ITU-SUDACAD Regional Forum

IoT for Development of Smart Sustainable Cities

Khartoum, Sudan

13-14 December 2017

Session 3

Security, Privacy, and Trust
in IoT Systems Integration
for Smart Sustainable Cities Implementation

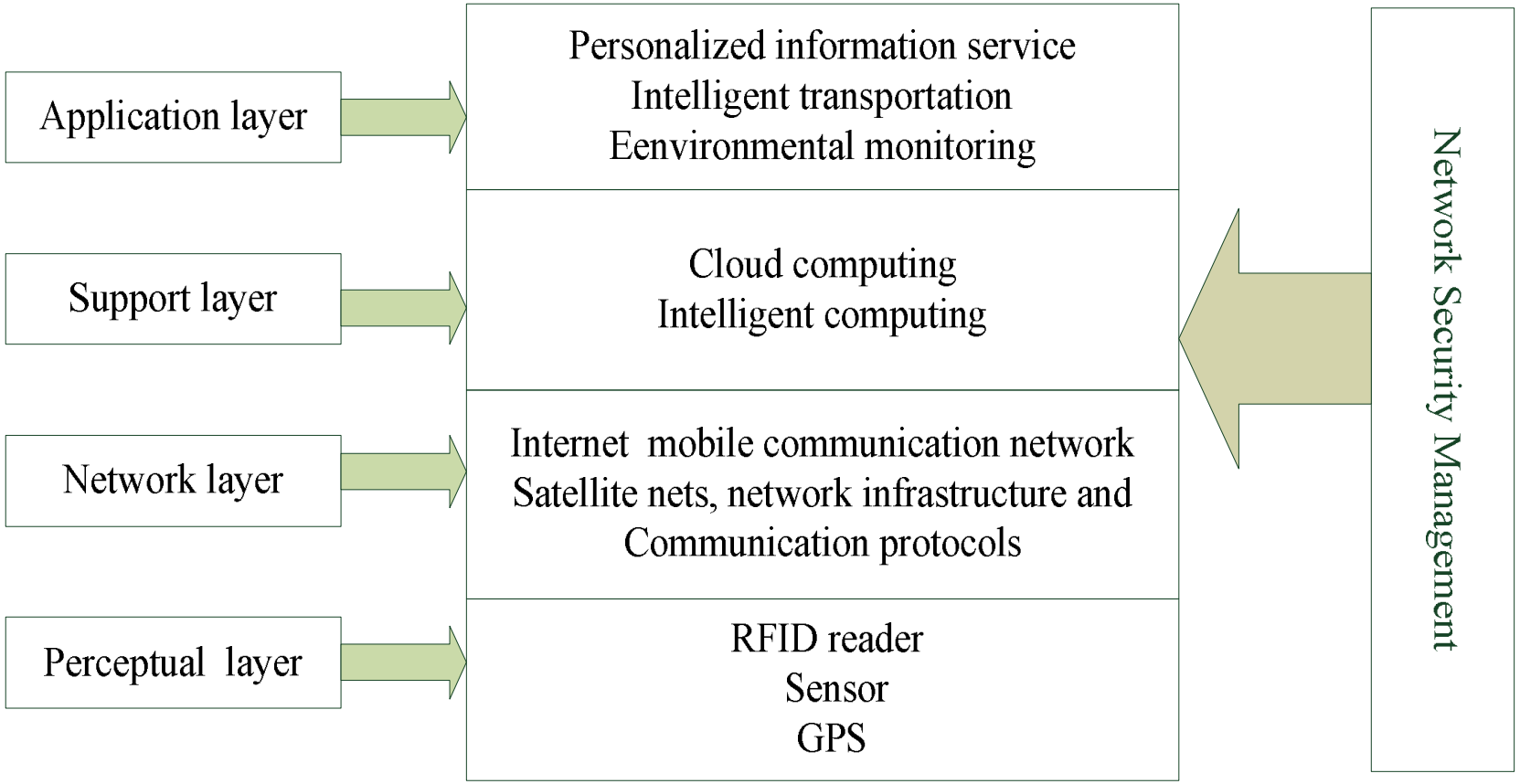
Prof. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org

