TATA COMMUNICATIONS

PORTFOLIO : SERVICE

SECURING THE INTERNET OF THINGS

TATA COMMUNICATIONS MOVE™

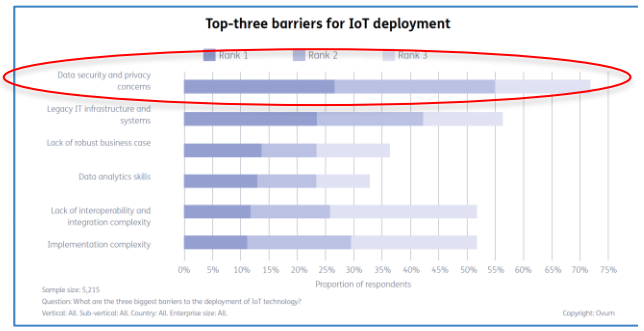
FEB 2018 | TATA COMMUNICATIONS

INTRODUCTION

As the Internet of Things (IoT) develops, there is a requirement to support an accelerating number of inter-connections in as secure a way as possible. This creates potential for significant vulnerabilities, whether they are inherent in the IoT solutions or resulting from the proliferation of end points, and IoT has been the subject of some high profile cyber security attacks, such as the Mirai Virus which targeted IP addresses of IoT connected devices to transform an IoT device into a vehicle for DDoS attacks. Mirai scans IP addresses to local home routers and other simple IOT devices where password security might have become lax. It then uses this simple vulnerability to install itself on a device, thus arming the device with a DDoS malware that can be woken at any time to perform an attack on the network. The need for a combination of global and secure operation is particularly relevant for use cases associated with transportation, logistics, supply chain operations and fleet management.

Safeguards are required to prevent misuse of connections. An IoT connectivity service provider has an important role to play in safeguarding IoT devices and SIMs. While securing any system against misuse and attack is now a critical part of any information management system, IoT based systems exhibit some unique characteristics. IoT based systems are typically composed of physically distributed devices, often located remotely. Another characteristic is that most devices will tend to exhibit the same pattern of data generation, with some variations depending on location. Thus a combination of location, context and usage patterns can also govern approaches to securing IoT connectivity. From the perspective of security, IoT also raises additional issues. One issue is that mobile devices being connected to the Internet means that some smart devices present a potential portal for malicious access. Also the sheer number of devices on the network creates a significant target for hackers, presenting multiple attack paths along which to gain entry into an enterprise network. This requires a proportionate response with layered security and control mechanisms. An appreciation of why hackers choose to target certain devices is important to understand – IoT devices are often deployed in remote locations, may not always be easy to physically secure and are large in number, presenting a range of vulnerabilities that atypical for an IT environment, but which are typical for a communications network – each of these factors makes IoT an attractive target for a hacker. Organizations involved with IoT projects need to have the re-assurance of a multi-layered approach to security, that can counter these vulnerabilities.

A recently published Ovum report indicates that among the top 3 barriers to IoT project adoption, data security was ranked the biggest concern by enterprises, followed by the restraints imposed by legacy IT infrastructure and business case issues.



This paper focuses on the specifics of securing cellular IoT based services. While IoT security is a very broad topic, it can be divided into 'Device Layer' security, 'Network security, 'Application & Cloud Layer' security and 'Threat Detection & Management'. While this paper focuses on device and network layers, reference is also made to the other layers, particularly Cloud security.

DIFFERENT APPROACHES TO IOT DEVICE CONNECTIVITY

There are multiple ways to manage IoT connectivity, including short range wireless, LP-WAN, Satellite and fixed line communications, as well as cellular. Each approach comprises multiple sub-options (i.e. cellular connectivity might be accomplished via 2.5G, 3G, 4G or 5G), and based on a variety of use case requirements each approach presents a different combination of authentication and security options and challenges.

Cellular connectivity brings a legacy of secure device access, identity management and authentication techniques, developed over many years in support of human-to-human mobile communications, combined with the security techniques that have been developed to protect IP based communication services. This creates a secure foundation for end-to-end IoT communications. Additional techniques are also deployed to protect IoT services.

Addressing security concerns around cellular IoT, analysis of spending on IoT related security indicates that the bulk of investment (~80%), through 2021 is expected to be upon device layer and network layer security.

