiveness of security measure? **Out of service devices** • Shall IoT device have EOL based on security vulnerabilities?	**Data Acquisition** • How to avoid repeat of data privacy issue observed already? • How to address change in data definition as legitimate change? **Privacy Preferences** • What are the alternatives to traditional privacy model that can address challenges of the Internet of things? **Privacy Mechanism** • How to motivate device manufacture to give more focus on privacy aspects? • Need for standardization worldwide on privacy considerations for IoT

Figure 6: IoT security/privacy questions

IoT: Security and Privacy Threats

Device & Hardware	• Unauthorized access • Unsecure external ports and network access • Lack of security configurability • Malicious software updates • Out of date legacy devices	**Communication**	• Vulnerable services over unsecure network • Lack of transport encryption • DDoS • Open ports via UPnP
Cloud	• Attacks on unsecure Cloud interface • In-cloud data leaks • SQL injection • Poorly configured SSL/TSL • Out of date legacy devices	**Application**	• Attacks on unsecure mobile/PC and applications • Lack of security configurability • Unsecure password recovery • No role based access • No application or password lockouts • Collection of unnecessary personal data and sharing over network

Figure 7: IoT security and privacy threats

Security Breach: Potential Candidates

The Internet of Things is emerging at a time when threats to data and systems have never been greater. There is an average of thirteen enterprise security breaches every day, resulting in roughly 10 million records lost a day—or 420,000 every hour. Below are few example of security breaches. Below are few example of security breaches in different industries.

Automobile

i. Manipulation of connected cars: Security experts Chris Valasek and Charlie Miller did a research on the vulnerability of connected cars when they hacked into a Toyota Prius and a Ford Escape using a laptop plugged into the vehicle's diagnostic port. They could manipulate the car's headlights, steering, and breaking.

Healthcare

i. Threats to medical devices: Scott Erven exposed major security breach that could pose serious threats to the health and safety of patients. They could remotely manipulate devices, including those that controlled dosage levels for drug infusion pumps and connected defibrillators and pacemakers.

Energy and Power

i. Dangers of smart grid: Department of Homeland Security discovered a flaw in hardened grid and router provider, RuggedCom's devices. By decrypting the traffic between an end user and the RuggedCom device, an attacker could launch attacks to compromise the energy grid.

Smart home

i. Smart security systems: IoT-enabled home security solutions and temperature control systems use sensors to collect and share data from multiple edge devices. If an attacker gains access to these smart systems through malicious means, the underlying functional logic of control systems is vulnerable to misuse, compromising the physical security of residents. Key security and privacy concerns to be addressed in this scenario are:
   a. What data is captured and transmitted by IoT devices and who can access it?
   b. Does the IoT product vendor have access to the data generated from these devices?
   c. Is the data that is sent to the actuator encrypted, and is there an authentication process involved in the transmission of data?

Banking, Financial services and Insurance

i. Smart Billing and payment systems: In a retail outlet, IoT sensors are used to tally the purchases in a customer's cart. This means customers do not need to stand in the queue for checkout and billing, with sensors sending the data to a cloud-based billing and payment systems. Customers can pay the bill through a payment app on their smartphones. In this scenario, the following security and privacy questions are significant:
   a. How is the data from sensors logged and for what duration? Is the data copied to multiple locations for back-up?
   b. Is the transaction compliant with PCI Payment Acceptance Data Security Standard?
   c. Is the data safe in transit – from sensors to the cloud, and from the cloud to customer's smartphones?
   d. Has any customer's PII been compromised?

Retail sector

i. Smart fitting rooms in retail outlets: RFID sensors are used in smart fitting rooms in retail outlets to allow customers to flip through a catalogue on a touch screen and indicate the items that need to be displayed in the dressing room. When a shopper walks to the dressing area, the smart mirror recognizes the items and displays different clothing items on the screen. Customer's shopping behavior and pattern data can be stored by the retailer for cross-sell recommendations. The following security and privacy questions are pertinent in this scenario:
   a. What data is gathered and transmitted by sensors, and does this data remain anonymous?
   b. Is there any possibility of intercepting the data gathered by sensors?
   c. Can the supply chain data be compromised during data transit?

ii. Smart vending machines: Smart vending machines allow customers to choose products from the display, during which, customer details are obtained through their smartphones by a Near Field Communication (NFC) smartphone payment system fitted to the vending machine. Merchants can use this data to improve stock replenishment, perform health checks on vending machines, and identify popular products. Security and privacy concerns in this scenario include:
   a. Is the data sent from sensors to a gateway device encrypted?
   b. Is any customer identifiable information stored in gateway devices or in the cloud?
   c. Can merchants exploit customer information for business benefits without the customer's consent?