IoT Security Requirements

Today's Facts

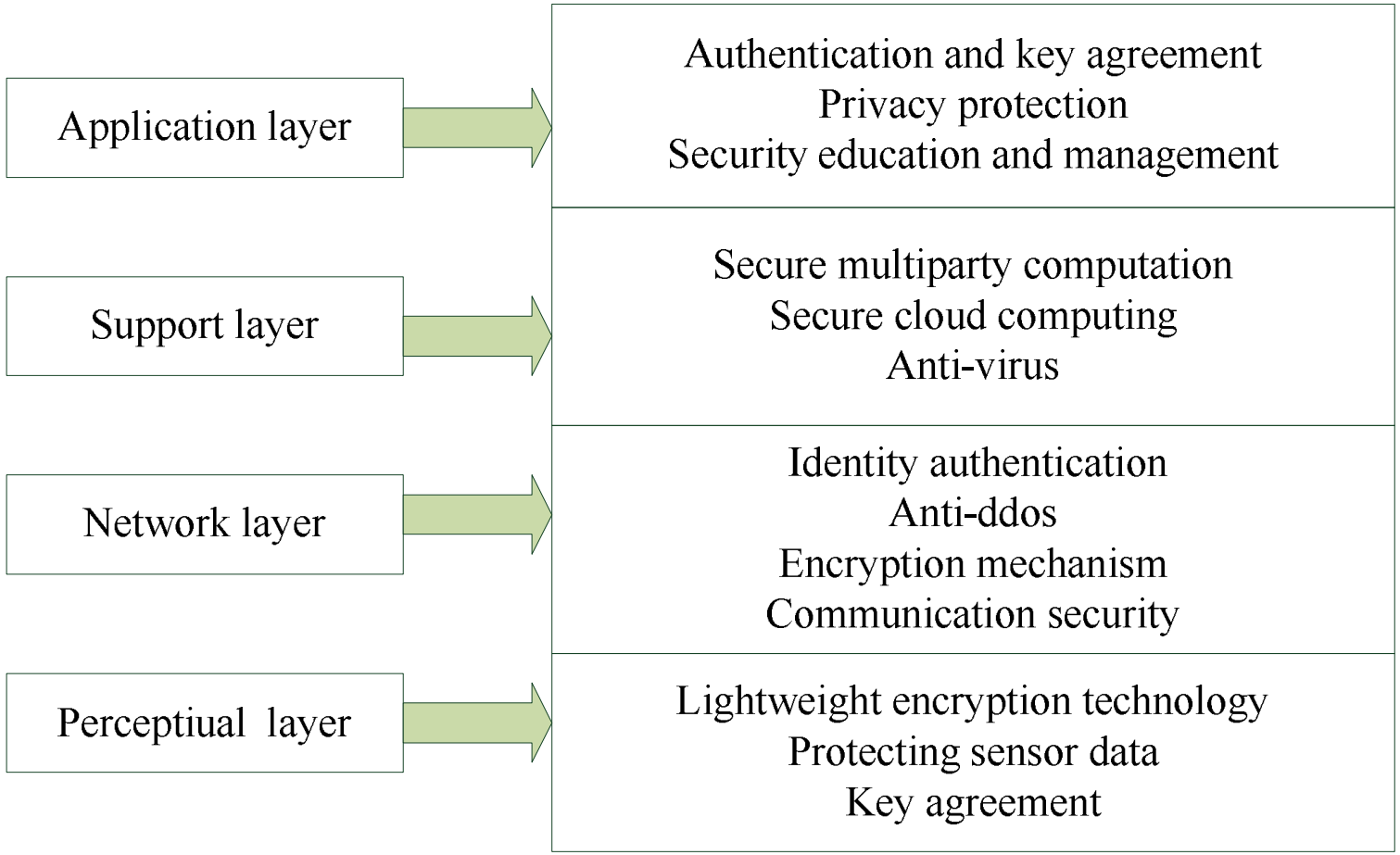
- Last decade: Internet of Things (IoT) approaching our lives silently and gradually
- Wireless systems (e.g., RFID, WiFi, 4G, IEEE 802.15.x) increasingly employed as technology driver for crucial smart monitoring and control applications.
- Widely perceived as the angular stone of the ICT market in the next decade. IoT is many-folded, embracing many different technologies, services, and standards:
  - Logical viewpoint: IoT systems depicted as collection of smart devices interacting on a collaborative basis to fulfill common goal.
  - Technological deployment: different processing and communication architectures, technologies, and design methodologies, based on target.
  - In the middle: a standardized or proprietary middleware could be employed to ease the access to virtualized resources and services. Might be implemented using cloud technologies, centralized overlays, or peer to peer systems.
- High level of heterogeneity and wide scale magnify security threats. Traditional security countermeasures and privacy enforcement cannot be directly applied to IoT technologies:
  - limited computing power,
  - scalability issues due to high number of interconnected devices.
- On the other hand, to reach a full acceptance by users, it is mandatory to define valid security, privacy and trust models.
- Adaptation and self-healing play a key role in IoT infrastructures. Accordingly, privacy and security issues should be treated with high degree of flexibility. In addition to conventional security solutions, need to provide built-in security in devices for dynamic prevention, detection, diagnosis, isolation, and countermeasures against successful breaches.

IoT Functional Layers View



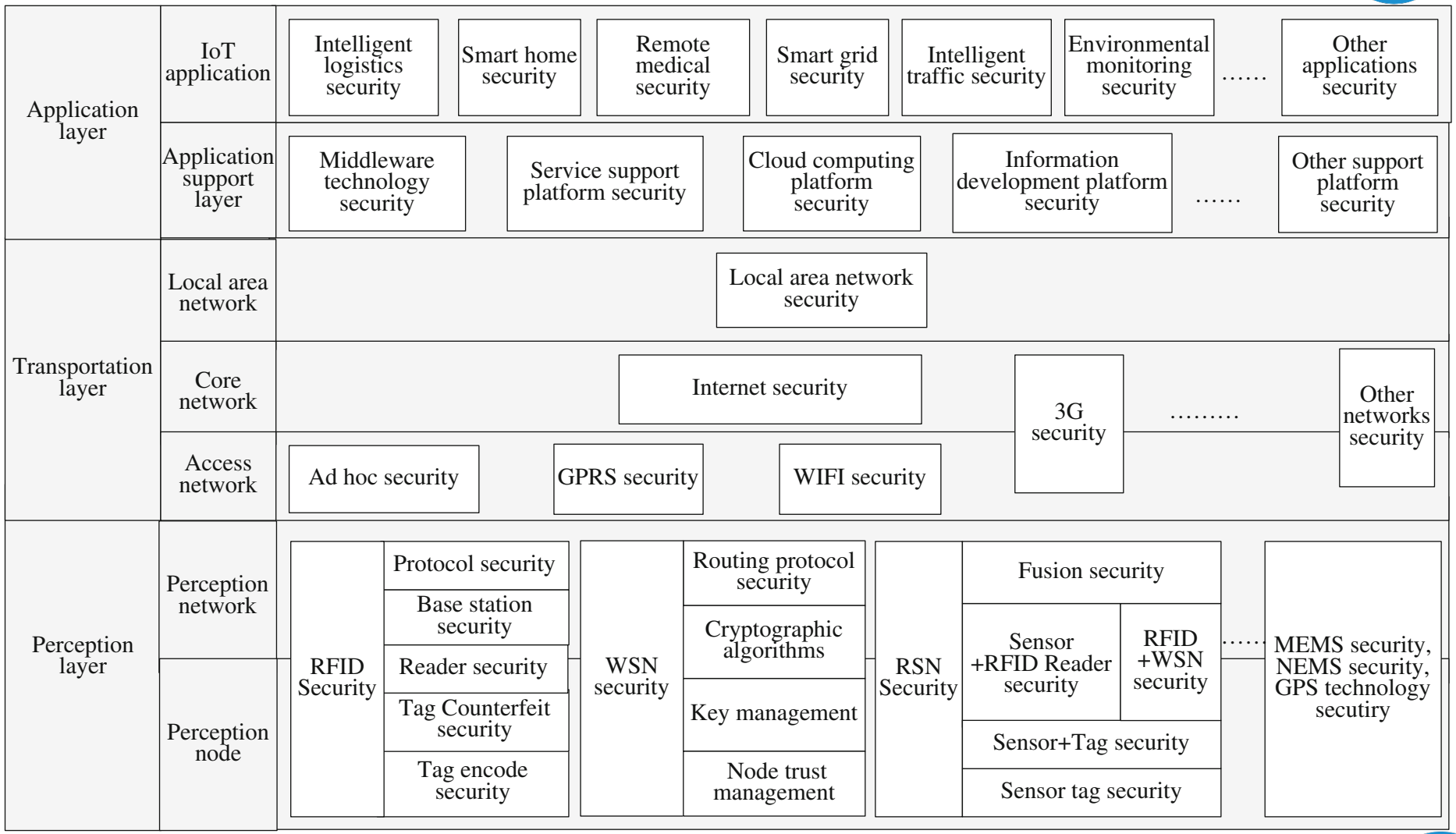
Source: H. Suo et al., "Security in the Internet of Things: A Review", in Proc. IEEE ICCSEE'12.

