IOT-Security and Privacy
ITU-APT Program
on
30-10-2018

By

Shailendra Kumar Sharma

DDG Smart Networks, TEC, DoT

IOT-Security and Privacy

Hearty Welcome
To all the Participants
In the
ITU-APT Program
Conducted by
ALTTC

IOT-Def

- **Internet of Things [b-ITU-T Y.2060]:**
- **A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.**

Points Addressed

- Concept of Trust
- IoT/M2M Security Threats
- Understanding the potential threats in IoT/M2M environment
- Frauds and attacks in IOT/M2M systems
- Challenges in IoT/M2M Security
- Challenges - Security of Embedded Systems
- Challenges – Security
- Challenges - Authentication and Authorization

Points Addressed

- Challenges - Heterogeneity and Resource Constraints
- Challenges - Privacy and its Preservation
- Challenges – Identity, Anonymity and Liability
- Mitigation of IoT/M2M Security Threats and Risks
- Address Security Early: Threat Modelling
- Build Security In
- Securing IOT/M2M-Security features and counter measures

Points Addressed

- **Potential risks in ICT infrastructures**
- Complexity of ICT Infrastructure
- Understanding of Trust
- Trust in ICT Environment
- Attributes of Trust
- Relationship between Security Privacy and Trust

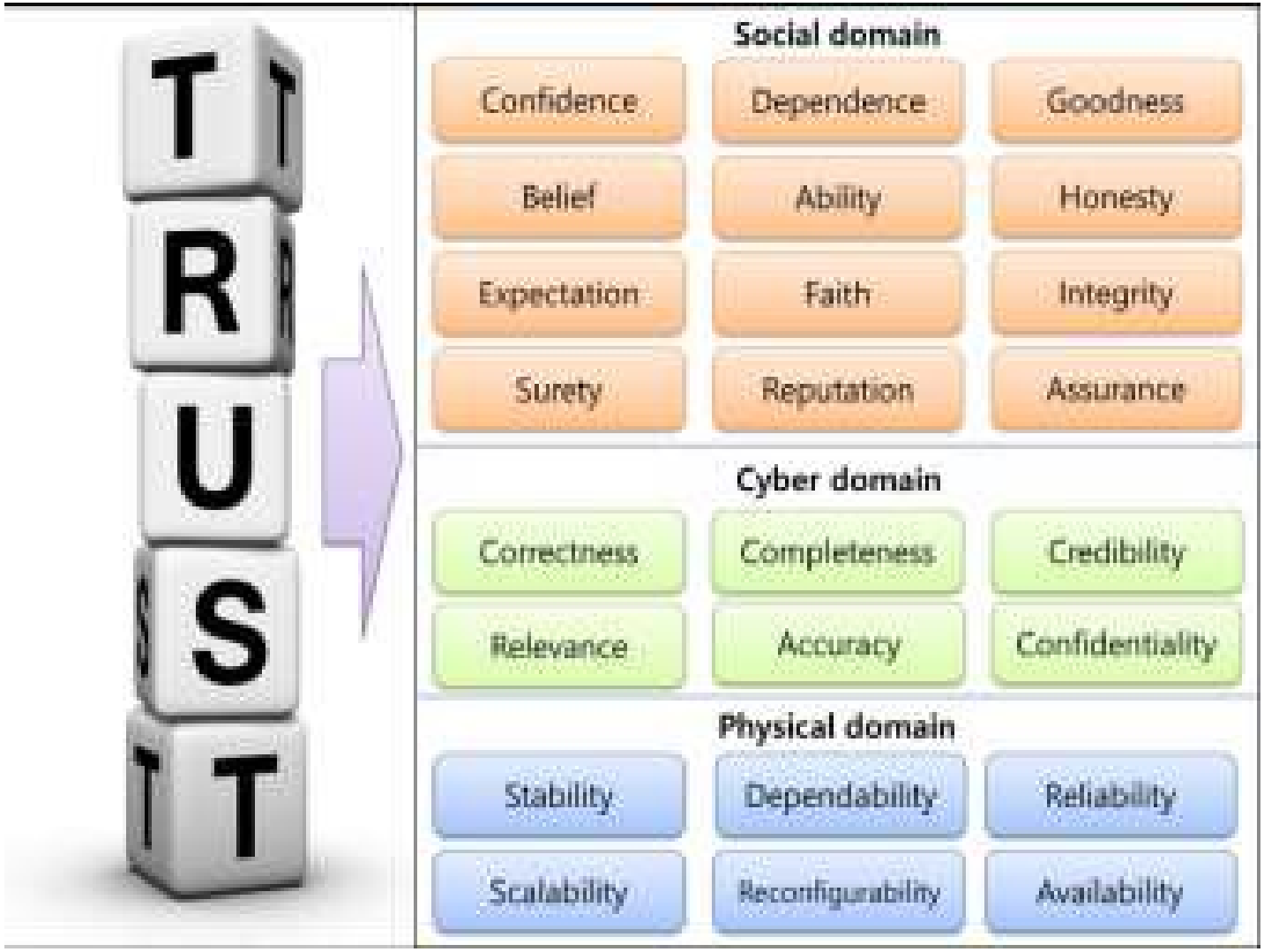
ITU-Def

- **Trust: Trust is an accumulated value from history and the expecting value for future. Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of physical components, value-chains among multiple stakeholders, and human behaviours including decision making.**
- NOTE 1 - Trust is applied to social, cyber and physical domains.