Building secure foundation for IoT

IoT networks are complex therefore securing each of the element spanning from IoT devices to connectivity to cloud layer is extremely important. All the elements need to work cohesively to provide end-to-end protected atmosphere, otherwise the attackers can exploit the weakest link. Based on the security and privacy threats mentioned in the previous section, we can conclude that IoT networks have additional and unique security needs as compared to traditional IT systems. Below are the recommendation to address security and privacy concerns.

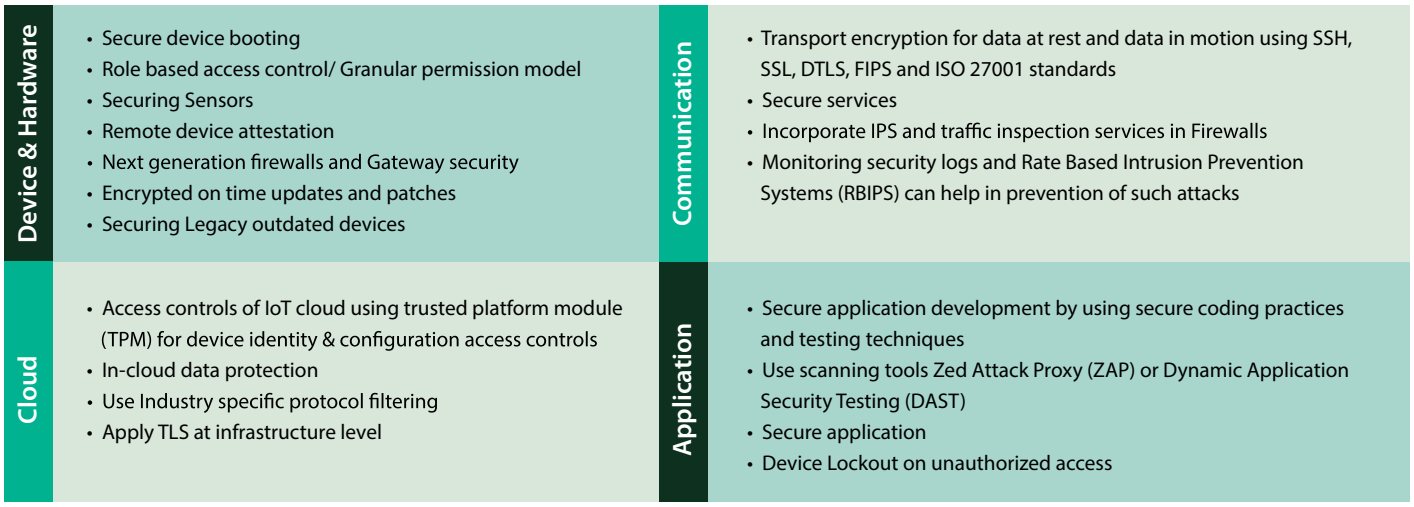


Figure 8: Recommendations for securing IoT

Below are additional information on recommendations to secure IoT:

Device and Hardware: Security must be embedded in the endpoint devices for their lifecycle and can be achieved by various mechanisms as mentioned here.

i. Secure device booting: Cryptographically generated digital signing should be used to verify and validate the authenticity of software present in device while first booting. All critical devices, whether an embedded device, sensor, hub, or anything else should be configured to only run signed code.

ii. Securing Sensors: Wireless sensors that provide last mile of connectivity for IoT-enabled services can be damaged by human influence or natural wear and tear. Memory and power limitations of IoT devices also make them vulnerable to eavesdropping and radio jamming attacks. Therefore, threat mitigation of IoT devices is imperative to secure smart services. For smart service implementation in open outdoor environments, periodic site survey is a must to track the IoT device outlay.

iii. Role based access control / Granular permission model: By building role based access control in operating system, the device can only access the required resources. In case of attack, the attacker has negligible access to other resources, hence the minimal effect of security attack on device and network. Administrative users must have separate permissions from normal users to access encryption options and security logs. Host based protections such as whitelisting instead of blacklisting, sandboxing, hardening and lockdown also secure devices.

iv. Remote device attestation: Use of Trusted Platform Module (TPM) enables remote attestation using cryptography identity techniques can confirm the integrity and authentication credentials of remote devices, without revealing devices and their owners identities.

v. Encrypted on time updates and patches: On-time, encrypted, signed and verified updates over the secure network are very important from security perspective. These software updates and security patches should consume limited bandwidth and basic functional safety should not be compromised.

vi. Securing Legacy outdated devices: The old legacy devices cannot be improved to have in-built security so they must be protected by placing them on an insulated overlay network that separates them from security attacks and also provides confidentiality and integrity protections for traffic transported from them.

vii. Next generation firewalls and Gateway security: These security systems offer analysis capabilities with near real-time visibility into emerging threats. They include features such as URL filtering to help mitigate phishing, and advanced malware mitigation to prevent denial-of-service attacks.

