IET Smart Cities

Perspective Article

Security for smart cities

eISSN 2631-7680
Received on 17th January 2020
Accepted on 23rd January 2020
E-First on 13th May 2020
doi: 10.1049/iet-smc.2020.0001
www.ietdl.org

Chai K. Toh[1,2] ✉
[1]*GLG Group, San Francisco, California, USA*
[2]*National Tsing Hua University, Department of Computer Science, Hsinchu City, Taiwan*
✉ *E-mail: ckgtoh@gmail.com*

Abstract: Smart cities are evolving globally and many governments have invested large sums of monies to develop smart cities. This development is not a result of an overnight decision but rather, smart cities have evolved through a period of time, directly from earlier work on the digital city to ubiquitous city, green city, connected city, sustainable city, eco-city etc. The present age sees the arrival of very high-speed wireless 5G connectivity, fast GPU multi-core-based servers, big data, cloud computing, artificial intelligence, and data analytics. Many of these new technologies have supported the development and realisation of smart cities. In this study, the authors present an outline of security for smart cities and provide a deeper understanding of what we meant by securing smart cities. They discuss the applicability of existing security methods of authentication, access control, encryption, firewalls, and their appropriateness to defending a smart city. Specifically, we cover the security of data, internet, water supply, electricity supply, city brain, and other critical city services and present the possible malicious attacks on a smart city and consequences. Finally, they discuss security best practices for smart cities.

1 Introduction

It is undeniable that we are moving towards the era of smart cities. Countries around the world are implementing smart cities, such as those in the UK, China, and Hong Kong. Smart cities, collectively, is an area that overlaps information and communications technology (ICT), urban sciences, environmental sciences, and social sciences. This multi-disciplinary field, although complex in its formation, is also exciting since it is going to transform the lives of millions of city residents. Threats can be viewed as attempts to attack a target in many forms, be it on data, access, control, services, connectivity etc. Threat prevention is always a requirement and a challenge for smart cities. Many have debated what is an effective 'FIREWALL' or 'SHIELD' for securing smart cities. There is also a lack of focus on cyber-security for smart cities [1, 2]. In this study, we intend to discuss this.

2 Understanding smart cities

2.1 Human versus city analogy

There are some resembles between humans and cities. People live and work in cities. A city's vibrancy is tied to its business operations and citizens' activities. If we look at what makes up a human, it is the brain, senses, and body. A human brain is the centre of intelligence, where reasoning and decisions are made and were information is processed and stored. Our human senses (through the eye, ear, nose, skin etc.) allow us to gather information and send them to the brain for processing. Finally, the human body provides all the other necessary functions to sustain liveability. Likewise, we can view a smart city has having a similar form of construction as that of a human being.

As shown in Fig. 1, the three building blocks of a smart city are as follows:

(a) *Brain* – the centre of control and decision-making authority of a smart city. It is the central command centre, where observations are analysed, abnormalities are monitored and detected, and events are triggered.

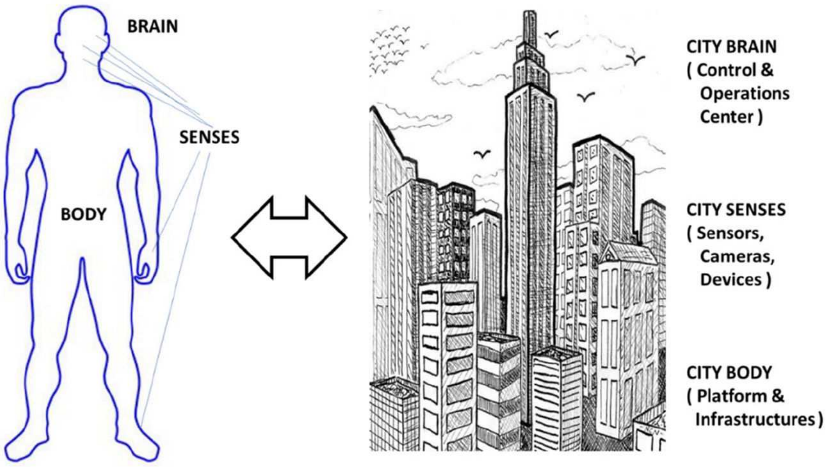


Fig. 1 *Analogy of a human versus a smart city*

(b) *Senses* – the inputs to the smart city systems include: vision, sound, sensor readings etc. Vision takes the form of cameras located at specific sites. Microphones can be used to record the conversation of crime scenes (and other used cases) to serve as event trigger points and evidence. For example, water flow gauges can be used to detect floods while smart meters can be used to record electricity and water usage.

(c) *Body* – the body of a smart city system refers to both infrastructures and ICT platforms. By infrastructures, we refer to buildings, roads, drains etc. By ICT, we refer to three platforms: (a) connectivity, (b) data, and (c) artificial intelligence (AI).

2.2 System architecture

From an ICT point of view, a smart city has four essential layers: (a) sensors or end points, (b) edges (gateways), (c) platform (data, AI, connectivity management), and (d) applications, i.e.

SMART CITY = [sensors] + [edge] + [platform] + [applications]

From a higher level of abstraction, a smart city is analogous to a living thing (after all it is indispensable without the Internet of Things (IoT)) [3]. Alibaba has viewed a smart city as having a 'city brain' [4], where the bulk of AI resides, so as to govern the activities and control of all things (internal and external). Huawei [5] has even coined the term 'smart city nerve system' to depict the existence of sensing and intelligence.

For a smart city, it is expected that IoT will be an indispensable part of the whole city platform. The 'inputs' to the smart city system will be sensors, be it video cameras, microphones, temperature sensors, water gauges etc. Sensors are devices that will interact with the physical world, collect data, and relay them back to the collection points over different wired (optical fibre, wires etc.) or wireless (WiFi, Bluetooth, narrowband-IoT etc.) links. The collection points are commonly termed as gateways. Sensors commonly use the message queuing telemetry transport or constrained application protocol messaging protocol to send data over wireless links to the gateway. The messages are usually small size packets and are light weight in order to conserve power consumption by the sensors in transmitting these data. Smart city applications residing on the cloud platform can interact with the gateway via the standard REST API.

As shown in Fig. 2, a smart city's system architecture is viewed to contain four horizontal layers and two vertical layers, with applications residing on top. The essential four horizontal layers are device and sensing layers, followed by connectivity, IoT management, and data-AI layers. The first layer concerns sensors and other devices (cameras etc.) that provide inputs to the smart city system. Sensor data are then connected to collection points (gateways) via the connectivity layer. The IoT connection management layer residing on the edge provides a collection of different sensor data sent over different links and different protocols, ensuring interoperability across heterogeneous devices and connectivity. Finally, the data-AI layer provides data processing, analytics, insights, and intelligence to drive smart city applications.