- NOTE 2 – Trust [ITU-T X.509]: Generally, an entity can be said to "trust" a second entity when it (the first entity) assumes that the second entity will behave exactly as the first entity expects. The key role of trust is to describe the relationship between an authenticating entity and an authority; an entity shall be certain that it can trust the authority to create only valid and reliable certificates.

ITU-Def

- NOTE 3 – Trust [ITU-T X.1163]: The relationship between two entities where each one is certain that the other will behave exactly as it expects.
- NOTE 4 – Trust [ITU-T X.1252]: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.
- NOTE 5 – Trust [ITU-T Y.2701]: Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.
- NOTE 6 – Trust [ITU-T Y.2720]: A measure of reliance on the character, ability, strength, or truth of someone or something.

Attributes of Trust



Relationship among security, privacy and trust

- **Security: systems need a variety of methods to prevent behaviours with malicious intents. Security mainly concerns technological aspects such as the confidentiality, availability and integrity. It also includes attack detection and recovery/resilience.**

Relationship among security, privacy and trust

- **Privacy: users need the protection of their personal information related to their behaviours and interactions with other people, services and devices. Privacy mainly concerns user aspects to support anonymity and restrictive handling of personal user data.**

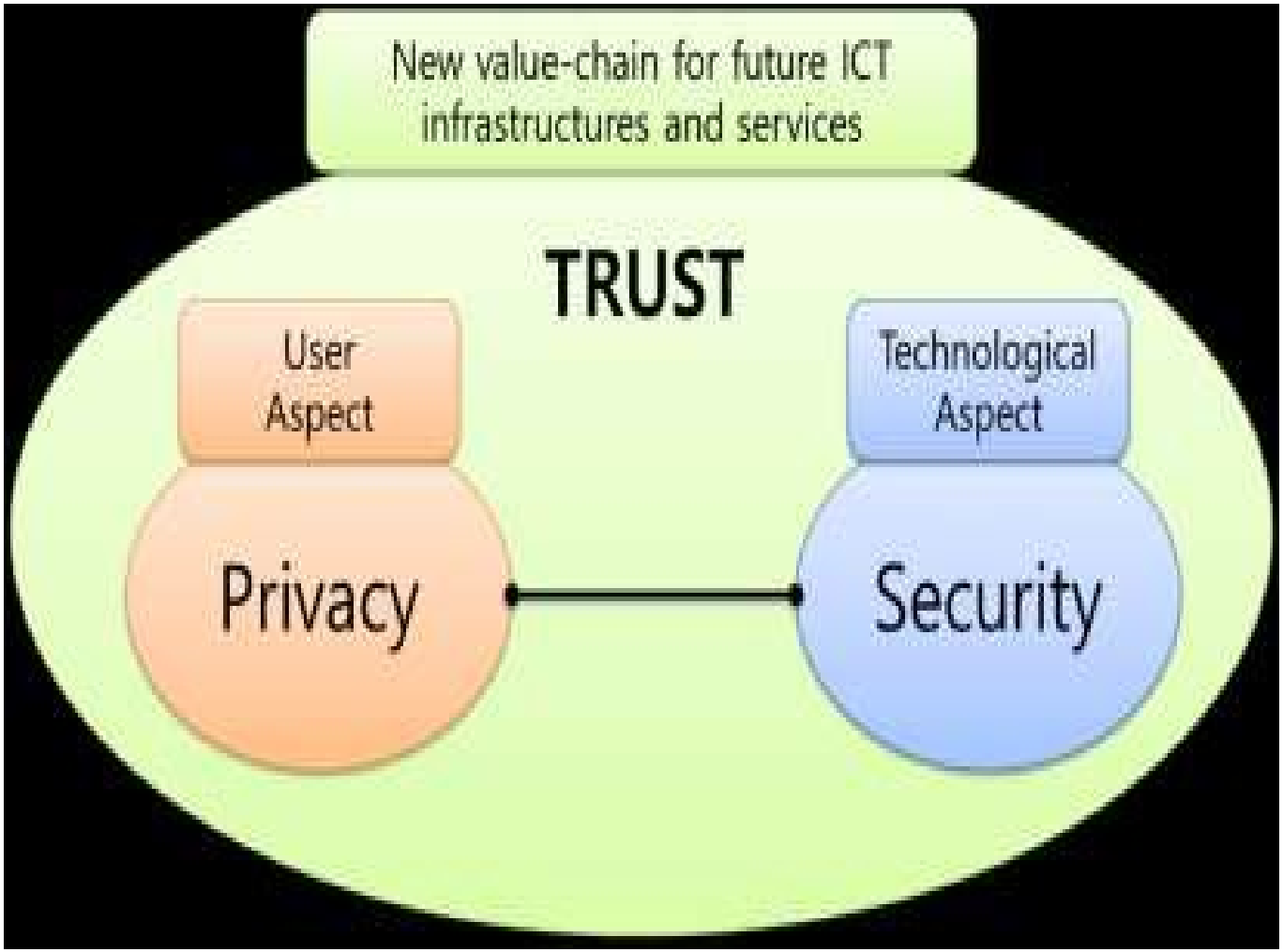
Relationship among security, privacy and trust