Global Market for IoT Security Solutions, by Type of Solution, Through 2021
($ Millions)

Solution	2015	2016	2021	CAGR% 2016–2021
Device layer security	1,589	2,368	7,087	24.5
Network layer security	513	694	1,715	19.8
Application and cloud layer security	205	238	1,029	34.0
Threat detection and management solutions	154	195	686	28.6
Security platforms	103	167	914	40.5
Total	2,564	3,662	11,431	25.6

It should be noted that while the volume of spend for device layer and network layer security is the significant area of investment, this does not mean that is where all the vulnerabilities in a service lie. The compound annual growth rate of application and cloud security, threat detection and security platforms is a reflection that these areas will become increasingly important over the next few years.

Endpoint devices and endpoint network connectivity is the most vulnerable part of an IOT system. It is difficult to apply strong security applications on many devices, due to a need to conserve battery life. Also low bandwidth on end point connectivity creates vulnerability to DDoS type attacks. The focus for this paper is network transport, cellular radio access and connectivity, protecting data in motion content and the IoT connected device.

1. Network – Monitoring and responding to network anomalies and device behavior
2. Communications Channel – Encrypting the transport Channel
3. Content – Encrypting the data in Motion
4. Device Access – 2-tier certificate access methodology, as well as user access authentication
5. Physical Device – Tamper detection on the device itself

INTRODUCING TATA COMMUNICATIONS MOVE™ – IOT CONNECT

As organizations embark on their digital journey and as Internet of Things becomes a fundamental component of this journey, mobile networks play a fundamental role. Cellular connectivity is a cost-effective way to reach remote assets or interact with customers, employees, suppliers and business partners in real-time. The transformative effect of IoT adoption calls for radical changes in how mobile network services are consumed and integrated into an organizations' business processes. Success in IoT deployments are also dependent on connectivity trade-offs such as mobile coverage, reliability, security and scalability to meet business critical requirements.

Tata Communications MOVE™- IoT Connect provides a borderless, reliable and secure, things -to-cloud connectivity capability, with a connectivity management wrapper to ensure consistent implementation and continuity.

Tata Communications MOVE™- IOT Connect, aggregates local radio access, across 600+ mobile network operators in 200 countries and territories around the world, connecting things, via a secure, globally deployed IP infrastructure, to enterprise applications in the cloud, including private cloud or major public cloud data center. Tata Communications MOVE™- IOT Connect supports comprehensive connectivity management functionality, to manage all aspects of the IoT connectivity lifecycle.

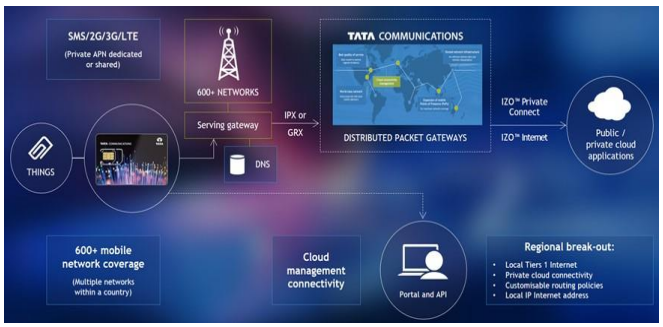


Figure 1: Tata Communications MOVE™ - IoT Connect connectivity overview

SECURITY ELEMENTS RELEVANT FOR TATA COMMUNICATIONS MOVE™

The Industrial Internet Consortium (IIC)[1] defines a security framework for IoT. Many of the aspects associated with this framework are of relevance for Tata Communications MOVE™, including:

* Data-in-Motion protection
* Endpoint Access and Endpoint Identity protection
* Communications & Connectivity Protection

The focus areas are indicated in the diagram below:

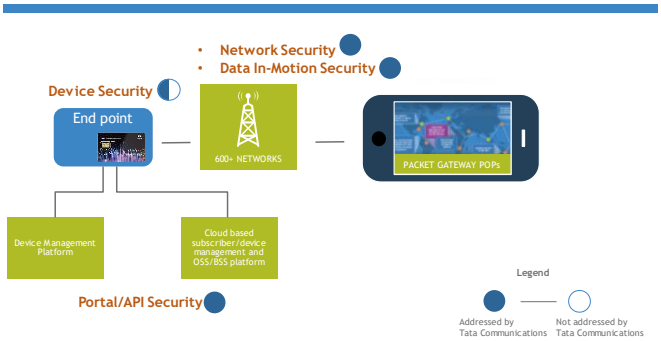


Figure 2: Security focus for Tata Communications MOVE™- IOT Connect

SOME ESSENTIAL PRINCIPLES OF CELLULAR IOT COMMUNICATIONS

Unlike consumer connected devices, such as Smartphones or laptop computers, IOT connected devices tend to follow a strict set of rules about what they can do and how they can do it.