At the upper layer, different smart city applications will utilise data and insights differently, and they will trigger appropriate events to occur (e.g. summoning the police to the crime scene for a smart city security application). AI technology can be used to help analyse the data and predict the correct output (such as facial recognition to identify the criminal under investigation). Hence, the data and processing layers are present in each smart city application. Ideally, one common data and AI platform layer can be present to serve all possible smart city applications but realistically, this is hard to achieve given the fact that there exist different administrative control domains (where one transport domain may not allow another say health domain access and sharing of data) and a centralised platform layer can result in a bottleneck at times of failures.

The vertical layers of the architecture concern security, operations, and control management. Since some smart city applications are developed for private parties, such as a private home estate or a private business building, they are considered silos on their own, with little or no requirement to interface to other smart city applications. However, certain smart city applications (e.g. smart transport, health, and environment) are serving the public and are established by the government and hence, these public smart city applications will require

(a) Operations and control management
(b) Applications interconnection and interoperability
(c) Comprehensive security

The Intelligent Operations Center (IOC) [6] or the Command and Control Center, for example, is an entity that allows the government to control its various smart city subsystems (transport, environment, public security etc.) centrally. This design will also allow the interconnection and interaction of various government smart city applications. For example, in the case of a crime happening at a road junction, the police will need access to smart transport, smart intersection, and smart lamp posts applications in order to gather all related data associated with the crime. It must also be able to control the cameras near or located at the crime scene. Hence, for government-hosted smart city applications, there is a need for these applications to interface and interact with one other, and allow for the exchange of relevant data.

A smart city system and its applications need to be secured and security features have to be built into each layer of the smart city platform, end-to-end, so as to ensure integrity, prevent intrusion and malicious attacks. This explains why security cuts across all horizontal layers. Devices need to be secured to ensure they are tamper proof. Sensor data transmitted over a secured wired or

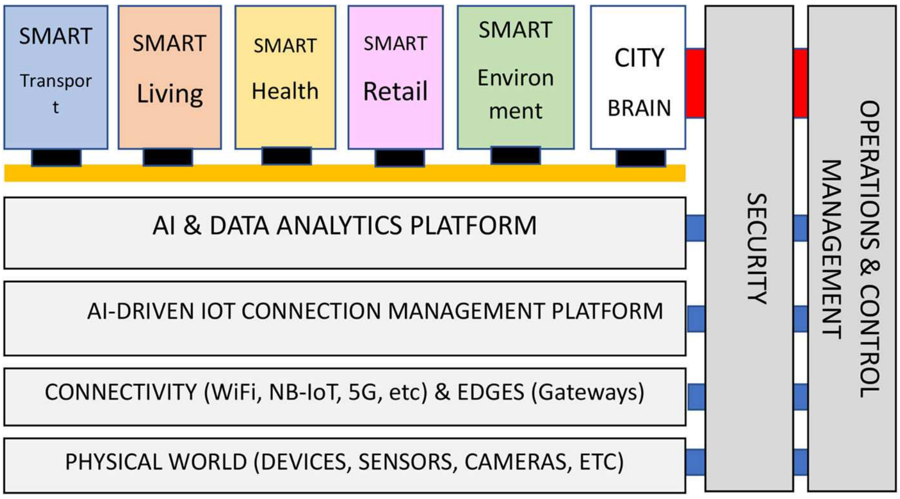

SMART Transpor t
SMART Living
SMART Health
SMART Retail
SMART Environ ment
CITY BRAIN
AI & DATA ANALYTICS PLATFORM
AI-DRIVEN IOT CONNECTION MANAGEMENT PLATFORM
CONNECTIVITY (WiFi, NB-IoT, 5G, etc) & EDGES (Gateways)
PHYSICAL WORLD (DEVICES, SENSORS, CAMERAS, ETC)
SECURITY
OPERATIONS & CONTROL MANAGEMENT

Fig. 2 *Proposed smart city system architecture, where security and city management cut across all layers*

Fig. 3 *Security protection shield of a smart city is equivalent to having multi-layers of security protection, from protecting the brain to the senses and body*

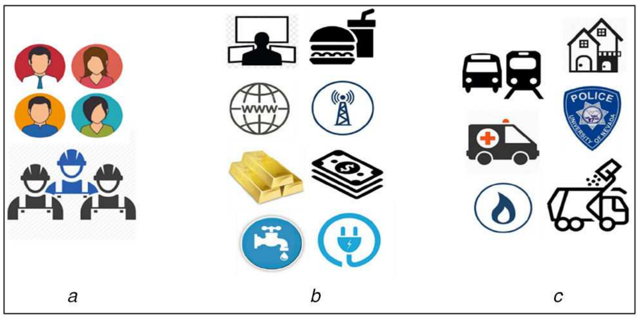


Fig. 4 *Three assets of a smart city*
(a) People, *(b)* Resources, *(c)* Services. All three need security and protection

Table 1 List of critical resources to protect in smart cities

No.	Critical resources to protect in a smart city
1	water
2	energy (electricity)
3	connectivity
4	data
5	IOC (brain of smart city)
6	financial assets

wireless link needs to be encrypted. Only authorised personnel should be granted access to devices, either locally or remotely. Data should be securely stored in distributed storage. Access to data should be granted to authorised applications and personnel. Data associated with each smart city application can be regarded as a standalone entity, securely stored in private or public cloud. They can be shared or kept secret. Many countries have established policies associated with data governance and depending on the location where data are kept, authorities have jurisdiction over the data and its misuse. We shall examine security for smart cities in greater depth in the next section.

3 Security for smart cities

3.1 How to view the security problem?

Security for smart cities refers to a bigger problem, and one should not view it in silos. By silos, we are referring to developing security solutions for specific smart city applications, such as smart transport, smart health, smart environment, smart living etc. Rather, one should view and understand what are the underlying factors that will govern and contribute to the secured operations and services of these smart city applications.

Effectively, we need to secure the ‘brain’, ‘body’, and ‘senses’ of a smart city, in addition to securing each smart city application. This calls for a comprehensive and total security solution to protect a smart city. As shown in Fig. 3, the security solution will not only shield and protect the city from attackers from intruders outside the city but also protect its internals – infrastructures, connectivity, applications, and services.