- **Trust: trust is broader concept that can cover security and privacy (Figure in next but one slide). Trust revolves confidence that people, data, devices will function or behave in expected ways. Trust can be used to build new value-chain for future ICT infrastructure and services.**

Relationship among security, privacy and trust

- For example, security and privacy have controlled a system and data securely in social-cyber-physical domains. However, traditional secure system concerns about how to authorize the entities as well as how to provide data to the authorized entities. Trust can give reliability to security and privacy as a parameter by measuring a discrepancy between observation and objective or subjective expectation of the reliable entities and data.

Relationship among security, privacy and trust



IOT- Security -NUTSHELL

A. Scale of IOT - 2015: 15Bn > 2020: 31Bn > 2025: 75Bn > 2030: 125 Bn (Gartner)

B. Security in IOT comprises of

1.End Point Devices Security
2. Network Communication Security
3. Application Level Security
4. Service Layer Security

Implementing above four security basically leads to Trusted Environment wherein the end user trusts the IOT Ecosystem.

1. Trust in ICT Environments
2. Physical Domain trust
3. Cyber trust
4. Cross-domain service trust

C. IOT - Security >> data / Information Security
Maintain

1. Confidentiality – of data / Information
2. Integrity - " "
3. Availability - " "
4. Accountability - " "
5. Audit ability - " "

D. Some IOT Standards

1. Industrial Internet Consortium (IIC) - : Industrial Internet of Things, Volume G4: Security Framework
2. IEEE Internet of Things – IEEE P-1363, P – 1619, P-2600, P-2413, 802.1AE, 802.1X
3. International Electrotechnical Commission (IEC) - IEC/TR 62443-2-3, "Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment.
4. International Organization for Standardization (ISO) - — Internet of Things Reference Architecture (IoT RA)
5. Cloud Security Alliance -
6. Internet Engineering Task Force (IETF) –
7. ITU-T SG20
8. 3rd Generation Partnership Project (3GPP):
9. oneM2M etc

•

IOT-Security

- The future of IoT/M2M cannot be realized without addressing security and privacy risks and policy issues.
- Securing and protecting the things that matter most—our systems, our data, and our privacy—is a shared responsibility.
- Security and privacy must become part of every product's feature set.