As a rule, the IOT client, which sits in the device, communicates with a defined enterprise IOT service, which sits in a network (or in the cloud). The enterprise IOT service "owns" the device communications and is accountable for gathering information generated by the device as well as ensuring the device's security.

Some major mobile network operators do not provide any specific incremental security capability for IoT connectivity services. The approach that is taken dis-aggregates individual components of the IoT value chain and then relates standard security features to each of these components.

Connectivity management platform vendors offer security around SIM theft/misuse reporting, along with portal security features. Some specialist IoT platform providers take a layered security approach, leveraging SIM based authentication methods which allows for mutual authentication of devices and data analysis systems.

Hardware based root of trust or trusted execution environments are increasingly becoming important in IoT deployments. Several OEMs and semiconductor manufacturers are offering products with these capabilities. A key applications area is the use of software based eSIMs, which save both cost and space for device manufacturers. It is likely that eSIM will herald a new paradigm in terms of commercial IoT services and the agility associated with a software based approach to SIMs.

In terms of network security, approaches center around creating private APNs with private links to the cloud.

In addition to native security capabilities provided by devices, the Tata Communications MOVE™-IoT Connect service includes network-based functions that help establish secure communications. These functions include:

- Over the Air (OTA) Server – OTA provisioning of IoT devices
- Auto Provisioning - in addition to provisioning, manages configuration and operation of IoT devices
- VPN premise-to-cloud services – for secure connectivity to applications in the cloud
- Traffic policing of valid destinations

Typically, provisioning functions serve to provide for the provisioning, configuration and operation of a device, using the SIM to provide the device its identity and authorization keys in the mobile network.

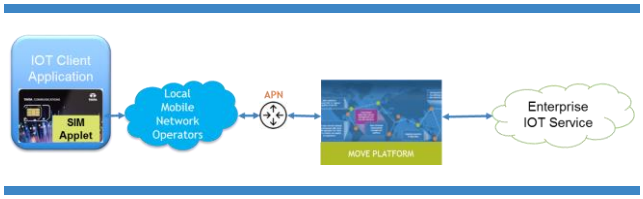


Figure 3: Tata Communications MOVE™- IoT Connect: Connecting devices to enterprise applications in the cloud

The Enterprise IOT Service is often located in a public or private cloud environment and is comprised of several functions that include the:

- Device Manager (DM)
- Data Collection, Analytics and Reporting Applications
- Status and configuration management

[1] http://www.iiconsortium.org/IISF.htm

The DM manages the IOT device itself as an asset in the Enterprise's inventory. The DM is utilized by the Enterprise IT or Logistics and Operations people to track the devices and ensure their correct provisioning.

The Data Collection and Reporting function is typically the Enterprise Application which uses the information gathered by the device to provide a service to the Enterprise. Often, such an application is specific to the type of devices deployed, but the application itself can be constructed using a number of readily available components from public cloud providers. For instance, this application could be a reporting function for a sensor network or a tracking program for fleet or shipping applications, but they may use similar database and reporting tools.

WHY GSM FOR IOT CONNECTIVITY? – SECURITY BUILT-IN

Securing Devices:

• A cellular-connected device equipped with a standard SIM uses hardware ciphering and encrypted key exchanges with trusted network authentication and authorization systems, allowing only authorized devices to connect

• All communications in the IoT architecture (e.g., device-to-device, device-to-cloud) can be regulated from the network, significantly enhancing the overall integrity of the IoT deployment

Securing the Transport Network with GSM Encryption:

• GSM device uses a combination of ciphering keys and encryption algorithms on the SIM itself to securely transmit and receive data

• Two-step encryption and identification process, the two-factor authorization technique makes cellular particularly secure.