IoT Security Layers View



Source: H. Suo et al., "Security in the Internet of Things: A Review", in Proc. IEEE ICCSEE'12.

IoT Security Stack



Source: Q. Jing et al., "Security of the Internet of Things: perspectives and challenges", Wireless Networks, 2014.

Security Features

- Perceptual Layer:

  Nodes are short of computer power and storage capacity. Difficulty to apply frequency hopping communication and public key encryption algorithm to security protection. Difficulty to set up security protection system. Meanwhile attacks from the external network such as deny of service also bring new security problems. On the other hand sensor data still need protection for integrity, authenticity and confidentiality.

- Network Layer:

  Core network has relatively complete safety protection ability, but Man-in-the-Middle Attacks and counterfeit attacks still exist, meanwhile junk communications and computer virus cannot be ignored. Security mechanism in this level is very important to the IoT.

- Support Layer:

  Mass data processing and intelligent decision of network behavior in this layer, intelligent processing is limited for malicious information. Challenge to improve ability to recognize malicious information.

- Application Layer:

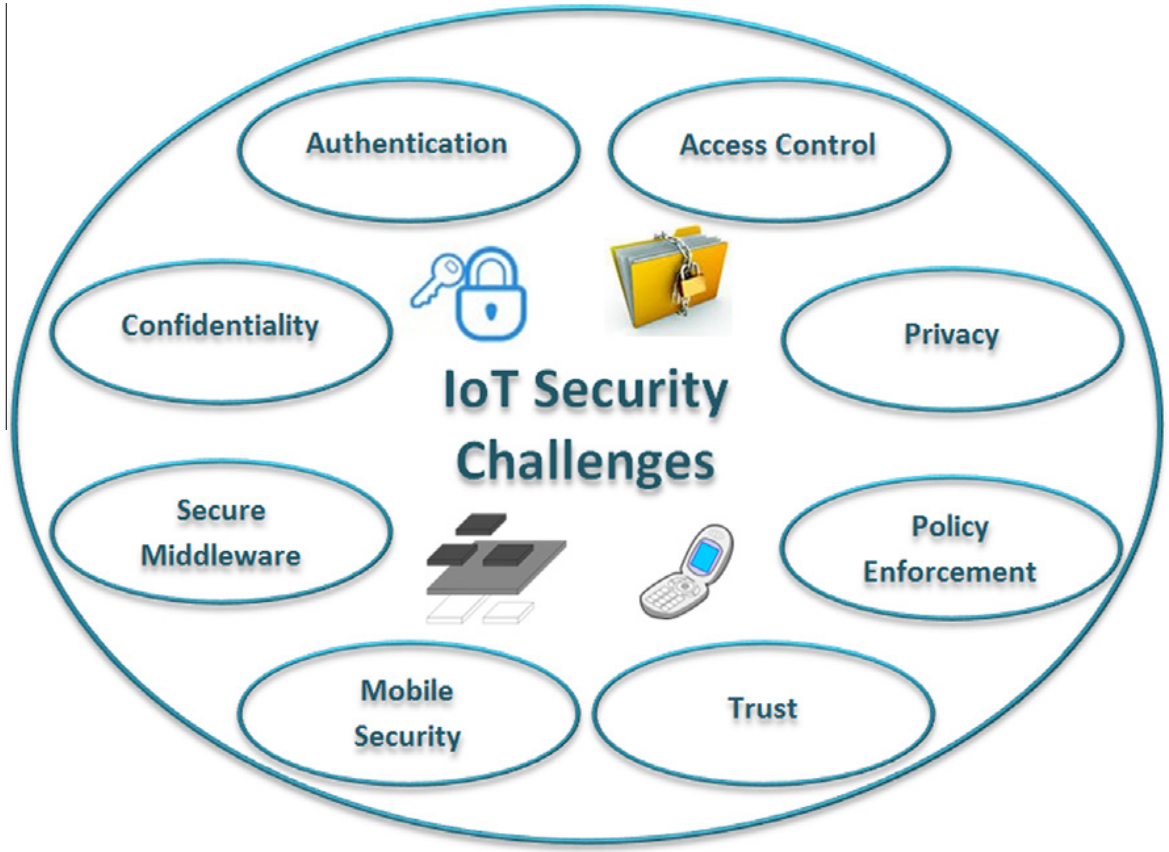
  Different security needs for different application environments. Data sharing one of the characteristics of application layer, hence creating problems of data privacy, access control, and disclosure of information.