IOT-Security: Affected Stakeholders

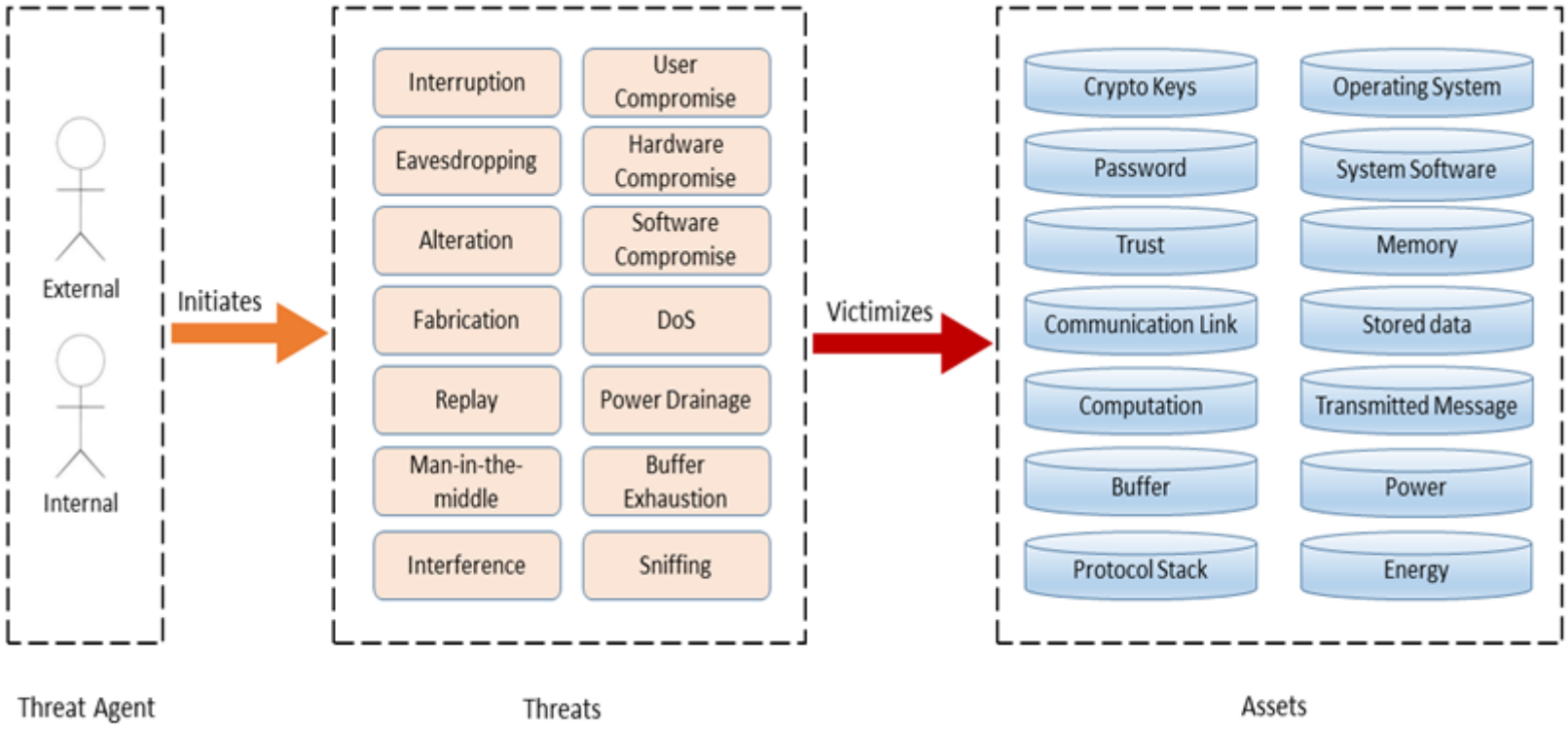
- The Following stakeholders are affected by the IoT/M2M Security threats
- M2M Application Service Provider;
- Manufacturer of M2M Devices and/or M2M Gateways;
- M2M Device/Gateway Management entities;
- M2M Service Provider;
- Network Operator
- User/Consumer

Understanding the potential threats in IoT/M2M environment

- In a completely closed network, like in a verticalized captive use case, security risks are minimal. But, as M2M embedded systems become IP-enabled and interconnected the attack surface becomes open to threats. Services provided by the IOT/M2M System to IOT/M2M applications establish the need for trusted security credentials to secure connections between applicative entities, including the other involved functions.

Understanding the potential threats in IoT/M2M environment

- An understanding of the potential threats in the IoT environment has been broadly shown in the Figure on next slide, whereby various internal/external threat agents initiating threat by virtue of interruption, eavesdropping, buffer exhaustion, software/hardware compromise etc. which victimizes the various assets (like memory, crypto keys, buffer, power, energy etc.) and may cause malfunctioning of these assets.



Source: http://secret.cis.uab.edu/research/iot-security/

Understanding the potential threats in IoT/M2M environment

- The devices and the control platform on which data may be consumed and shared could have different ownership, policy, managerial and connectivity domains. Consequently, devices will be required to have equal and open access to a number of data consumers and controllers concurrently, while still retaining privacy and exclusivity of data where that is required between those consumers.