Network Security Using GSM Connectivity:

• Provides a standardized and cost-effective approach that creates private networks between the enterprise and its connected devices

• Enterprises can use custom access point names (APNs), as a way to extend the local area network (LAN) out to the remote device This enables enterprises to allocate their own private IP addresses, as well as to specify additional levels of authentication and authorization beyond that provided by the GSM network

THE SIM

In a cellular connected mobile device, the SIM has its own processing environment which is used to establish communications for the SIM. Within this processing environment, the SIM can contain an applet which is used to establish a secure link over which the device can be authenticated within the service. This applet contains code which allows it to establish communications with a cloud environment (Public or Private)

IOT Client Applications running on the IOT Device, will establish secure communications with the public or private cloud using credentials provided by the SIM for communications with the Device Manager and subsequent Data Collection and Reporting Applications.

The diagram below is a representation of the approach that Tata Communications MOVE™ takes to manage SIM and enterprise IoT service relationships.

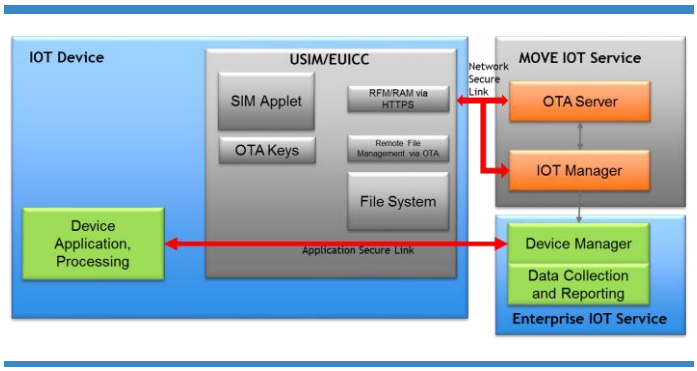


Figure 4: Tata Communications MOVE™ – IOT Connect SIM content and Enterprise IOT Service Relationships

Within the SIM is a processing element, an applet and several files which contain the information required to establish a secure link with very specific services in the network. These files are installed at manufacturing time, and updated via the OTA Server. We discuss these techniques and Tata Communication's unique approach under Content Security below.

VULNERABAILITIES OF IOT DEVICES

The ubiquity of IOT devices exposes the IP network to an ever-increasing threat of attack. Devices gather data, control buildings, manage vehicles, help run power stations and can themselves be turned into dangerous tools.

The two fundamental modes of attack involving IOT devices consist of:

- Attacks on the data generated and consumed by IOT devices
- Using devices as the source of active attacks on Internet resources

Attacks on data are typically done by intercepting content data either in the end points (device or server) or the network (mobile network or Internet).

These data attacks consist of:

- Listening to data (Stealing content)
- Modifying data (Falsifying content)

Using devices as a source of active attacks on Internet resources is known as a Distributed Denial of Service (DDoS) attack. Such attacks are enabled by compromising the software on the device in a way that causes them to send traffic to a destination other than their normal endpoint. This is a particularly troublesome method of attack as it is extremely difficult to pin point and shut down. As more devices enter the network, the effectiveness of these DDoS attacks increases proportionally.

To protect the service, both the Network and the End Device need to be made secure. This means the device must be created, provisioned and deployed in a way that prevents illicit access and any data in motion must be made secure so that it cannot be intercepted. Furthermore, the network path must be made secure in a way that prevents the device from behaving outside its prescribed role.

To accomplish all of this requires an approach which provides multiple layers of security. We view these layers in terms of where and how we monitor and control the IoT device's behavior and communications access:

- Network: Monitoring and responding to device behavior
- Communications Channel: Encrypting the transport Channel
- Content: Encrypting the data in Motion
- Device Access: 2-tier certificate access methodology
- Physical Device: Tamper detection of the device itself