Other important things such as tamper resistance hardware, virtual firewalls, physical security of device and its storage mediums and disabling open external ports can ensure the safety of hardware and data (at rest) present in devices.

Communication or transport channel

i. Transport encryption: Data at rest and data in motion must be encrypted using standard security techniques such as Secure Sockets Layer (SSL), Transport Security Layer (TLS), Datagram TLS (DTLS), Secure Shell (SSH), cryptographic algorithms, ISO 27001 and Federal Information Processing Standard (FIPS). Firewalls should be designed by incorporating IPS and traffic inspection services to better detect suspicious traffic.

ii. Secure services: Preventing open ports in device helps reducing security attacks such as buffer overflow, fuzzing and DoS attacks. Secure coding practices, using switches with ACL and TCP connection splicing capabilities, monitoring security logs and Rate Based Intrusion Prevention Systems (RBIPS) can help in prevention of such attacks.

Cloud/Web

This layer offers services such as data aggregation, data analysis and data processing.

i. Access controls of IoT cloud: Cloud services often have login/credential-based services for authenticating users. Trusted platform modules (TPM) must be used for device identity and configuration access controls.

ii. In-cloud data protection: This will prevent data leakage during data transmission, data processing and when data is stored in the cloud. Applying TLS at the infrastructure level, including data centers, will ensure protection from internal threats and security breaches.

Application

Mobile/web/cloud applications must be developed with industry security standards.

i. Secure application development: Standard secure coding practices and testing techniques must be used to prevent security issues pertaining to XSS, SQLi, CSRF, DoS attacks etc. OWASP suggests using scanning tools such as Zed Attack Proxy (ZAP) or Dynamic Application Security Testing (DAST) to secure from these attacks.

ii. Secure application: General techniques such as account lockout, password recovery mechanism, unexposed credentials over network and session management must be used.

Privacy Considerations in IoT

Privacy is very sensitive subjects in context of IoT protection. In IoT, Users would have access to an unprecedented number of personalized services, all of which would generate considerable amount of data, and the environment itself would be able to acquire information about users automatically. IoT could certainly intensify a range of undesirable situations. Facebook accounts already affect a user's employability and personal interactions. Imagine exponentially more such exposure opportunities.

Privacy by design

One recommended solution is privacy by design, in which users would have the tools they need to manage their own data. The solution is not too far from current reality. Whenever users produce a data fragment, they can already use dynamic consent tools that permit certain services to access as little or as much of that data as desired.

Transparency

Transparency is also essential, since users should know which entities are managing their data and how and when those entities are using it. Stakeholders such as service providers must be part of this equation, which might make take-it-or-leave-it license agreements obsolete. Businesses will adjust their services according to the amount of personal data the user provides.

Data management

A huge issue is, deciding who manages the secrets. Technically, cryptographic mechanisms and protocols protect data throughout the service's life cycle, but some entities might lack the resources to manage such mechanisms. In other words, one data management policy will not fit for all situations. Consequently, there must be policies on how to manage various kinds of data as well as some policy-enforcement mechanism. It requires interpreting, translating, and optimally reconciling a series of rules and standards each of which might be in a different language and any policies must align with legislation on data protection, which itself could change.

Search Query

Search queries can reveal information about the person who initiated it by tracking the IP address of the source. For instance, a smart refrigerator makes online queries for food items that its owner likes. In this scenario, businesses can track such queries and profile the owner based on his or her fondness for specific food items. This data can then be used for target advertising without the individual's consent.

IoT security and privacy market impacts

As mentioned above in introduction section of this paper, the research reports have predicted the growth of IoT market to multi trillion USD and increase in number of connected devices to around 50 billion by 2020. These encouraging numbers will surely lift the research and spending in IoT security and privacy area. Security and privacy are key enablers and potential inhibitors of IoT adoption. They are the major concerns which is slowing down the IoT adoption. All the stakeholders involving original equipment manufacturers (OEM), internet service providers, cybersecurity companies and consumers must start addressing concerns such as software security, embedded security, data privacy and lack of interoperability standards for better IoT enablement.

In anticipation to IoT security and privacy market opportunity, most of the major Cybersecurity companies and internet service providers have already started preparing roadmaps and architecture. The IoT has redefined the security of device, network and data privacy by expanding the scope of enterprise responsibilities to new platforms, channels and layers.