Table 2 List of critical services to protect in smart cities

No.	Critical services to protect in a smart city
1	law enforcement
2	health (medical) services
3	fire rescue services
4	transport services
5	housing services

3.2 What is there to secure?

In designing security solutions for smart cities, one needs to examine: (a) what is there to protect, (b) what are the end goals of the attackers, and (c) the types of attacks. To understand what is there to protect in a smart city, we need to look at its assets. A smart city's assets are its resources, people, and services. By resources, I am referring to

(a) financial assets – monies, commodities (gold etc.), other assets (stocks etc.),
(b) infrastructures – telecommunications, internet, data centres, offices, homes, etc. and
(c) life essentials – water, electricity, food, medical supplies etc. (Fig. 4).

By people, I am referring to the humans who live and work in the city. This includes both young and old. People form the talent pool and workforce of a city, and they support the business operations and drive the city's economy. Finally, by city services, I am referring to public health, water and electricity supply, public sanitary, sewage services, police, ambulance services etc.

All of these are important assets for a smart city. Attackers can be tempted to strike due to a city's wealth or its richness in resources, prompting them to steal such assets. However, not all attackers are lured to theft. Other end goals include attackers who are more interested to create chaos by disrupting or halting services. Also, most attacks are malicious and they generally fall into the following two categories:

(a) Attacks that disrupt the lives of city residents
(b) Attacks that disrupt business operations in the city

Both of these end goals are traumatic to the lives and economic well-being of a city. Also, the type of attacks can be defined by the locality

Local attacks – physical presence at the site or vicinity of the attack. This is where command centres with video surveillance help to capture attackers and identify them.
Remote attacks – away from the site but using internet connectivity to gain control of computer systems to disrupt city services. These attackers are usually residing outside the city and will need to be hunt down through their internet protocol (IP) network addresses.

Without losing focus, one should identify which are the more critical resources and services compared to others. Critical resources and services are those essential for day-to-day normal operations of the city that support citizens' lives and business operations. With this in mind, the following six most critical resources and services to protect have been identified and are shown in Tables 1 and 2. In the next few sections, security aspects associated with each of these critical resources and services will be elaborated.

3.3 Securing water supply

An essential element for human survival is water, which is why it is highest in priority. A city cannot continue its normal life without the presence of water, both for personal consumption and businesses (in restaurants etc.). Attacks on water source point and water transport can disrupt water supplies. Again, such attacks can be done physically by the attackers on site, shutting off power

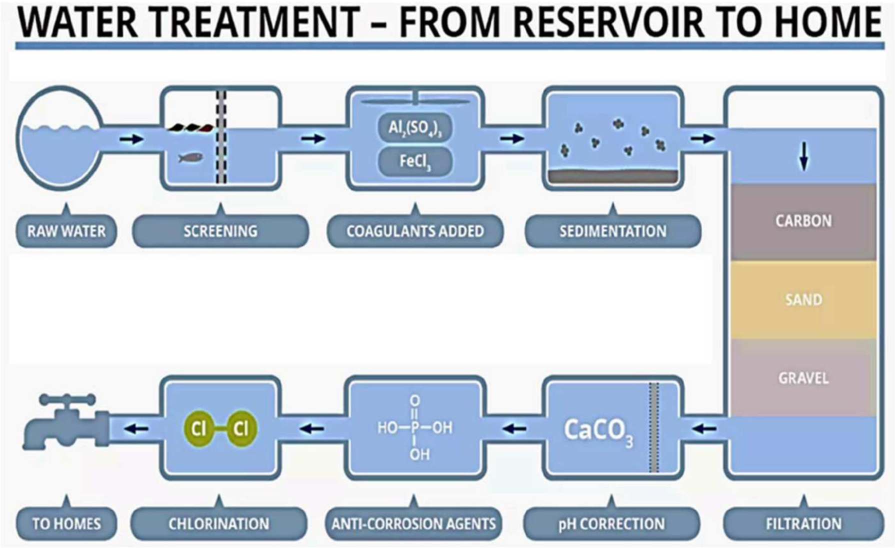


Fig. 5 *Water supply involves water treatment prior to delivery on a tap (source: https://www.compoundchem.com/wp-content/uploads/2016/04/The-Water-Treatment-Process.pdf)*

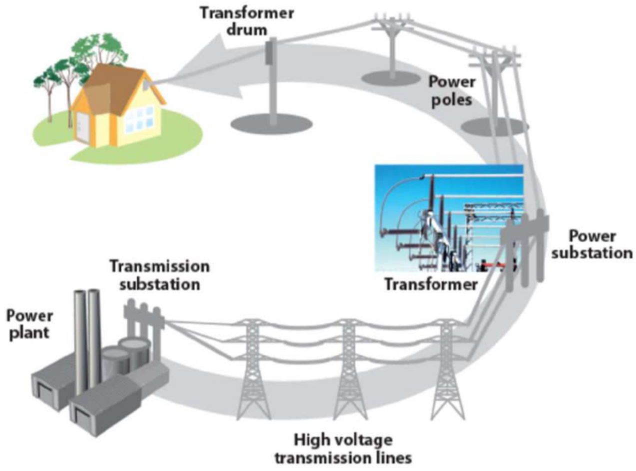


Fig. 6 *Power supply, transmission, and distribution network [11]*

pumps, and breaking water transport pipes in the supply chain. Attacks that are done on site are usually warded off by the presence of security guards and on-site security video surveillance.

However, digital attacks that are done by attackers that are remote (outside the city) can be hard to catch. Through cyberspace, they gain control over the water management system to shut down or reduce water supply to the city. Watchdogs programmes have to be present 24 × 7 to constantly monitor for anomalies and remote access to the water management system should be restricted to a hand few or even forbidden.

According to [7], water contamination is a critical event to be prevented. Terrorists can resort to poisoning the drinking water reservoir to infect millions of people quickly, resulting in sickness or death. In the USA, the Bioterrorism Act (2002) [8] is a legal framework and action to address this issue. The Bioterrorism Act requires that drinking water utilities that serve more than 3300 people to conduct vulnerability assessments and develop emergency response plans. As shown in Fig. 5, by tampering with any part of the water treatment and supply process, one can infect water supply with chemical hazards.