Security Requirements

- Perceptual Layer:
  - Node authentication to prevent illegal node access;
  - Data encryption to protect confidentiality of information transmission between nodes; key agreement important process; Lightweight encryption for resource efficiency;
  - Integrity and authenticity of sensor data.
- Network Layer:
  - Identity authentication to prevent the illegal nodes;
  - Confidentiality and integrality mechanisms.
- Support Layer:
  - Cloud computing and secure multiparty computation;
  - Strong encryption algorithm and encryption protocol;
  - Stronger system security technology and anti-virus.
- Application Layer:
  - Authentication and key agreement across heterogeneous network;
  - User privacy protection;
  - Education and management (information security, especially password management).

Summary of Requirements

- Authentication
- Confidentiality
- Access control
- Privacy
- Trust
- Enforcement
- Secure middleware
- Mobile security



Source: S. Sicari et al., "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks 76 (2015) 146-164.

Authentication and confidentiality

Access control

- Permissions in the usage of resources, assigned to different actors of a wide IoT network:
  - Data holders: Users and things, as data holders, must be able to feed data collectors only with the data for specific target.
  - Data collectors: must be able to identify or authenticate users and things as legitimate data holders.
- In IoT: processing of streaming data vs. discrete data (conventional databases) — Performance and temporal constraints, access control for a data stream more computationally intensive than in traditional DBMS (DataBase Management System). Queries directly executed on incoming streams, can be of large volumes and arrive at unpredictable rates.
- Major challenges related to access control in an IoT scenario are:
  - How to guarantee the access permission in an environment where not only users, but also things could be authorized to interact with the system?
  - Is it more effective to exploit a centralized, distributed, or semi-distributed approach to manage scalable IoT architecture?
  - How to handle the huge amount of transmitted data in a common recognized representation?
  - How to support the identification of entities?

Privacy

- IoT finds application in many different fields, e.g.:
    - patients remote monitoring,
    - energy consumption control,
    - traffic control,
    - smart parking system, inventory management, production chain,
    - customization of the shopping at the supermarket,
    - civil protection.
- Users require protection of personal information related to:
    - Movements,
    - Habits,
    - Contacts and interactions.
- Users privacy should be guaranteed.

Trust

- Concept used in various contexts with different meanings.
- Complex notion — critical importance — no definitive consensus exists in the literature.
- Main problem: approaches towards trust definition do not lend themselves to the establishment of metrics and evaluation methodologies.
- Moreover, satisfaction of trust requirements strictly related to identity management and access control issues.
- Following issues still open in IoT trust management:
  - Introduction of well-defined trust negotiation language supporting semantic interoperability of IoT;
  - Definition of proper object identity management system;
  - Development of trust negotiation mechanism in order to handle data stream access control.

Enforcement

- Policy enforcement refers to mechanisms used to force the application of a set of defined actions in a system.
- Policies are operating rules which need to be enforced for the purpose of maintaining order, security, and consistency on data.
- Few works describe how to manage policies enforcement with reference to IoT scenarios
- Important to identify enforcement mechanisms suitable for the specific IoT context:
- equilibrium between the guarantee of security and privacy issues and the computing efforts requested by the exploited mechanisms themselves.
- Efforts done to define proper languages for privacy policies specification, but no standard yet to addresses specifically IoT paradigm.

Secure middleware

- Large number of heterogeneous technologies within IoT paradigm
- Several types of middleware layer are employed to enforce the integration and the security of devices and data within the same information network.
- Data must be exchanged within middleware respecting strict protection constraints.
- Different communication mediums for wide scale IoT deployments need to be considered; e.g. many smart devices can natively support IPv6 communications, existing deployments might not support the IP protocol within the local area scope, thus requiring ad hoc gateways and middleware.
- To design an effective solution, need to address following questions:
    - How heterogeneous devices and users can dynamically interact and agree on the same communication protocols, ensuring also security and privacy?
    - How to make the solution suitable for different platforms and therefore not dependent either on the exploited interfaces or protocols?

Mobile security

- Mobile nodes in IoT often move from one cluster to another.
- Cryptography based protocols are required to provide rapid identification, authentication, and privacy protection.
- Security issues of mobile devices are under investigation by the scientific community.
- Available solutions partially address the needs, thus requiring further efforts in order to allow the integration with other IoT technologies.

Examples of European Projects

	Butler	EBBITS	Hydra	uTRUSTit	iCore	HACMS	NSF	FIRE	EUJapan
Authentication	x			x	x	x	x	x	
Confidentiality	x	x	x		x	x	x	x	x
Access Control	x	x		x	x	x	x	x	
Privacy	x				x		x	x	x
Trust				x	x		x		
Enforcement									
Middleware		x	x		x				
Mobile	x						x		

Source: S. Sicari et al., "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks 76 (2015) 146-164.

Challenges

- High activity in IoT — Variety of questions need to be solved, at different layers of the architecture and from different aspects of information security.

- Security Structure

  IoT will remain stable-persisting as a whole over time, putting together the security mechanism of each logical layer can not implement the defense-in-depth of system, so it is a challenge and important research area to construct security structure with the combination of control and information.

- Key Management

  Key management basis of more security mechanisms — hot research area — still the most difficult aspect of cryptographic security. Lightweight cryptographic algorithm or higher performance of sensor node is still not applied.

- Security Law and Regulations

  Security law and regulations still not main focus. IoT is related to national security information, business secrets and personal privacy. Need for legislative point of view to promote development of IoT policies and regulations.

- Requirements for Burgeoning Applications

  High security necessary for guaranteeing system performance, and encouraging trust and adoption.