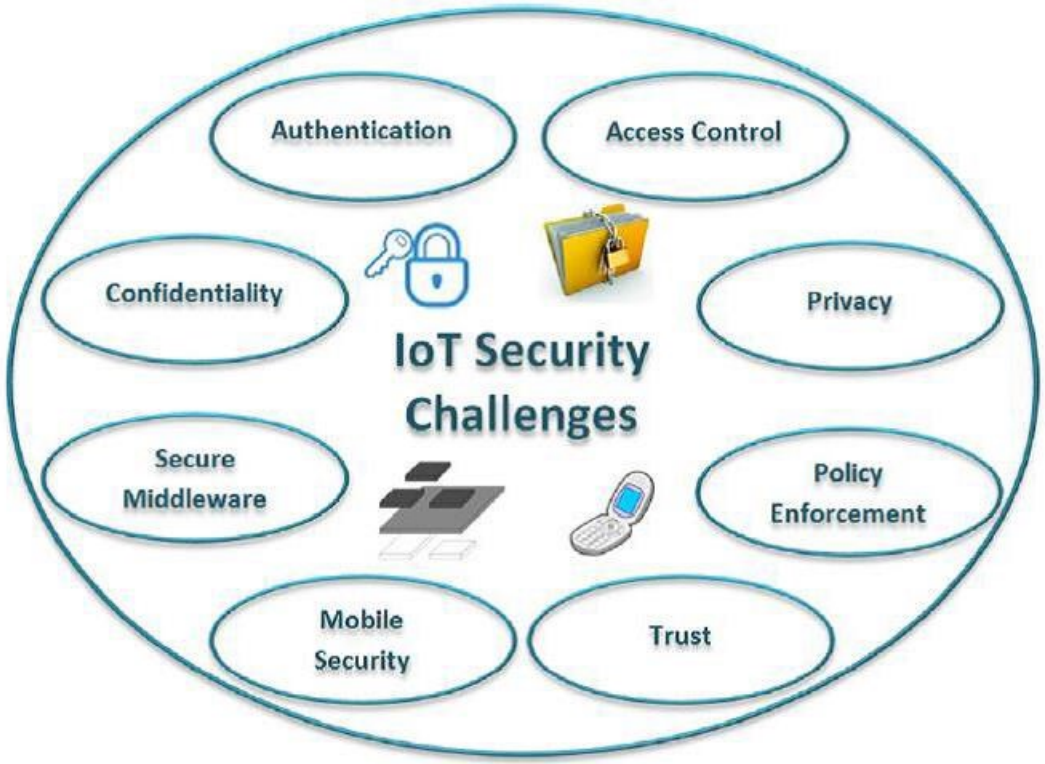
Understanding the potential threats in IoT/M2M environment

- There are seemingly competing, complex security requirements to be deployed on a platform with potentially limited resources, which are enumerated below:
- Authenticate to multiple networks securely
- Ensure that data is available to multiple collectors
- Manage the contention between that data access

Understanding the potential threats in IoT/M2M environment

- The IoT can be affected by various categories of security threats including the following:
- Common worms jumping from ICT to IoT
- "Script kiddies" or others targeting residential IoT – Home control
- Organized crime: Access to intellectual property, sabotage, and espionage
- Cyber terrorism

Challenges in IoT/M2M Security



Challenges - Security of Embedded Systems

- In addition to the unique risks for M2M systems, embedded systems in general contain inherent security risks
- Many of the embedded systems in place today are unlikely to be connected to a network 100 percent of the time. Inconsistent or intermittent network connectivity increases the chances of a device connecting to an unsecured network. If an embedded system is online only occasionally, it is more likely to be dependent on a single node for network access, which creates a single point of failure or attack. Additionally, devices with only occasional connectivity are more difficult to monitor for issues and more difficult to troubleshoot and upgrade.

Challenges - Security

- The IoT is where the Internet meets the physical world. A major disruption of the traditional model for the new brings its own set of challenges. The following lists some security challenges and considerations in designing and building IoT devices or systems:
- Typically small, inexpensive devices with little or no physical security.
- Though inexpensive, every device still has to compute something and also have some security feature. Also, it should not to latency in processing

Challenges - Security

- Computing platforms, constrained in memory and compute resources, may not support complex and evolving security algorithms due to the following factors:
- Limited security computes capabilities.
- Encryption algorithms need higher processing power
- Low CPU cycles vs. effective encryption
- Designed to operate autonomously in the field with no backup connectivity if, primary connection is lost.

Challenges - Security

- Mostly installed prior to network availability which increases the overall onboarding time.
- Requires secure remote management, up-dating during and after onboarding.
- Scalability and management of billions of entities in the IoT ecosystem.
- Identification of endpoints in a scalable manner, Sometimes the location may be more important than the individual identifier (ID).
- Management of Multi-Party Networks

Challenges - Security

- The IoT entities will generally not be a single use, single ownership solution. Consequently, Identification and authorization of M2M devices in a dynamic and autonomous world will pose serious research challenges. Authentication mechanisms should work side-by-side with distributed trust management and verification mechanisms. Any two M2M devices should be able to build and verify a trust relationship with each other, and this problem is certainly more challenging in environments without a security infrastructure in place. Trust will be an important requirement for designing new identification and authentication systems for M2M.