3.4 Securing energy

Most of the smart cities applications today are powered by electricity. Without power, most of the smart city system and business will cease to operate and the city left in darkness. Hence, securing power source and power delivery is critical to smart cities. Power generation can be halt by physically destroying the site, or interrupting the electricity generation process. This demands stringent site security to ensure power generation will not be interrupted, and there exists backup power in times of interruption. Power delivery [9], however, refers to power relayed through power lines, transformers, relays, switches, and power stations. Hence, attacks on any of these components can interrupt power supply, crippling all smart city applications. In fact, it has been reported that terrorists [10] were targeting energy generation sites as possible places to attack in order to create massive city blackouts and potentially driving street riots. It is important that a comprehensive strategy and framework be established in order to secure both power generation and power delivery to the city (Fig. 6).

Furthermore, since an energy infrastructure system is highly networked, there exists a chance for a cascade of disruptions, thereby multiplying the impact of a single localised attack. This can result in massive blackouts in multiple cities. Smart cities must have built-in robustness and isolation capability to counter such attacks.

3.5 Securing connectivity

Smart city infrastructures require connectivity to connect sensors, cameras, data centres etc. Hence, connectivity is the other bloodline (in addition to power) for smart cities. Connectivity can occur over wired and wireless network infrastructures. This could also be viewed as securing IoT. IoT security includes device, data, and connection security. In [12], device security includes hardware security (tamper proof), access and authentication control. Data security is achieved by encryption while connection security is attained by using light weight secured end-to-end transport protocols.

Existing telecom networks used to support fixed broadband and mobile cellular networks are reasonably secured, with few incidents of connectivity hijacking. However, for a smart city, the security requirements should be raised higher since people expect a smart city to be more secured than normal cities. Table 3 presents a list of security protection methods for different types of wireless links, which will be discussed below.

WiFi security: securing wireless networks requires securing the wireless link. It requires a secured media access control (MAC) protocol where access to the link will be controlled. In WiFi, WiFi protected access (WPA) was developed by the Wi-Fi Alliance to provide more sophisticated data encryption capability and better user authentication than wired equivalent privacy (WEP), which was the original Wi-Fi security standard.

Bluetooth security: Bluetooth [13] offers several security modes: 1, 2, 3, 4, and device manufacturers determine which mode to include in a Bluetooth-enabled gadget. In almost all cases, Bluetooth users can establish 'trusted devices' that can exchange

Table 3 List of wireless links and corresponding security protection methods

Type of wireless links	Security protection methods
• WiFi	WEP and WPA
• Bluetooth	authentication; confidentiality; authorisation [13]
• LORA	See [14, 15]
• SIGFOX	firewall; anti-eavesdropping; authentication; replay avoidance. See [16]
• LTE	see the guide to LTE security [17]. Security mechanisms include authentication, cryptographic protection mechanisms, hardware protection mechanisms, and network protections.

Table 4 List of security-embedded protocols for network and end-point protection

Protocol security	Remarks
• IPSec	uses encapsulating security payload and authentication header to encrypt and authenticate data and tunnels (packet encapsulation) to form VPN
• DNSSec	protect against multiple concurrent requests for name resolution, thereby avoid overloading and crashing the server
• HTTPS	protection for web users in accessing data and web pages
• TLS	transport layer security (TLS) is a cryptographic protocol that provides end-to-end communications security over the Internet.
• SSL	secured socket layer (SSL) is used to provide a secured encrypted link for information transfer between a client and a web server.
• VPNs	provide a secured path for information transaction over the unknown route and over unsecured networks

data without asking permission. When any other device tries to establish a connection to the user's gadget, the user has to decide whether to allow it. Service-level security and device-level security work together to protect Bluetooth devices from unauthorised data transmission. Security methods include authorisation and identification procedures that limit the use of Bluetooth services to the registered user and require users to make a conscious decision when opening a file or accepting a data transfer. As long as these measures are enabled on the user's phone or other devices, unauthorised access is unlikely to occur. A user can also simply switch his Bluetooth mode to 'non-discoverable' and, therefore, avoid connecting with other unsafe Bluetooth devices entirely.

LORAWAN security: the LoRaWAN security design adheres to state-of-the-art principles: the use of standard, well-vetted algorithms, and end-to-end security. LoRaWAN security include: (a) mutual authentication, (b) integrity protection, and (c) confidentiality. Mutual authentication is established between a LoRaWAN end-device and the LoRaWAN network as part of the network join procedure. This ensures that only genuine and authorised devices will be joined to genuine and authentic networks. LoRaWAN MAC and application messaging are origin authenticated, integrity protected, replay protected, and encrypted. This protection, combined with mutual authentication, ensures that network traffic has not been altered, is coming from a legitimate device, is not comprehensible to eavesdroppers and has not been captured and replayed by rogue actors. LoRaWAN security further implements end-to-end encryption for application payloads exchanged between the end-devices and application servers. LoRaWAN security uses the advanced encryption standard (AES) cryptographic primitive combined with several modes of operation: CMAC2 [14] for integrity protection and CTR3 [15] for encryption. Each LoRaWAN device is personalised with a unique 128-bit AES key (called AppKey) and a globally unique identifier (EUI-64-based DevEUI), both of which are used during the device authentication process.

SIGFox security: SIGFox [16] is a low-power low-cost solution to connect sensors and devices. The radio communication between the base stations and the SIGFox cloud, as well as the SIGFox cloud itself, are secured using signature-based authentication and virtual private network (VPN). Users are connected to the SIGFox cloud using the hypertext transfer protocol secure (HTTPS) encrypted interfaces. SIGFox has a built-in firewall that prohibits internet access to SIGFox devices without going through SIGFox core network and data are protected both in transit and at rest. Data-in-motion security is achieved through message authentication and replay avoidance. Through the use of a message token and an authentication key, verification of the token ensures the authentication of the sender and the integrity of the message. For data at rest security, SIGFox base stations and its core network use trusted platform module, also known as ISO/IEC 11889, to secure hardware through integrated cryptographic keys.

Long-term evolution (LTE) security: LTE is the key 4G cellular technology that is globally used today to support broadband mobile cellular communications. Concerning security, the USA National Institute of Science and Technology (NIST) organisation has published a comprehensive report on LTE Security [17], which covers: (a) hardware security, (b) cryptography, (c) air interface security, (d) E-UTRAN security, (e) backhaul security, and (d) core-network security. LTE infrastructure components (e.g. evolved node B, mobility management entity, serving gateway) may use commodity hardware, firmware, and software, making it susceptible to publicly known software flaws. Threats directed at LTE networks include:

- Malware attacks
- Air interface eavesdropping
- Radio jamming
- Physical attacks on infrastructures

Securing wired networks will also require securing the wired link. Most wired connections occur over Ethernet, over co-axial cables or fibres. There is nothing stopping someone from tapping on a wired link to look at on-going waveforms and trying to extract data, but with signals encrypted, extraction is difficult.