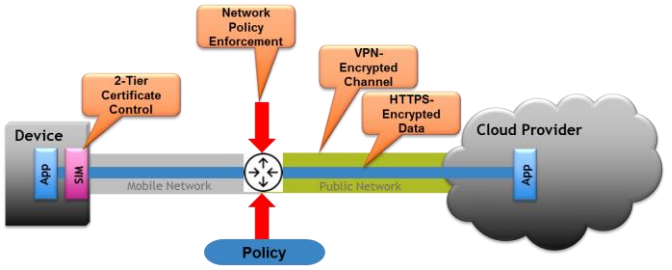


Figure 5: Multiple Layer Security Approach

NETWORK SECURITY

Additional layers of security can always be added to ensure the integrity of an end-to-end IoT channel. This can include additional functionality added at the IOT Packet Gateway (PGW), which is a key location for data collection in the connected system. Without sufficient security measures in the PGW, there is significant potential to introduce cyber-attacks. Loss of a gateway in the communication chain, can jeopardize integrity of the end-to-end IoT communication ecosystem, because the gateway acts as a bridge between the edge devices and applications in the cloud. Techniques including Deep Packet Inspection and DDoS protection can be added at the PGW.

A well-behaved device will act in a very predictable way. The device will only attempt to access its service-side endpoint at its appointed time. This predictability in behavior is a key advantage in securing IoT networks.

When a device is not behaving in the expected way, it might be because the device is faulty or compromised. These conditions are detectable by applying policies in the network which can apply to a specific device, device type or APN. Such policies can include time of day, source or destination address, volume and content-related parameters which can immediately prohibit a device from deviating from its prescribed behavior and provide the information which will allow the service to quickly react to the situation.

Tata Communications MOVE™ packet core network is instrumented with advanced policy enforcement (PCEF) capabilities which can be configured to prevent compromised devices from participating in an IoT network.

As part of the Tata Communications MOVE™ service offering, each Enterprise's IOT assets can be restricted to only communicate to its designated service-side endpoints. Any attempt to communicate elsewhere can be:

- Blocked: From reaching unauthorized endpoints
- Logged: With additional network and device data
- Alerted: To monitoring services and security personnel
- Removed: From the network to prevent further mischief

COMMUNICATIONS CHANNEL SECURITY

Traffic flowing across the public internet, to and from the Tata Communications MOVE™ Service is inherently vulnerable. Using a VPN offers a degree of security against Man-in the Middle attacks, but to be able to truly hide a network and its assets, we utilize a capability from NetFoundry, that removes the need for VPN altogether. Tata Communications incubation company **NetFoundry**, provides additional levels of security with carrier agnostic, secure, application-to-application private connectivity (referred to as APP-WAN) on-top of the public Internet, across any mix of access networks – with military-grade security, manageability and reliability, extensible for unique market needs. NetFoundry applies an approach called 'Zero Trust' data-centric network design, placing micro-perimeters around specific data or assets so that more-granular rules can be enforced, thus preventing lateral movement of an attack through a network.

With NetFoundry an IoT Administrator can 'spin-up' secure IoT communication channels on-demand and at massive scale. With this approach IoT deployments use existing Internet connection to access NetFoundry's managed global core infrastructure, with secure access to any global location. NetFoundry Networks provide rigorous enterprise grade security and performance across the public Internet, independent of the diverse clouds and other endpoints that they connect. NetFoundry helps to disguise IoT traffic paths, by bifurcating the data paths, thus preventing predictable IoT device usage patterns, from exposing vulnerabilities.

When a mobile endpoint communicates to an application located in either a public or private cloud a portion of the communications path must transit an internet connection. By providing a secure private network path via Tata Communications IZO™ cloud connect services, we can help provide protection over Public Network paths.

Using a suite of tools enabled via Tata Communications IZO™ service, an Enterprise customer can select and configure a secure endpoint within their cloud account which will terminate a secure IZO™ connection over the Internet. When combined with Tata Communications MOVE™-IoT Connect APN, the Enterprise Customer can be assured of a private, end to end channel for their entire Mobile communications solution.

Above and beyond this level of security, Tata Communications MOVE™-IoT Connect also offers Static and Private IP addressing options that will enable large IOT network topologies which can operate behind the corporate firewall. This improves inventory control and security, allowing the Enterprise to apply its own rules to its IOT assets.

CONTENT SECURITY

Securing data in motion requires a set of security credentials which can be used to encrypt the data at the transport layer protocol. The most common protocol security utilizes Transport Layer Security and its predecessor Secure Sockets Layer (TLS/SSL). TLS is the cryptographic protocol used to convert standard, unsecured HTTP browser sessions into Secure HTTPs browser sessions.