Thank You

شكراً

ITU-SUDACAD Regional Forum

IoT for Development of Smart Sustainable Cities

Khartoum, Sudan

13-14 December 2017

Session 3

Security, Privacy, and Trust
in IoT Systems Integration
for Smart Sustainable Cities Implementation

Prof. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org

Scenarios and Techniques for SSC

Smart Sustainable Cities Considerations

- Smart and sustainable city deployments will be carried out by a diverse ecosystem of providers in innovative domains, involving state-of-the-art technology, including critical and complex ICT implementations.
- Deployments can address different components and city systems, like intelligent transportation, connected health care, public safety and security, emergency services, smart grid and smart metering, intelligent buildings, etc.
- Increasing IoT complexity, hyper-connectivity, generation of significant amounts of data, will also mean increasing vulnerability, both to malicious attacks and unintentional incidents.

Hyper complexity + hyper connectivity + hyper data volumes = hyper vulnerability

- By conceiving interconnected urban systems with cybersecurity and data protection in mind, city administrators will be able to ensure service continuity, safety and well-being for citizens and businesses.
- Need to explore requirements and challenges of creating secure, reliable, and resilient SSCs. How administrations and the overall city ecosystems can provide resilient "smart" solutions that leverage digital information while protecting against malicious violations, unintentional damage and natural disasters.

Key definitions

- Notions of "resilience", "cybersecurity", and "data protection" are gaining increasing momentum, and are becoming extremely pertinent in SSC contexts as they relate to the risks posed to service continuity by threats from the cyberspace.
- **Resilience:**
  - "Ability to recover from security compromises or attacks", *ITU-T Study Group 17 (SG17)*
  - "The ability of a system or a sector to withstand, recover, adapt, and potentially transform in the face of stressors such as those caused by climate change impacts", *FG-SSC*.
  - Resilience linked to a series of attributes:
    - Robustness and ability to maintain performance and to continue operating, even under a cyber-attack or other incident (e.g. natural disaster).
    - Redundancy of system components that allow the system to resume operations, within a defined delay of time, in case of abrupt interruption, total or partial.
    - Flexibility and adaptability to new circumstances, including the systems ability to prepare for future threats by adjusting/rectifying issues that allowed the incident to occur, or that took place during an incident.
    - Achieving resilience and cyber resilience in a SSC context will ensure service continuity to its citizens.

Key definitions

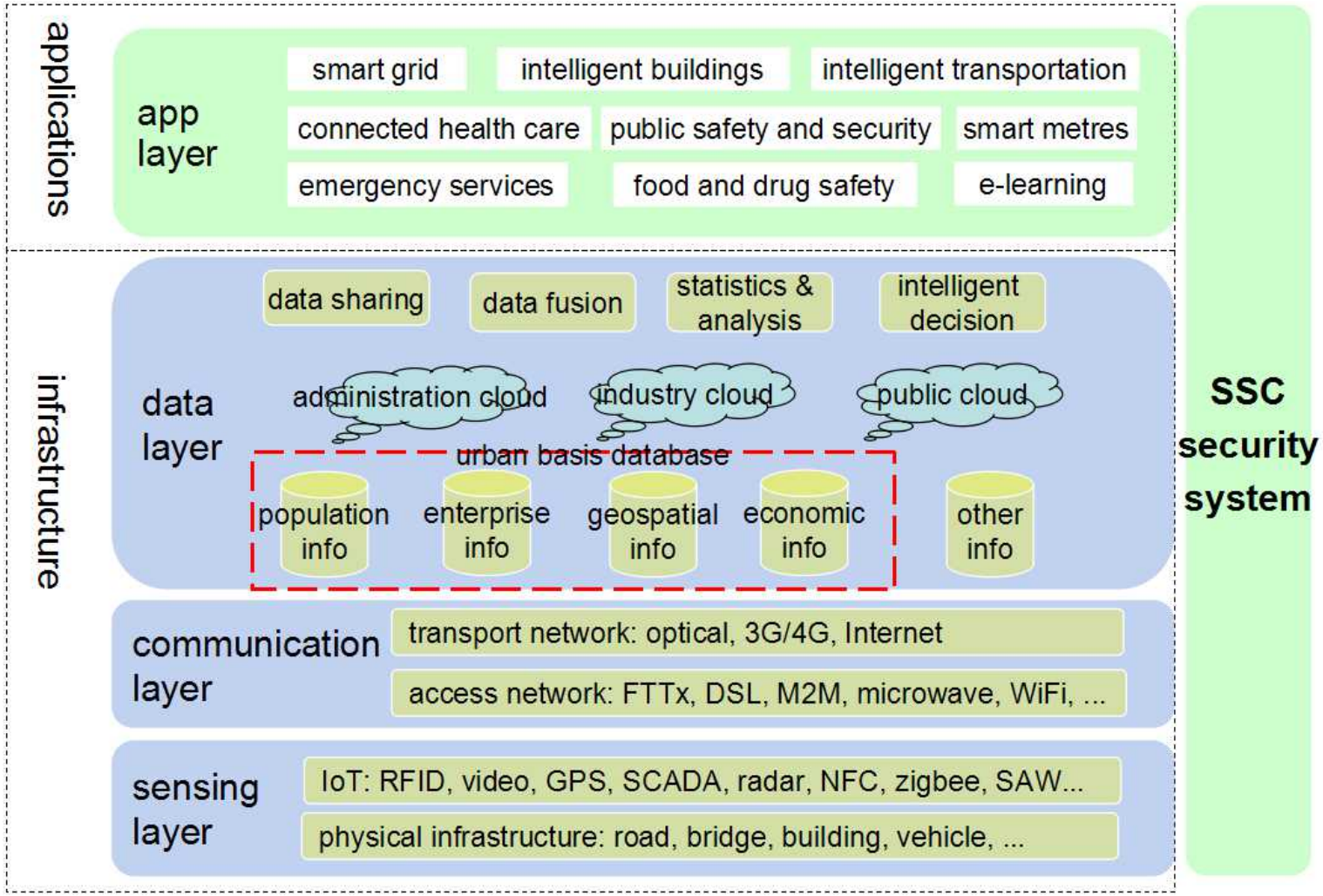
- **Cybersecurity:**
  - Concept refers to the discipline of ensuring that ICT systems are protected from attacks and incidents, whether malicious or accidental, threatening the integrity of data, their availability or confidentiality, including attempts to illegally "exfiltrate" sensitive data or information out of the boundaries of an organization.
  - Applies to network and server environments, as well as to endpoints (i.e. the individual terminals). Cybersecurity includes software tools, processes and people as key components of a successful implementation of the discipline.