Challenges - Security

- As authentication is related with identification, M2M systems will probably need to incorporate some type of secure identifier, tying information identifying the device or application with secret cryptographic material. Current proposals point to the usage of ITU-T specified X.509-based certified secure identifiers, for example using IEEE 802.1AR, or on the other end of self-generated uncertified secure identifiers, also called cryptographically generated identifiers, for example, the use of private keys in GSM Network authentication.

Challenges - Security -Privacy

- As M2M systems require that privacy is balanced against disclosure of information, new authentication mechanisms relying on appropriate secure identifiers and incorporating privacy-preserving mechanisms are required. This aspect may also be incorporated in new trust computation mechanisms, as the evaluation of the risk in accepting communication with a partially unknown device may also consider the level of privacy accepted for an M2M application.

Challenges - Security -Trust

- As distributed and autonomous trust mechanisms will be required for M2M environments, trust must be established on an M2M device from the start. Local state control via secure boot (local trust validation) may be enforced for M2M devices, similar to the mechanisms previously analyzed in the context of the ETSI M2M architecture. This secure boot may allow the establishment of a trusted environment providing a hardware security anchor and a root of trust, from which different models for trust computation may be adopted. In this context, the Trusted Computing Group (TCG) has proposed autonomous and remote validation models.

Challenges - Authentication and Authorization

- **Authentication**
- At the heart of IOT secure framework is the authentication layer, used to provide and verify the identify information of an IoT entity. When connected IoT/M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device. The way to store and present identity information may be substantially different for the IoT devices. Note that in typical enterprise networks, the endpoints may be identified by a human credential (e.g., username and password, token or biometrics).

Challenges - Authentication and Authorization

- **Authorization**
- The second layer of this framework is authorization that controls a device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity. With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information. For example, a car may establish a trust alliance with another car from the same vendor.

Challenges - Heterogeneity and Resource Constraints

- Given the limitations on the computational capabilities of many sensing and actuating platforms, security technologies must be developed to cope with and supported by architectures with the characteristics similar to the ETSI M2M architecture. For example, applications using passive Radio-Frequency Identification (RFID) tags are unable to support security mechanisms requiring the exchange of many messages and communication with servers on a network domain.

Challenges - Privacy and its Preservation

- Privacy is one of key importance nowadays. People are concerned about their personal data that is on the internet. The right to privacy in India has developed through a series of decisions over the past 60 years. In an unanimous judgment by the Supreme Court of India (SCI) in Justice K.S. Puttaswamy (Retd) vs Union of India, in August 2017, has ruled that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

Def and understanding-Privacy

- Defining privacy is no easy task, as the concept is an elusive one. It incorporates multiple perspectives (legal, technical, sociological) and is culturally, politically and historically "bounded".
- An increasingly pervasive internet also raises important socio-ethical concerns that are worth considering.

Def and understanding-Privacy

- The debate surrounding privacy in a ubiquitous Internet of Things hinges upon
- an individual's ability to control the blurring boundary between the public and private spheres, and to
- determine who can access his/her private sphere and under what conditions.25 Privacy has been defined by
- scholars as "the power to control what others can come to know about you"26 and "the right to determine
- how, when and to what extent data about oneself are released to others."27

Def and understanding-Privacy

- The concept of privacy often leads to discussions about anonymity. Although they are related, privacy and
- anonymity have some important differences. In communications, privacy implies possession of and control
- over personal information and the terms and conditions under which it is used, stored, or disclosed to others.
- Anonymity, on the other hand, implies the absence of information about the identity of a person, and relates
- to the terms and conditions under which such information might be collected – e.g. a person can be
- “anonymous” on the internet by using programs that disable cookies or hide the geographic location of the
- user.

Challenges - Privacy and its Preservation

- Enterprises try to protect their information, communication and application infrastructure, causing them to have private mail servers, data storages etc. Privacy can be divided into a few categories that have unique technical aspects:
- Communication privacy
- Position privacy (Location privacy)
- Path privacy
- Identity privacy (Personal privacy)
- Personal data, Local information privacy (use crypto for data protection)

Challenges - Privacy and its Preservation

- Sticky policies are a way to cryptographically associate policies to encrypted (personal) data. These policies function as a gate keeper to the data. The data is only accessible when the stated policy is honoured. System keeps track of personal data relating to the user, as well as applied policies and service customizations.