Protocol security: in addition to 'link security', there is also a need for security embedded into the protocol, i.e. 'protocol security'. Most internet data communications over wired or wireless links use the transmission control protocol/user datagram protocol/IP suite. Internet access and service provision are key to many home and business users. Disruption in the provision of internet services can shutdown many business operations etc. Table 4 presents a list of security enabled protocols to provide network and end-point security.

3.6 Securing data

Most smart city applications will sense, collect, process, and analyse data to yield meaning insights and using these insights to create meaning services. For example, smart-transport applications will collect vehicular-, driver-, traffic-, and passenger-data while smart-health applications will collect patient- and doctor-data. Regardless of which smart city applications, data will be generated as part of the smart city platform and these need to be secured, both in content and in storage. Such data can be protected in several ways:

(a) Access control – denying unauthorised access to the data.
(b) Encryption – protect the content of the data.
(c) Authentication – authenticate the source.
(d) Signatures – confirm the validity of the data.
(e) Privacy – disassociate data from the identify and location of the user.

Table 5 List of data to secure in a smart city

Types of data to secure	Remarks
transport	• aviation travel records
	• land transport data
	• driver data
	• vehicle data
	• trains, buses, taxis, etc.
	• traffic lights
health	• patient records
	• doctor records
	• medical supplies records
	• medical staffs' information
finance	• personal financial data
	• business financial data
	• tax data
utility	• water usage
	• electricity usage
	• gas usage
	• users (consumers) data
telecom	• subscribers' data
	• infrastructure data
	• utilisation data
	• transactions data

Table 6 A list of critical data to protect and the responsible entities in a smart city

Types of data	Responsible entity
• citizens' data	• government
• financial data	• financial institutions
• urban data	• government
• utilities data	• providers and government
• transport data	• government
• health data	• healthcare providers and government
• weather data	• government
• criminal data	• law-enforcers and government
• housing data	• government

Recently, there have been incidents of data breaches, such as the leakage of personal data by Equifax [18], the loss of personal email data by Yahoo [19], the loss of customers' data by Citibank [20], and Standard Chartered [21]. All these have caused a public outcry and the call for government action. Therefore, for a smart city, one needs to look at protecting the various types of data associated with each smart city application and held the respective entity responsible and accountable to, as shown in Tables 5 and 6.

From Table 6, a large bulk of data is under the responsibility of the government. Hence, governments should establish comprehensive policies and frameworks to protect data. For example, in the USA, the Department of Commerce and justice court have fined Yahoo Inc. for the data breach. Providers from private institutions should also ensure their methods of protecting customers' data indeed fulfil tough requirements. Regulations, standards, and best practices for protecting data are still evolving and so far, no global standard has emerged.

In the European Union (EU), the General Data Protection Regulation (EU) 2016/679 ('GDPR') [22] is introduced, covering data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also concerns the export of personal data outside the EU and EEA. The European Commission's Data Protection Directive [23] was adopted by the European Parliament and ministers from national governments in 1995. The directive contains key principles with which member states must comply. In the processing of personal data, one must comply with eight enforceable principles of good practices. They are

(a) Fairly and lawfully processed
(b) Processed for limited purposes
(c) Adequate, relevant, and not excessive
(d) Accurate
(e) Kept no longer than necessary
(f) Processed in accordance with the data subject's rights
(g) Secured
(h) Transferred only to countries with adequate protection

In the USA, laws are introduced to ensure information security measures are used. Some of the recent acts introduced include:

- 2000 U.S. Congress Electronic Signatures in Global National Commerce Act ('ESIGN') [24]
- 2002 Homeland Security Act (HAS) [25]
- 2002 Federal Information Security Management Act of 2014 [26]

Hence, using technologies alone cannot fully and adequately protect data. Laws and regulations are needed to ensure compliance by organisations in possession of and responsible for the processing of data.

3.7 Securing the smart city brain

A smart city system needs to be secured and accessed only by authorised personnel. Protecting access to devices, networks, and platforms is crucial in securing smart cities. Many cities around the world have used a centralised smart city operation and control centre concept.

Huawei, for example, has created the IOC – intelligence operation centre [6], to perform smart city monitoring, control, and response function, supported by real-time image capture, live video feeds, maps with live status information and updates on roads, people movement etc. This is illustrated by Fig. 7.

The IOC must be fully secured. Gaining access and control over a smart city's IOC is regarded as a catastrophic event similar to that of an invasion of the city and that needs to be quickly isolated. The IOC must be swiftly repossessed by the authorities. Security issues associated with an IOC include the following:

- Issue of a compromised insider: this is often hard to detect as the attacker is an under-cover authorised personnel.
- Issue of remote hack: people who have remote access rights to the IOC must be limited to no more than a handful in order to narrow down the culprits should an attack is made remotely.
- Stolen passwords: access passwords of authorised personnel at the IOC site may be stolen by malware and phishing techniques. To deal with this type of weakness, multi-factor access control can help narrow down and prevent intruders.
- Operational misbehaviours: IOC must have the ability to monitor and track operation misbehaviours by IOC staff. All events triggered at the IOC are monitored in real-time and logged into data storage for subsequent follow up and investigations.
- Backup and takeover control: if an IOC is invaded, it has to be quickly disabled. With replication of another IOC, the compromised IOC can be disabled by the other, rendering it useless. The disablement can be done in the form of cutting off the power to the IOC or disabling its connections to compute, storage, network, sensors, and all external interfaces. A master–slave mode can also be established so that the compromised IOC is made a slave (hence obeying the master IOC), with the master capable of disabling the slave IOC functions completely.