- **Data protection**
  - Notion refers to tools and processes used to store data relevant to a certain IoT system or environment, as well as recover lost data in case of incident – be it fraudulent, accidental or caused by a natural disaster.
  - One critical element about data is the concept of data ownership, which refers to who is in charge of data, who can authorize or deny access to certain data, and is responsible for its accuracy and integrity, in particular personally identifiable information (PII).

Implications in SSC

- IoT is a key element of SSC development and refers to devices with embedded technology (e.g. sensors), and/or Internet connectivity, able to be reached and exchange information.
- The amount of data generated can be considerable. Big data will need to be appropriately and centrally stored, managed, analyzed, and protected. City operations centre supervise the interaction between systems and ensures continuity, integrity, and resilience.
- With time, the interconnected and interdependent services of smart cities will evolve under a centralized governance dashboard of specialized stakeholders, responsible for setting policies and processes, managing IoT assets, services and protocols, and ultimately administering the services for constituents. IoT control and management capabilities will be crucial in order to guarantee an efficient, secure and resilient governance and delivery.
- The European Network and Information Security Agency (ENISA) indicates that "processes" are seen as the most important pillar to secure critical infrastructures and industrial control systems (ICSs) – much more important than technology and people.

Architecture of SSC



Source: ITU-T Focus Group on Smart Sustainable Cities Technical Report, "Cybersecurity, data protection and cyber resilience in smart sustainable cities".

Layers of SSC Architecture

- **Sensing layer:** is the basic requirement for SSC to achieve its "smart" component. It provides the superior 'environment-detecting' ability and intelligence for monitoring and controlling the infrastructure, the environment, the buildings and the security within the city. It uses radio frequency identification (RFID) devices, sensors, supervisory control and data acquisition (SCADA) and other Internet of things technologies, providing ubiquitous and omnipotent information services and applications for individuals and society.
- **Communication layer:** is the "infobahn" or the backbone of SSC. The communication network should consist of large-capacity, high-bandwidth, highly reliable optical, pervasive networks, to relay and transport the city's intelligence. At the same time, the citizens can access the network "anytime, anywhere, on-demand".
- **Data:** is a vital and strategic resource of smart and sustainable cities. The data layer makes the city "smarter": its main purpose is to ensure that fragmented data is shared by the functions of data association, data mining, and data activation. The data layer contains data centre from industries, departments, enterprises, as well as the municipal dynamic data centre and data warehouse, among others, established for the realization of data sharing and data activation.
- **Application layer:** includes the various applications that manage the SSC's systems. This level exploits the previous layers and operates using their services.

SSC Potential Threats and Proactive Solutions

- Infrastructural architecture of SSC can be vulnerable to a number of threats given its complexity, cross-level nature, and extent.
- Dramatic increase in cyberattacks can be explained by the fact that more and more motivations can effectively and efficiently be served through the Internet. Perpetrators are attracted and can succeed, because cyberattacks are less detectable than physical actions, they do not physically expose the attackers, can be extremely inexpensive, can be launched by a geographically remote location, the attribution is extremely difficult, and even if someone is identified, the prosecution is even more problematic due to the lack of definitive international legislation and uncertain jurisdiction.
- Hackers motivations can range from a criminal intent aimed at financial gain, through to industrial espionage, cyber sabotage, cyber warfare, and political activism, among others. Any of these can be conceived, take place, and have damaging repercussions in SSC.
- Numerous episodes of city-infrastructure sabotage have been recorded in recent times, suggesting that ICT vulnerabilities can jeopardize the safe delivery of services to citizens, and/or their continuity.
- Vulnerabilities can involve data "in transit" (i.e. being transmitted between devices) or "at rest" (i.e. while stored).

Example 1– Smart grid, intelligent buildings and other critical infrastructure

- Cities are responsible for between 60% and 80% of the world's energy use. Therefore, optimizing energy delivery and consumption is vital.
- Smart grid technology aims to tailor the generation and supply of energy to user consumption, thus increasing efficiency, reducing costs and environmental impact. In particular, consumer "smart metres" and sensors, equipped with IP addresses, can communicate information about energy utilization patterns to the supplier, while allowing end-user control. This can help manage real-time demand, and even provide advice to consumers about their use habits.
- Buildings, both residential and commercial, provide an important opportunity to optimize energy consumption and enhance the well-being of residents and workers. Intelligent buildings, particularly office environments, are able to leverage smart grid technologies to influence energy supply and consumption by controlling lighting, climate control and IT.
- Smart grids and related infrastructure need protection from attacks that could cause severe blackouts.
- Attackers exploiting vulnerabilities in SCADA systems, based on traditional software platforms, can lead to intrusions with the potential to disrupt data exchange between utility control centres and end users, and severely compromise the delivery of energy services.
- Intruders can also install malware designed to obtain sensitive information, to control the networks that operate the service and cause a denial-of-service situation. This can be countered through intrusion prevention techniques, coupled with robust policies in areas such as network usage, browser patches, e-mail usage, as well as users' awareness of the issue and their education and preparedness on the subject.
- At the end-user level, smart metres may simply be hacked and compromised for fraudulent purposes: to alter proof of consumption or to 'steal' energy from other users, while preventing the provider from detecting service flaws.
- The European Union (EU) has engaged in a number of initiatives in the critical infrastructure protection (CIP) space.