New start-ups have also started delivering their role in the segments such as device authentication, data encryption and layered network segmentation. Large security companies have also started acquiring these IoT startups to support their roadmaps and security service portfolio.
Original equipment manufacturer (OEM) spending is increasing to provide intrinsic device security and keeping interoperability intact.

Most of the international organizations have started working on common standards for IoT security. International Standards Organization (ISO) has already built a working group to assess the ISO 27000 family of security standards adaptation to address IoT security needs. IEEE standard association has been working on standardized architectural framework which is expected to address IoT security, governance and safety issues.

Several IoT vendor alliances such as IoT Security Foundation, OWASP, Thread Group, the Open Interconnect Consortium, the AllSeen Alliance and the Industrial Internet Consortium are working on IoT development, ensuring use of data encryption and other security principles

Conclusion: Building way for smart and connected world

To realize the true potential of this technology, security and privacy concerns need to be effectively addressed. In addition to self-regulation, a structured and well defined cyber-security and privacy policy must be developed with efficient collaboration between governments, enterprises and standard governing bodies.
It is also important to ensure that IoT specific legislation and industry standard protocols do not suppress innovation. This will allow individuals and communities to reap the advantages of the IoT and build a smarter connected world that offers intelligent solutions for big and small challenges across all walks of life.

The collaborative model has been identified and recommended as an effective approach among industry, various LOB's and public authorities to help secure the Internet and cyberspace, including the Internet of Things. Continuous work is needed to evolve collaborative and shared risk management-based approaches that are well suited to the scale and complexity of IoT device security and privacy challenges of the future connected world.

About the authors

Shri Krishan - Principal Consultant, Infosys

Shri works as Principal Consultant and his expertise lies in the areas of CRM, Fulfillment, Assurance, Billing and Business Analytics for leading Telecom providers. With over 18 years of experience in Telecom domain, he has played advisory roles to CXOs for OSS/BSS solution evaluations and improving customer experience. He is passionate about analyzing and expressing view points on significance of trending technologies for telecom industry, such as SDN/NFV, 5G and IoT. Shri can be reached at Shri_Krishan@infosys.com.

Vishal Sharma - Senior Consultant, Infosys

Vishal is a Senior Consultant in Telecom domain and has keen interest in the areas of BPM, Fulfillment and Assurance. He is ITIL v3 and IBM SOA foundation certified and has over 10 years of experience. Vishal has worked across business process consulting, program delivery, OSS/BSS solutions and improving customer experience. He is passionate about analyzing emerging technologies such as IoT, SDN and 5G. You can reach him at Vishal_Sharma17@infosys.com.

Pawan Dubey - Consultant, Infosys

Pawan is a business solution consultant with a focus on OSS/BSS-Service Assurance and Fulfilment for leading Telecom providers. With over 6 years of experience, he has played a key role in developing commercially viable end-to-end technical BSS solutions, furthering business success by applying e-TOM industry Standards, applications and the definition of high level solutions for development of operational processes and procedures. He is passionate about analyzing and expressing view points on relevance of trending technologies for telecom industry, and has published many thought papers on subjects like – M-Agriculture, IoT Security and Privacy etc. Pawan can be reached at Pawan.Dubey@infosys.com.

Appendix

Industry Forums Recognition:

1. TM Forum Live ! Asia Conference, December 2016: Event Website: http://tmforumliveasia.org/
   Published Portal: http://inform.tmforum.org/internet-of-everything/2016/09/iot-isnt-secure-people-wont-use/
2. 5th Annual Enterprise Mobility Summit, Toronto, October 2016: http://www.mobileenterprisecanada.com/
3. IoT Show.in (Electronic For You Group), March 2017: http://iotshow.in/; http://efy.in/iot-show/

References

1. Source: The Internet of Things - How the next evolution of the internet is changing everything, Cisco 2011 https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
2. Source: Morgan Stanley: 75 billion devices will be connected to the Internet of Things by 2020, Business Insider 2013. http://www.businessinsider.in/Morgan-Stanley-75-Billion-Devices-Will-Be-Connected-To-The-Internet-Of-Things-By-2020/articleshow/23426604.cms
3. Source: The Internet of Things: Mapping the value beyond the hype, McKinsey 2015.
4. Source: http://www.iotconnectivitysolutions.com/news/2016/07/14/8391784.htm, July, 2016
5. Source: http://www.gartner.com/newsroom/id/3185623, Gartner, 2016
6. OWASP Internet of Things Project, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

For more information, contact askus@infosys.com

Infosys®
Navigate your next