Challenges - Privacy and its Preservation

- For some M2M applications (in the context of the IoT) the user will require to be able to control the amount of personal information exposed to third parties, for instance in maintaining privacy while exposing personal records in healthcare applications. On the other end, other M2M applications may require that some of that information is available in case of necessity, for instance with M2M vehicular applications in case of traffic accidents.

Challenges - Privacy and its Preservation

- **Privacy Preservation**
- Preservation of privacy has been a concern since the dawn of the Internet. IoT will exacerbate the problem because many applications generate traceable signatures of the location and behaviour of the individuals. Privacy issues are particularly relevant in healthcare, and there are many interesting healthcare applications that fall within the realm of IoT. In this environment, it is essential to verify device ownership and the owner's identity while decoupling the device from the owner.

Challenges - Privacy and its Preservation

- . Shadowing is a mechanism that has been proposed to achieve this. Identity management in the IoT may offer new opportunities to increase security by combining diverse authentication methods for humans and machines. Privacy and compliance are intertwined and are under the purview of country regulation

Privacy-Aadhaar-SC Verdict

YOU AND YOUR AADHAAR

A five-judge Bench of the Supreme Court has upheld by a 4-1 majority the validity of the Aadhaar Act, putting the seal of approval on the world's largest biometric identification exercise. The judgment, has, however, read down a few aspects of the Act, and struck down several significant — and controversial — provisions.

PRANAV MUKUL
NEW DELHI, SEPTEMBER 26

WEDNESDAY'S SUPREME Court Aadhaar ruling has highlighted two main aspects of the unique identification project — one, Aadhaar as digital identity infrastructure and, two, its application as public infrastructure for various purposes. On the first aspect, the majority judgment has upheld the validity of the project, and stated that the architecture of Aadhaar, and the provisions of the Aadhaar Act, do not tend to create a surveillance state. However, the judgment has also red-flagged several applications of Aadhaar that do not meet the test of proportionality, such as the linking of Aadhaar with mobile number and bank accounts, and declared them unconstitutional.

Fears have been expressed that Aadhaar had created, or could create, a surveillance state. What has the court said?

The majority verdict of four judges says the manner in which the Aadhaar project operates, ensures that the provisions of the Aadhaar Act "do not tend to create a surveillance state". During the enrolment process, "minimal biometric data in the form of iris and fingerprints is collected", and the Unique Identification Authority of India (UIDAI) — which oversees the Aadhaar enrolment exercise — "does not collect purpose, location or details of the transaction". The suggestion that Aadhaar would create a surveillance state was "not well founded", the judgment says, "and in any case, taken care of by the diffluence exercise carried out with the striking down certain offending provisions in their present form".

Linking of bank accounts and all other financial instruments such as mutual funds, credit cards, insurance policies, etc with Aadhaar were mandatory as part of the 2017 amendment brought to Rule 9 of the Prevention of Money Laundering Act (Maintenance of Records) Rules, 2005. The Supreme Court has now declared the amendment unconstitutional. It did so because the amendment did not stand the proportionality test in the triple test, thus violating the right to privacy of a person which extends to banking details. The court cited *Ram Jethmalani & Ors vs Union of India & Ors* (2012), in which it held that revelation of bank details without *prima facie* grounds of wrongdoing would violate the right to privacy. It also noted that under the garb of prevention of money laundering or black money, there cannot be such a sweeping provision which targets every resident of the country as a suspicious person. "Presumption of criminality is treated as disproportionate and arbitrary," the judgment said, declaring the amendment unconstitutional.

But what happens to all the Aadhaar details that people have already given to banks?

The issue of the right to be forgotten, in case of Aadhaar data that have been collected, remains a grey area. The judgment does not clearly state that entities such as banks and mobile companies will have to delete the collected information. On a similar issue, the court has upheld the validity of Section 59 that also validates all Aadhaar enrolment done prior to the enactment of the Aadhaar Act, 2016. The court has said that since enrolment was voluntary in nature, those who

Privacy-Aadhaar-SC Verdict

In his minority judgment, Justice D Y Chandrachud said that from the verification log, it was possible to locate the places of transactions carried out by an individual over the past five years. The majority verdict has, however, said that authentication logs should be deleted after six months, instead of the five years required under the existing regulations. Justice Chandrachud also noted that it was possible to track an individual's location through the Aadhaar database, even without the verification log. "The architecture of Aadhaar poses a risk of potential surveillance activities through the Aadhaar database," he said.

The second big concern has been about the security of the biometric data. What view has the court taken on the magnitude of protection accorded to the collection, storage and use of such data?