Recommandations

- Public key infrastructure (PKI) or managed PKI can be used to avoid the fraudulent manipulation of smart metres in large scale and advanced metering infrastructures (AMIs), thus securing data integrity, revenue streams and service continuity.
- The smart grid can be secured at the communication layer by implementing PKI directly into metres, enabling identification, verification, validation and authentication of connected metres for network access. PKIs are ideal for large-scale security deployments requiring a high level of security with minimal impact on performance. In a PKI environment, it is essential that private keys and certificates be guarded by a reliable management solution that protects against ever-evolving data threats.

Example 2 – Intelligent transportation

- Keeping the city moving is critical. Transportation strategies have an impact on public safety, the environment, energy, emergency response services, the ability to do business, and on the delivery of other critical services, as well as the overall maintenance of the quality of life of citizens.
- Real-time traffic flow information, coupled with telecommunications, global positioning systems (GPSs), machine-to-machine (M2M) communication, wireless fidelity (Wi-Fi) and RFID technologies, as well as data analytics and prediction techniques, can be used to enhance private and public travel. Sensors can collect information about traffic conditions at critical city spots and send this information, via wireless communication, to centralized control systems. This data can then influence decision-making or even operate processes like traffic light synchronization.
- Optimizing transportation models requires a high degree of complexity from the ICT infrastructure and its components to avoid disruptions. These can be the result of malicious intent or simply well- meaning insiders' actions. For example, traffic management could be impaired by hacking into the navigation system that directs a bus driver into the city through a wrong route, due to false information about traffic volume.

Recommandations

- The data transmitted from devices may be subject to spoofing. Unencrypted traffic data may be subject to attackers injecting false traffic reports into satellite navigation devices, as proven by cybersecurity experts.
- Vulnerabilities can also put information at risk due to unintentional actions, mistakes, carelessness or inadequate processes.

Example 3 – Connected health care

- Health care delivery can benefit from a connected approach, with electronic patient records available to all medical services. This will enable public health professionals and clinicians to collaboratively access information in a secure way, at any time, from anywhere and from any mobile device.
- In many cases, telemedicine solutions connected through broadband, wireless or satellite, can prove vital in situations where the infrastructure or specific contingencies do not allow for the physical presence of a specialist, in cases such as natural disasters or remote geographical locations.
- An ageing population needs traditional care, as well as assisted living and health monitoring services to enable independence at home. This can be achieved through the utilization of sensors and devices connected to health operators through broadband, wireless and data analytics, and crucially, the deployment of privacy, identification and security systems.
- In the case of a road accident, a malicious intrusion that compromises communication between first respondents and operational centres could prevent its accurate localization and the efficient dispatch of emergency units. Equally, during such incidents, emergency services might need to operate using medical data for injured patients by accessing a central location, and they should operate on the basis of reliability and integrity of the information.

Recommandations

- In this context, back-up, cybersecurity and authentication solutions can ensure that health care systems offer reliability and integrity, as well as patient privacy.

Example 4 – Public safety and security

- Above all, cities need to be safe. Public safety and security has become paramount for city administrations, whether protecting them against crime, natural disasters, accidents or terrorism.
- From conventional street violence to complex financial offences, identity thefts or data breaches, the crime scenario is extremely dynamic and can only be tackled by increasingly sophisticated technologies and processes.
- Tele-surveillance systems are becoming pervasive in urban settings and, coupled with real-time communication capabilities, can help emergency services intervene promptly in incidents.
- In the immediate aftermath of a serious accident or catastrophic event, reliability and security become key factors. The ability to share information between agencies, to operate sophisticated tele-surveillance systems, to guarantee connectivity to incident response teams and first responders, to gather and analyse heterogeneous intelligence and data about incidents in real time, allow municipalities and emergency services to increase safety conditions for citizens, businesses, assets and infrastructure.

Recommandations

- It is critical that tele-surveillance systems maintain their integrity and availability and that emergency services can rely on wireless or M2M communication to obtain directions and instructions from operational control centres.
- When information is transferred and managed over unsecured lines between different operators (both internal and external) and with heterogeneous systems, data encryption is required. By leveraging strong two-factor authentication and one-time password entry, only trusted personnel can gain access to critical data and control systems. Digital certificates can also be used for authentication, signing and encryption.

Example 5 – Wireless communications and hotspots

- Both large and small municipalities offer free wireless hotspots in addition to those provided by airports, hotels, and shops. As this trend continues to grow, more and more citizens will be exposed to potential vulnerabilities, in particular the younger population who are at risk of being lured into unsafe websites and chat rooms.
- Designing and building encryption solutions into devices ensures that they can only communicate with the required control centre, and that communications can be authenticated.
- Public WiFi connections (both free and paid) are increasingly common, but security for such connections may be lacking or is insufficient. WiFi connections can be provided in coffee shops, hotels, airports, parks and even in some streets. The host buys a wireless access point, connects that device to the Internet, and broadcasts its signal within a public place. Anyone with a wireless card within range of the host's access point can access its network and use the Internet. In order to make it quick and easy to use their hotspots, some hosts disable much of the security built into their wireless devices. This is a notable trade-off. Without encryption, your plain text data passes unprotected through the air, where it can be intercepted by cybercrooks.

Recommandations

- Attention should be paid to the surrounding area when accessing hotspots, in order to verify that nobody is able to read one's laptop screen. A privacy screen can be used for extra security.
- The network configuration should be changed in order to manually select each wireless network that the system joins.
- File sharing should be turned off while at a hotspot. Highly sensitive or personal data should be stored elsewhere, and when using instant messaging or e-mail, nothing should be sent that one would not want made public.
- There exist products that enable users to become “invisible” on the network by creating a virtual private network (VPN). These products encrypt the username, password and other confidential information that users may have entered online, allowing the users to control what they share online, no matter where they connect to the Internet. Internet banking, stock trading or other sensitive online financial transactions should be avoided while using a public hotspot.
- Security software should be kept current and active.