3.8 Securing smart city financial assets

Financial assets include both tangible and intangible assets from city residents, business corporations, and government. Most of these financial assets are held by financial institutions, be it banks, securities firms or credit unions. Possible attacks include

Fig. 7 *Huawei's IOC is the brain of a smart city (source: Huawei https://e.huawei.com/en/solutions/industries/smart-city/ioc)*

Table 7 Types of smart city services and possible attacks

Type of critical services	Remarks
water	• disrupt the supply of water to households and businesses • resulting in public outcry and threatening personal health
gas	• hinder the delivery of gas to households • leaving residents unable to cook food
electricity	• disrupt the supply of electricity to the city • resulting in city blackouts and an unsafe environment
police	• hinder and delay the summon of police • resulting in crimes unattended to and loss of lives
fire rescue	• hinder and delay the summon of fire rescue • resulting in property damage and lives lost
traffic lights	• create traffic disorientation, jams, delays, and accidents • create chaos on the streets • hinder the delivery of services
public lifts	• maliciously disrupt the normal operation of lifts • causing delays, accidents, and anxiety
waste clearance	• household rubbish clearance services are disrupted • threatening public hygiene, health, and safety of residents
public environmental cleaning	• falsify video images of street cleanliness • resulting in dirty and unhygienic streets, drains, and parks
public parking services	• blockage of parking by falsifying status of no parking spaces • resulting in road congestion and anxiety
payment of utility bills	• payment of bills prevented or not registered • resulting in unexpected termination of utility services
banking services	• withdrawal of money prevented • credit card transaction services halted • financial transactions interrupted or financial theft
aviation services	• disrupt travel services at airport • passengers strangled at airports, creating chaos and distress

- disabling financial services (such as online banking, online trading etc.)
- financial thefts (stealing money, stocks etc.)
- accounts information thefts (user and financial data)

Firewalls are mostly used in protecting financial IT systems from outsiders, along with intruder detection and prevention systems. Security in terms of user access control, user multi-factor authentication, data encryption, secured network and transport connections, malware and virus protection, logs inspection, end points protection etc., are all needed to protect the financial assets of a smart city.

3.9 Securing smart city critical services

In the case where municipal city services (such as the delivery of electricity, gas etc.) are disrupted by hackers, the lives of millions of city residents will be crippled. This is a major catastrophic event. Table 7 shows a list of possible attacks and the effects as a result of disrupting several types of critical services.

Disrupting law enforcement (police) and fire rescue operations is also fatal. Furthermore, disruption of transport services (trains, buses, taxis, flights) and traffic lights are also disastrous (misuse of traffic lights can result in accidents and congestion). Disruption to essential city services is considered a crime and an act of terrorism in many countries nowadays. A smart city must, therefore, secure all of its essential services. Attacks on a smart city's critical services can take the form of

(a) Denial of service – totally stopping the provision of essential city services.
(b) Disrupting services – intermittent availability of city services.

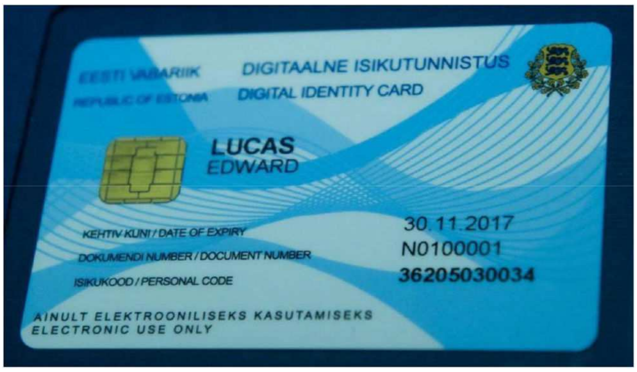
3.10 Blockchain and smart cities

The beauty of blockchain technology lies in its use of public-key encryption and consensus protocols to validate transactions and authenticate a ledger in a distributed manner, without the need for a centralised authority. Since the roll out of bitcoin and the use of blockchain technology, many people have accepted the use of blockchain to provide security for financial transactions. Its incorruptible distributed ledger technology has allowed bitcoin to evolve as a digital cryptocurrency invested by millions. However, how can blockchain be applied to smart cities? Can blockchain be used to make cities more efficient, transparent, secure, and resilient? These are tough questions awaiting to be answered (Table 8).

Currently, blockchain is being used in smart contracts [27] – where multiple parties (seller and buyer) can securely establish business agreements. Smart contracts facilitate, verify, and enforce

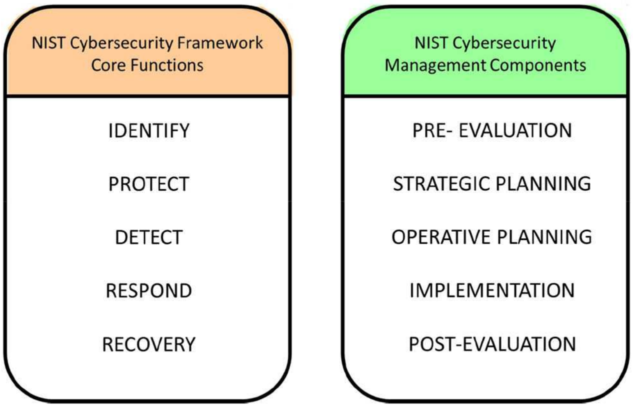
Table 8 Global blockchain initiatives (source PWC [12])

Country	Remarks on the application of blockchain
Sweden	real estate transactions are made using blockchain
UK	blockchains are used in the distribution of grants
Estonia	blockchain helps to maintain transparency in medical records
Ghana	blockchain used to provide tamper-resistant property ownerships
Russia	blockchain used to provide secured trading and transactions between shareholders
Korea	banks have created blockchain-based eco-system
Singapore	blockchain used to help prevent trade invoice fraud



EESTI VABARIIK
REPUBLIC OF ESTONIA
DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD
LUCAS
EDWARD
KEHTIV KUNI / DATE OF EXPIRY 30.11.2017
DOKUMENDI NUMBER / DOCUMENT NUMBER N0100001
ISIKUKOOD / PERSONAL CODE 36205030034
AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

Fig. 8 *Estonian digital identity card (source [31])*



NIST Cybersecurity Framework Core Functions
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVERY

NIST Cybersecurity Management Components
PRE- EVALUATION
STRATEGIC PLANNING
OPERATIVE PLANNING
IMPLEMENTATION
POST-EVALUATION

Fig. 9 *NIST cybersecurity framework core functions and management*

the negotiation or performance of a contract digitally. Smart contracts also allow credible transactions to be made without the need for third parties.

Estonia [28] has been using distributed ledger technology since 2012 in areas such as healthcare, judicial/legislative services, personal data, ID management, and more. Dubai [29] will apply blockchain to city-wide logistics and storage industries, as well as shifting to a 100% paperless government and storage system. Several possible applications of blockchain to smart cities have been suggested [30]. They include

- Identity – the decentralised identity management system can provide a secured mechanism for storing and validating user identities. This reduces identity thefts and other frauds.
- Payment – municipal city services payment can be made through a blockchain payment platform.
- Energy – facilitate a resilient power grid by providing a secured platform for energy providers, buyers, and traders.
- Transport – facilitate a secured peer-to-peer transport platform for share ride users and providers.
- Waste management – the process of waste clearance and transportation can be managed over a distributed ledger, to enable organised tracking of schedules and tasks.
- Government services – the use of smart contracts for managing citizens' rights, votes, taxes, asset management etc. In Estonia, E-Residency [28] allows the use of a digital ID to digitally sign documents and contracts and the verification of the authenticity of such documents.
- Insurance – blockchain can potentially disrupt the insurance industries [32] by the use of automated verification of claims and payments data from third parties, thereby reducing administrative costs.
- Healthcare – health records use blockchain technology to secure their content and prevents unauthorised changes to personal health data (Fig. 8).