The majority judgment underlines that UIDAI has mandated only registered devices to conduct biometric-based authentication transactions. With the use of these registered devices, the biometric data is encrypted within the device using a key, and is, therefore, captured live. Before returning to the application being used by the service provider, the registered device blocks the personal identity data by encrypting it. This creates a unidirectional relationship between the host application and the UIDAI. The use of registered devices in Aadhaar authentication, therefore, rules out any possibility of the use of stored biometric, or the replay of biometrics captured from another source. Further, as per the regulations, authentication agencies are not allowed to store the biometrics captured for Aadhaar authentication.

cessful implementation of programmes — in the absence of a credible system to authenticate identity, it was becoming difficult to ensure that subsidies, benefits and services reached their intended beneficiaries. Also, given that the use of Aadhaar had increased over time, necessary measures were taken to ensure security of information provided by individuals while enrolling.

However, the judgment has questioned certain provisions of the Act on the grounds of privacy. Section 57 is one example — it has said that the provision which enables corporate bodies and individuals to also seek authentication, that too on the basis of a contract between the individual and such bodies or persons, would impinge upon the right to privacy of the individual.

The judgment has looked at Section 139AA of the Income Tax Act, 1961 — which made Aadhaar mandatory for filing returns and applying for PAN — in the context of the right to privacy, and said that the provision satisfied the triple test: (i) existence of a law, (ii) a legitimate state interest, (iii) test of proportionality. The court also said that if in the regulations, a provision was made that impinged upon the right to privacy, it could be challenged.

What has the court said about Aadhaar for children? Will it be essential for admission to school?

The consent of parents/guardians will be essential for the enrolment of children under the Aadhaar Act, and "on attaining the age of majority, such children... shall be given the option to exit from the Aadhaar project if they so choose in case they do not intend to avail the benefits of the scheme".

With regard to school admissions, the

AADHAAR IS...

NOW NOT NEEDED FOR

- Employee pension
- Admission to school
- Taking CBSE, NEET, JEE, UGC exams
- Re-verification of mobile number
- Bank accounts
- Mutual fund investments
- Insurance policies
- Credit cards
- New/existing post office schemes
- New/existing NSC accounts
- New/existing PPF accounts
- New/existing Kisan Vikas Patra accounts

STILL NEEDED FOR

- PAN card
- National Child Labour Project (NCLP)
- Scholarships for school students, such as National Means-cum-Merit Scholarship Scheme, National Scheme of Incentive to Girls for Secondary Education, Inclusive Education of the Disabled at Secondary Stage
- Mid-day Meal for children
- Assistance/scholarship given by Department of Empowerment of Persons with Disabilities
- Supplementary Nutrition Programme under ICDS Scheme
- Payment of honorarium to AWWs & AWHs under ICDS Scheme
- ICDS Training Programme
- Supplementary Nutrition for children offered at creche centres
- Honorarium to creche workers and creche helpers
- Maternity Benefit Programme
- Scheme for Adolescent Girls
- National Mission for Empowerment of Women
- Ujjwala Scheme
- Swadhar Scheme
- Integrated Child Protection Scheme
- STEP programme
- Rashtriya Mahila Kosh
- Pradhan Mantri Matru Vanana Yojana
- Painting, essay contests under IEC component of human resource development and capacity building

AADHAAR CAN BE USED AS

Aadhaar while filing income-tax returns. Following the Supreme Court

specifically refuse to give consent would be allowed to exit the Aadhaar scheme.

Mobile phone companies and mobile wallets have been constantly insisting that customers link their phone numbers with Aadhaar. What has the court ruled on this?

The March 23, 2017, circular of the Department of Telecommunications, which mandated Aadhaar-based reverification of mobile numbers, has been held illegal and unconstitutional given that it was not backed by any law. In effect, the court has barred telecom companies from insisting that their customers furnish their Aadhaar details for the customer identification process. The provision in the Aadhaar Act that allowed private entities to conduct authentications, too has been held illegal, due to which corporate bodies including banks, telecom operators, mobile wallets, etc will not be able to press any customer for his or her Aadhaar number.

There was an argument that the passage of the Aadhaar Act as a Money Bill — in order to bypass Rajya Sabha where the government was in a minority — was unconstitutional. What has the Supreme Court ruled?

All the avenues where furnishing Aadhaar has remained mandatory pertain to Section 7 of the Aadhaar Act, which makes receipt of a subsidy, benefit or service subject to establishing identity by the process of authentication under Aadhaar or furnishing proof of Aadhaar, etc. It is very clearly declared in this provision that the expenditure incurred in respect of such a subsidy, benefit or service would be from the Consolidated