TLS/SSL are cryptographic protocols which harness symmetric cryptography using keys which are unique for each connection. The keys are based on shared secret information which is exchanged at the start of each session by the endpoints. Typically, at least one of these endpoints are authenticated using a public-key cryptography using a digital certificate. These digital certificates are usually 'signed' by a trusted Certificate Authority (CA).

Note, however, that we stated that keys are unique to each connection. In our model in figure 2, we see at least two connections. One of these is a secure connection established to the OTA Server (located in the network of the Tata Communications MOVE™ platform) and the other is to the public or private cloud containing the Enterprise IOT Service.

The most common transport protocols used by IOT device (MQTT, CoAP, AMQP, etc.) require an encryption scheme to provide full end to end security. The challenge in mobile environments comes from the fact that when a SIM is created, there is no way of knowing the keys required for the secure communications to the particular public or private cloud which will be used by the enterprise.

In an ordinary mobile service, the security credentials for the Enterprise IOT Service would need to be exchanged over the mobile network, with the Client Application prior to having a secure channel over which to exchange. Alternatively, a manufacture could create and install the credentials in the device (along with the applications and software) as the devices are being manufactured, but this is both cumbersome and expensive.

For Tata Communications the priority is to secure the end to end mobile communications channel in a way that allows the Enterprise to exchange their own keys for the Enterprise IOT Service without the vulnerability of exposing the credentials over a potentially insecure connection.

When a SIM is issued for a Mobile Device, it includes a set of secure identifiers which are used for establishing communications over the mobile network, as well as to 'well-known' network endpoint(s). In terms of the Enterprise to which the SIM is allocated, some of the secure identifiers provided can be used by the Enterprise applet at start-up for the purposes of establishing secure communications to specific endpoints.

With Tata Communications MOVE™-IoT Connect, one of these network endpoints is a Certificate Server (IOT Manager) which is used to provide a second set of secure identifiers using a secure channel which is established by the first set of secure identifiers. Upon first use, the SIM will employ its initial set of security credentials to set up a secure channel to the OTA server to obtain this second set of files containing the security credentials for the Enterprise Cloud (Public or Private) environment.

Once the SIM has securely obtained the second set of Credential files, the Client Application can extract these files from the SIM and use them to establish an end to end secure channel (via HTTPs) to their Enterprise IOT Service cloud provider. This secure channel can now be used to create a secure communications path for the Client application.

This two-tiered approach greatly improves the service security because we establish system independence between the SIM management portions of the service (Network-based) and the application portions of the service (Enterprise public or private cloud). We also allow the downloading of the initial credentials over a secure channel, so these keys cannot be intercepted.

The Customer never sees the Tata Communications MOVE™-IoT Connect certificate and the customer can provide their own certificates for their chosen cloud (Public or Private) provider.

Note that by providing their own certificates, the enterprise not only restricts the destinations that the device can speak to but also contains the span of 'trust,' making it easier for security personnel to manage the overall service.

DEVICE SECURITY

Tata Communications does not extend its security scope to the physical protection of IOT assets from being intercepted and modified for malicious purposes. This does not mean that we are not able to deploy tools and techniques to detect such modifications and block them.

A common infiltration technique involves removing the SIM and placing it into another device. Every SIM has its own serial number imprinted on it known as the Integrated Circuit Card Identifier (ICCID). Each device's modem has a serial number known as the International Mobile Equipment Identity (IMEI). The Tata Communications MOVE™ IOT Manager performs a match on first use wherein the device IMEI is matched to the assigned ICCID for that device. This pair is matched upon first use with 3 options of management which can be exposed to the Enterprise Operations manager in a way that allows:

- Exact matched pair - Any mismatch detected will deny the SIM from accessing our network and both credentials must be checked in any data to be collected for that device.
- ICCID Primary – Allows the data to be collected for that device in the cloud with the ICCID.
- IMEI primary – Allows the data to be collected for that device in the cloud with the IMEI.

Another technique used to hijack data is to gain access to the device application with the intent of altering the route of the device data. In this case the intent is to possibly manipulate the data to spy on content collected by the device or to use the device as part of a Distributed Denial of Service (DDoS) attack on other network entities. In these cases, the Mobile Packet Core Network policy methods mentioned earlier are used to detect such attempts and deny the device such alternate paths.