3.11 Security best practices

According to the EU Agency for Network and Information Security [33], a list of best practices for cybersecurity protection of [34] smart cities has been identified. They are:

- Use of VPNs
- Encryption of data
- Use of network intrusion detection system
- Use of physical protection
- Install access control
- Install alarms and surveillance
- Implement security policy
- Creation of activity logs
- Maintenance of backups
- Regular auditing
- Shutdown procedures

Introducing best practices is a good approach for many countries to implement and learn from each other experiences. Every smart city should contribute to the definition of security best practices, report and share every vulnerability so that such incidents will not happen again in other cities. In addition to the efforts made by the European ENISA, the American NIST addresses these issues by introducing a cybersecurity framework [35], as shown in Fig. 9. The prime purpose of the framework is to develop a common language for better understanding and interpretations of cybersecurity risks to stakeholders. The framework introduces five main core functions as

(a) Identify – to develop an understanding of the cybersecurity risks associated with people, systems, assets, data, and capabilities.
(b) Protect – to develop safeguard measures to limit and contain a security event while protecting and ensuring the delivery of services.
(c) Detect – to develop methods to identify security beaches and anomalies.
(d) Respond – to react to an event by containing it, limiting its harmful impact.
(e) Recovery – to quickly restore capabilities and services impaired by the security event and prevent further similar attacks.

A well-defined management process is used in the evaluation, strategic planning, operation and implementation of security functions, especially for municipal city projects.

Since most smart city projects are huge, a well-defined management process is necessary. As shown in Fig. 10, to successfully secure a smart city, one would need to integrate recommended security standards [36], frameworks [37], policies, best practices, and learn the experiences from others. It has to be a continual fine-tuning process so that most security issues can be addressed. This means that smart cities in different countries must be willing to openly share their experiences and provide feedback to facilitate the realisation of complete city protection – a process that will require the co-ordination of the International Telecommunication Union and country government leaders.

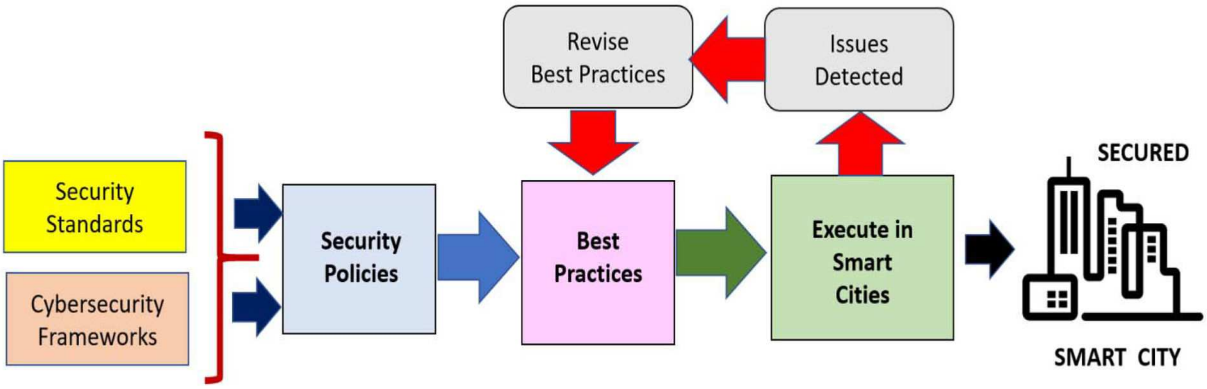


Fig. 10 *Process flow for the realisation of security protection for a smart city*

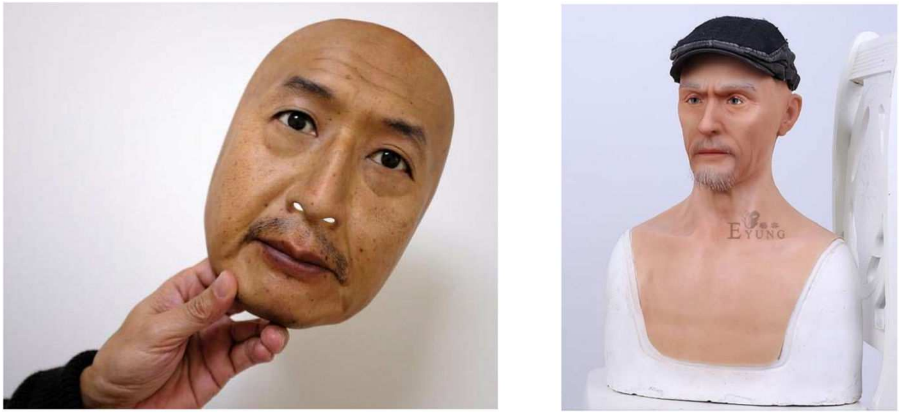


Fig. 11 *Silicone mask technology today can create human-like faces that potentially can impersonate anyone, and fooling facial recognition. Source [38]*

Table 9 Fraud associated with face impersonation

Year	Country	Remarks
2015	France	case of a fake French minister wearing a silicone mask and scamming away 80 million euros. [39]
2018	Nigeria	case of an impersonating first lady who gained access to Nigeria's presidential complex to run business scams [40]

3.12 Emergence of facial clones and fraud

With the increasing reliance on video and facial recognition in smart cities, many public safety systems use AI and facial recognition technologies to match wanted criminals or missing persons. Also, many retail, enterprise, and passport control gate entry systems around the world have increasingly deployed facial recognition technology to scan and validate travellers, visitors, shoppers, and authorised personnel. Such increase reliance can result in a negative effect, where fraudsters will impersonate others to hide their identities while committing crimes in public or private places. In fact, there are already several cases where fraud using silicone masks (see Fig. 11) has resulted in millions of financial lost (see Table 9). An important aspect of security for future smart cities is to validate persons beyond mere facial recognition, by using biometrics, iris recognition, finger prints, voice, handwriting etc. This opens room for further research.