Recommendations to ensure SSC service continuity

Smart sustainable cities should prioritize providers who offer solutions and methodologies for security, backup, data loss prevention, archiving and disaster recovery, and who are able to protect and manage heterogeneous environments resulting from legacy systems and newer deployments, including open source, managed mobile devices, and virtualized systems.

- **Protecting information proactively**

  SSC contexts increasingly involve big data considerations, and subsequently the need to centralize and manage the vast amount of information that is continuously generated and used. Taking an information-centric approach, embedding security within data and taking a content-aware approach to protecting information, is vital for identifying ownership of: (a) the location of sensitive information, and (b) who has access to it. Classifying data and utilizing encryption helps to secure sensitive information and to restrict access to unauthorized individuals.

- **Authenticating users**

  Strong authentication enables organizations to protect public assets by verifying the true identity of a smart device, system or application. This prevents individuals from accidentally disclosing credentials to an attack site, and from attaching unauthorized devices to the infrastructure.

Recommendations to ensure SSC service continuity

- **Leveraging threat intelligence**

  In order to understand the major attack trends, city officials and CIOs can count on an established observatory, like the Global Intelligence Network, to provide one of the most extensive and accurate vendor-neutral analyses of trends on malware, security threats and vulnerabilities from security research centres around the world. The same information is also used to compile the annual Internet Security Threat Report, which contains vital information about current and emerging threats and vulnerabilities.

- **Balancing traditional versus cloud delivery**

  Within a SSC environment, all the smart services mentioned so far in the analysis can be delivered through a traditional client-server approach, but also through a cloud computing model, both private and hybrid, in order to leverage "as-a-service" capabilities and efficiencies.

  These models require a secure virtualized environment where data can be safely guarded and processed with appropriate service level agreements (SLAs) in order to guarantee the provision of essential services to citizens. Authentication and encryption policies and techniques can help ensure the integrity of the cloud environment and its safe operation in the virtual space. Availability and disaster recovery solutions should guarantee compliance with SLAs, as well as resilience for critical city services.

Recommendations to ensure SSC service continuity

- **Managing security services and Computer Emergency Response Teams (CERTs)**

  SSC should also consider outsourcing security services to providers who can leverage extensive, global expertise in the field of cybersecurity to minimize security-related disruptions and data loss. The ICT leadership can then be relieved from this particular complex and time-consuming aspect and focus on the functional duties of running the city's ICT.

  SSC should also rely on their national CERTs to align with national coordination on cyber incidents and security, and thus benefit from the international visibility this type of coordinated efforts provide.

- **Protecting infrastructure**

  Securing endpoints, messaging and web environments, defending critical internal servers and implementing the backup and recovery of data, should be among the key priorities of SSC strategists. Organizations also need visibility and security intelligence to respond to threats rapidly.

- **24x7 availability of the critical infrastructure**

  Ensuring resilience in case of an incident can be achieved through the adoption of solid backup and recovery software or appliances, as well as adequate policies, processes and tools.

Recommendations to ensure SSC service continuity

- **Developing an information management strategy**

  This should include an information retention plan and policies. Organizations need to refrain from using backup for archiving and legal retention, and should instead implement deduplication mechanisms to free up resources, adopt a full-featured archive system, and deploy data loss prevention technologies.

- **Access control at the boundary of network**

  Access control at the boundary can isolate attacks away from internal networks. Different boundaries can be implemented, with different policies enforced.

  A firewall that consists of access rule, verification tools, packet filtering and application gateway, can greatly improve the security of an internal network. Since only selected protocols can pass through the firewall, the network environment has become more secure. Firewall can prevent well-known unsafe protocols, making it impossible for external attackers to use these vulnerabilities to attack the internal network. The firewall should be able to reject all of the above types of attack packets, and immediately alert the administrator.

Recommendations to ensure SSC service continuity

- **Protecting intrusion dynamically**

  Intrusion detection is another important dynamic security technology, which can collect and analyze information from a number of key points of computer network and system, and find out whether there is any suspicious behaviour, sign of an attack or policy violation. There are three types of intrusion detection systems (IDSs):

  - network-based IDS;
  - host-based IDS;
  - integrated IDS.

- **Preventing DDoS attacks**

  There are different mechanisms that can enhance the ability to withstand DDoS through increasing the cost of attack. These include the use of high-performance network equipment, the guarantee of sufficient network bandwidth, the upgrade of the host server hardware, the use of static pages whenever possible, the enhancement of the operating system transmission control protocol (TCP)/IP stack, and the installation of specialized anti-DDoS firewall.

Recommendations to ensure SSC service continuity

- **Network security audit**

  A network security audit carries out compliance management by fine-grained auditing the network operating behaviour of the business environment. Through recording, analyzing, and reporting the network behaviour of system and authorized users, the network security audit can function as a mechanism for planning and preventing, concurrently monitoring, as well as reporting and tracking the source after the incidents take place. Consequently, network security audits can strengthen the internal and external networks behavioural regulation.

- **Child online protection in SSC**

  As the analysis conducted thus far has demonstrated, the design of a comprehensive cybersecurity strategy for SSC should take into account multiple sources of vulnerabilities, as well as existing and emerging threats. Children are among the most vulnerable users of online services.

Conclusions

- SSC deployments will involve multifaceted developments carried out by a diverse ecosystem of providers in innovative domains, as well as the adoption of state-of-the-art technologies characterized by critical and complex ICT implementations.
- However, the rise in ICT complexity has also translated into increasing levels of vulnerability, both to malicious attacks and to unintentional incidents.
- Protecting both the systems and the data with rigorous policies, up-to-date technology and techniques, will prove vital in ensuring the continuity and the resilience of all the services involved in the SSC architecture.
- Only by conceiving interconnected urban systems with security and information protection in mind, SSC administrators will be able to ensure the safety and the well-being for citizens and businesses alike.
- City planners and administrators should take proactive steps to ensure systems' security and data protection from the early stages of the SSC's inception and planning process. This constitutes a crucial step towards building resilient, smart sustainable cities.

Thank You

شكراً