Tata Communications MOVE™-IoT Connect uses a technique called SIM bootstrapping for device authentication and communication security at the transport layer. This approach to SIM management creates strong session keys between devices and data analysis systems. The use of SIM bootstrapping lets mobile communications service providers create symmetric encryption security, with mutual authentication at both device and enterprise server level.

CONCLUSION

Security is critical to any enterprise IoT service strategy. IoT assets are quite often located outside of the physical premises of an organaisation and can be exposed to both remote and physical tampering.

We have reviewed four layers of security protection:

1. Network – Monitoring and responding to device behavior
2. Communications Channel – Encrypting the transport channel
3. Content – Encrypting the data in motion
4. Device – 2-tier certificate access methodology and tamper detection

By establishing communications policies and security which not only protects IoT data, but monitors and restricts device behavior, Tata Communications MOVE™-IoT Connect, with associated Tata Communications services including IZO™ and NetFoundry can secure IOT implementations, such that IoT projects can be commissioned and deployed in the knowledge that there are multiple layers of security in place to protect the data that is being generated and the enterprise that is using the service.

APPENDIX - GSMA AND IOT SECURITY

Network Security

GSMA guidelines relating to network security for mobile network operators

- Mobile Network Operators should implement Extended Access Barring (EAB) to protect against signalling storms/attacks
  - EAB configuration can be performed in the UICC or the endpoint device itself
  - Mobile Network Operators are thus able to restrict network access to devices configured for EAB
- GSMA's Fraud and Security Group (FASG) is a forum for Mobile Network Operators to share fraud/security information and incident details
- GSMA's Authentication and Encryption Algorithms for security of 2G/3G and 4G systems
  - Mutual authentication occurs (the Endpoint device is authenticated by the network and the network is authenticated by the device). Use MILENAGE authentication and integrity encryption algorithms. Mobile Network Operators should consider the support of TUAK Authentication algorithm.
- Network Operator should implement backhaul encryption

Data Security

GSMA guidelines on data security for mobile network operators

- Mobile Network Operators should ensure that data that transits the public network is encrypted between the point data enters the public infrastructure to the point it leaves the network
- Mobile Network Operators can provide private networks where dedicated communication channels are provided for the use of a single customer to ensure that no data traverses a public network. Private networks can be created by:
  - Use a tunnelling protocol such as Layer 2 Tunnelling Protocol (L2TP) and secured using protocols such as Internet Protocol Security (iPsec)
  - Creating a dedicated network for the IoT Service by deploying a separate instance of the core network with shared radio network

Additional GSMA Security Guidelines

- Mobile Network Operators who process data need to sign a Data Processing Agreement (DPA) with the IoT service provider
- Mobile Network Operator members are expected to operate their networks under the terms of the licenses issued by their national regulators, thus compliance with local security requirements relating to IoT is expected
- Mobile Network Operators should source their UICCs from manufacturers whose manufacturing and provisioning processes are accredited according to the GSMA's Security Accreditation Scheme
- Mobile Network Operators should implement IoT endpoint device blacklisting and connection to the GSMA Central Equipment Identity Register database
- GSMA's Mobile Connect Initiative and OpenID Connect and ETSI MSS are examples of multi factor authentication enablers that can enable an IoT Service Provider to obtain additional authentication and information from their end

Tata Communications Limited
VSB, Mahatma Gandhi Road,
Fort Mumbai, 400 001
India

About Tata Communications

Tata Communications Limited (CIN no: L64200MH1986PLC039266) along with its subsidiaries (Tata Communications) is a leading global provider of A New World of Communications™. With a leadership position in emerging markets, Tata Communications leverages its advanced solutions capabilities and domain expertise across its global and pan-India network to deliver managed solutions to multi-national enterprises, service providers and Indian consumers.

The Tata Communications global network includes one of the most advanced and largest submarine cable networks and a Tier-1 IP network, as well as nearly 1.5 million square feet of data centre and collocation space worldwide.

Tata Communications' depth and breadth of reach in emerging markets includes leadership in Indian enterprise data services and leadership in global international voice.

Tata Communications Limited is listed on the Bombay Stock Exchange and the National Stock Exchange of India.

www.tatacommunications.com | @tata_comm
http://tatacommunications-newworld.com | www.youtube.com/tatacomms

For more information, visit us at www.tatacommunications.com.

Contact us

Share