4 Conclusion

Smart cities' developments have begun around the world and have presented great challenges to industries and government. A smart city is incomplete without a comprehensive security framework and mechanisms to protect its citizens, businesses, operations, and services. This study highlights the importance of security for a smart city and presents a list of possible attacks and identifies areas to secure and protect, such as (a) water, (b) energy, (c) data, (d) connectivity (internet), (e) city brain, and (f) critical city services (police, fire, banks, healthcare, and transport). Security for smart cities is an emerging topic of importance that requires deeper and further research, and the problem should be viewed as security for a system of systems, from devices to applications, and from providers to users.

5 References

[1] Cybersecurity in smart cities. Master thesis, Lund University, Sweden. Available at http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8950557&fileOId=8950904

[2] Challenges of cybersecurity for smart cities. Available at https://personalpages.manchester.ac.uk/staff/m.dodge/Dodge_Kitchin_Challenges_of_Cybersecurity_for_Smart_Cities.pdf

[3] Cano, J., Berrios, V., Garcia, B., *et al.*: 'Evolution of IoT: an industry perspective', *IEEE Internet Things*, 2018, **1**, (2), pp. 12–17

[4] Zhang, J., Hua, X.-S., Huang, J., *et al.*: 'City brain – practice of large-scale artificial intelligence in the real world', *IET Smart Cities J.*, 2019, **1**, (1), pp. 28–37

[5] Huawei, Leading New ICT: Creating a Smart City 'Nervous System', Huawei. Available at https://e.huawei.com/en/publications/global/ict_insights/201806041630/commentary/201807131639

[6] Huawei Intelligent Operations Center (IOC). Available at https://e.huawei.com/en/solutions/industries/smart-city/ioc

[7] US Environmental Protection Agency – Water System Security & Resilience. Available at https://www.epa.gov/homeland-security-research/water-system-security-and-resilience-homeland-security-research

[8] Public Health Security and Bioterrorism Preparedness and Response Act of 2002. Available at https://www.govinfo.gov/content/pkg/PLAW-107publ188/pdf/PLAW-107publ188.pdf

[9] Amin, S., Giacomoni, A.: 'Smart grid: safe, secure, self-healing', *IEEE Power Energy Mag.*, 2012, pp. 33–40. Available at https://pdfs.semanticscholar.org/4e9c/125ac6a150caed4232adf33f4ce34f4ef682.pdf?_ga=2.133390475.444503469.1556531750-2067409591.1556531750

[10] Toft, P., Duero, A., Bieliauskas, A.: 'Terrorist targeting and energy security', *Energy Policy*, 2010, **38**, (8), pp. 4411–4421

[11] ETSD: Energy Transmission, Storage and Distribution, Report, 2015. Available at https://www.energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf

[12] PWC – PWC's Global Blockchain Survey, 2018. Available at https://www.pwccn.com/en/research-and-insights/publications/global-blockchain-survey-2018/global-blockchain-survey-2018-report.pdf

[13] 'Bluetooth security', Electronic Notes. Available at https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php

[14] 'Securing the LORA networks', Gemalto, 2016. Available at https://www.pole-scs.org/wp-content/uploads/2018/03/LoRa-Security-20160315-Pole-SCS.pdf

[15] 'LORAWAN security white paper', LORA Alliance, 2017. Available at https://lora-alliance.org/sites/default/files/2018-04/lora_alliance_security_whitepaper.pdf

[16] 'Make things come alive in a secure way', SIGFOX, Technical White Paper, 2017

[17] 'Guide to LTE security', NIST, 2017. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

[18] Equifax Data Breach, Fortune Magazine, 2018. Available at http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

[19] Yahoo agrees to $50 million settlement for those affected by the 2013 data breach, Fortune Magazine, 2018. Available at http://fortune.com/2018/10/24/yahoo-settlement-data-breach/

[20] 'Citigroup data breach: a lesson and warning for all', Forbes Magazine, 2011

[21] 'Standard chartered says bank client data stolen in Singapore', Bloomberg News, 2013

[22] EUR-Lex: 'Regulation (EU) 2016/679 of the European parliament and of the council'. Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj

[23] EUR-Lex: 'Directive (EU) 2016/680 of the European parliament and of the council', 2016

[24] US Congress: 'Electronic signatures in global and national commerce act', 2000. Available at https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

[25] Department of Homeland Security: 'Homeland security act of 2002'. Available at https://www.dhs.gov/homeland-security-act-2002

[26] US Senate: 'Federal information security modernization act of 2014'. Available at https://www.congress.gov/bill/113th-congress/senate-bill/2521

[27] Ream, J., Chu, Y., Schatsky, D.: 'Upgrading blockchains: smart contract use cases in industry'. Deloitte Report, 2016. Available at https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovatie-upgrading-blockchains-smart-contract-use-cases-in-industry.pdf

[28] 'E-Estonia guide', 2018. Available at https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf

[29] 'Smart Dubai: blockchain insights', 2019. Available at https://www.smartdubai.ae/docs/default-source/default-document-library/blockchain-insights-report-en.pdf

[30] Gupta, S.: 'Using blockchains in smart cities', Meetings of The Mind, 2018. Available at https://meetingoftheminds.org/using-blockchain-in-smart-cities-29319

[31] Schwede, S.: 'Estonia digital transformation', 2017. Available at http://www.e-konference.eu/sites/default/files/estonias_digital_transformation_-_sten_schwede.pdf

[32] 'Blockchain: A potential life changer for life insurance', Technical Report, Cognizant, 2017. Available at https://www.cognizant.com/whitepapers/blockchain-a-potential-game-changer-for-life-insurance-codex2484.pdf

[33] ENISA: 'Cyber security for smart cities – an architecture model for public transport', Report, 2015

[34] Smart Cities Cyber Security Management, Consultancy Report. Available at https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-SCCCM.pdf

[35] NIST: 'Framework for improving critical infrastructure cybersecurity', 2018

[36] New global cybersecurity standard for smart cities and critical infrastructure released, Smart Energy International Magazine, 2019

[37] 'Cybersecurity, data protection, and cyber resilience', Technical Report, FG-SSC, ITU-T, 2015

[38] Reuters News: 'Face off: realistic masks made in Japan find demand from tech, car companies', 2018. Available at https://www.reuters.com/article/us-japan-masks-facial-recognition/face-off-realistic-masks-made-in-japan-find-demand-from-tech-car-companies-idUSKCN1NK1VT

[39] BBC News: 'The fake French minister in a silicone mask who stole millions', 2019. Available at https://www.bbc.com/news/world-europe-48510027

[40] BBC News: 'Nigeria's secret service arrest 'fake first lady'', 2018. Available at https://www.bbc.com/news/world-africa-46438909