CHAPTER
7

Blockchain: Technologies for Facilitating Cyber-Physical Security in Smart Built Environment

Jong Han Yoon[1], Xinghua Gao[2] and Pardis Pishdad-Bozorgi[1*]

[1] School of Building Construction, Georgia Institute of Technology, USA
[2] Myers-Lawson School of Construction, Virginia Polytechnic Institute and State University, USA

7.1 Introduction

In smart built environments, people's lives digitally connect with city services, buildings, infrastructures, and utilities through information and communication technologies (ICTs) (Gračanin *et al*., 2015). Typically, a smart built environment may consist of components, such as smart cities, smart grids, smart buildings, and smart devices.

In a smart city, the digital connection between people's lives and city services will provide people with a better quality of life, a better social life, and energy sustainability through optimized city services management based on the analysis of the information on digital connections (Zubizarreta *et al*., 2016). These connections are enabled by ICTs, such as the Internet of Things (IoT) technology and cloud technology (Baig *et al*., 2017; Zang *et al*., 2017). The technologies also make electric power grids more energy-efficient and reliable by collecting and providing energy-associated information, thus informing generators' and consumers' decisions for an optimal energy management (Gunduz and Das, 2020). These new technologies-enabled grids are typically called 'smart grids'. Compared with traditional power grids, the smart grids provide more reliable, secure, and economical transmission of electricity by protecting,

*Corresponding author: pardis.pishdad@gatech.edu

monitoring, analyzing, and controlling the electricity transmission processes (Gunduz and Das, 2020). The technologies (i.e. IoT and cloud) also empower smart buildings, which enable building occupants to have more convenient and comfortable lives because the building systems are optimally operated and controlled with advanced technologies, such as Big Data engineering and IoT (Jia *et al*., 2019); for instance, Building Automation System (BAS), which is a complex network-based distributed control system enabling communication and cooperation of electrical/mechanical subsystems, provides optimized control of HVAC, lighting, and air humidity and also manages building security and safety (Wang *et al*., 2015). Smart devices assist other components of the smart built environments (i.e. smart city, smart grid, and smart building) by enabling them to collect and process associated data from a physical world and connecting the smart built environments so that they can exchange data for their operations (Silverio-Fernández *et al*., 2018).

Since the ICT applications in the smart built environments are continually increasing and evolving, the potential benefits that the smart built environments can provide are also growing. However, coupled with the advantages of smart built environments are some concerning disadvantages, like cyber attacks. With an increase usage of ICT applications, the smart built environments are increasingly subjected to cyber attacks. The threat of cyber attack to smart built environments has been investigated by many researchers (Overman *et al*., 2011; Wang *et al*., 2015; Paridari *et al*., 2016; Baig *et al*., 2017; Minoli *et al*., 2017). In smart built environments, cyber attacks will be more serious because they directly impact people's lives. In this setting, the cyber security risks and physical security risks are resulting into Cyber-Physical Security risks. Such risks can be substantial when huge quantities of data, collected and processed by ICT to operate smart built environments, are attacked (AlDairi, 2017). In the case of smart buildings, the private data of occupants, such as their location or behavior patterns, can be stolen from ICT platforms and exploited with criminal intent (Do *et al*., 2018); for example, criminals may disable a smart building's security system via cyber attack, taking over the assess control, which endangers the occupants. In the context of Smart Grid, cyber attack can lead to breaks in national security, disruption of public order, and loss of life or large-scale economic damage (Vitunskaite *et al*., 2019; Gunduz and Das, 2020).

Blockchain technology has the potential to mitigate the threats and risks of cyber attacks against smart built environments. The blockchain can generate a data platform for IoT systems in which data theft and tampering are basically impossible with its hash function, consensus mechanism, and capability of distributing the data transaction records to every participant (Samaniego and Deters, 2016). Even though these benefits can enhance cyber security of smart built environments, a limited number

of studies demonstrate that the blockchain-based data sharing platform can enhance the security for the smart built environments (Biswas and Muthukkumarasamy, 2016; Aung and Tantidham, 2017; Dorri *et al*., 2017; Mylrea and Gourisetti, 2017; Pop *et al*., 2018; Qu *et al*., 2018; Minoli, 2019; Agung and Handayani, 2020; Makhdoom *et al*., 2020, Qashlan *et al*., 2020) {Gunduz, 2020 #152}.

In this chapter, through literature reviews, the authors investigate the potential of blockchain in mitigating cyber-physical risks in the smart built environments. The authors highlight key aspects of the Cyber-Physical Security and risks, discuss potential of blockchain for addressing them, and propose future research directions to enlighten new researchers.

7.2 Cyber-physical Risks in Smart Built Environments

This section discusses the definition of each layer of smart built environments and reviews the literature regarding the cyber-physical risks according to the type. The smart built environments are characterized with separate layers: Smart city, smart infrastructure, smart buildings, and smart devices. Even though the smart city consists of numerous smart components (e.g. smart infrastructure, smart transportation, smart governance, smart services, etc.), in this section, the authors address the built-environment components, such as smart infrastructures, buildings, and devices. In addition, the authors focus on the energy network of smart infrastructures, which is the smart grid. These components are interconnected with each other through ICTs, such as IoT devices, cloud database, and Big Data. This interconnection enables the operation of the smart city (Mohanty *et al*., 2016) (Fig. 7.1). Because each layer has its specific cyber-physical risks, focusing on the unique characteristics of each layer will clarify the differences among the reviewed works.

7.2.1 What is Smart City?

Although a great number of studies define what a smart city is, the authors refer to the definition that highlights the connection between smart systems and people's lives through Cyber-Physical Systems (CPSs). CPSs use internet network and integrating computational technologies to access data, process data, and impact surrounding physical environment (Monostori, 2018).

Smart cities are resilient, facilitate mobility, add efficiencies, conserve energy, improve the quality of air and water, identify and solve problems quickly, recover rapidly from disasters, collect data to make better decisions, deploy resources effectively, and share data to enable

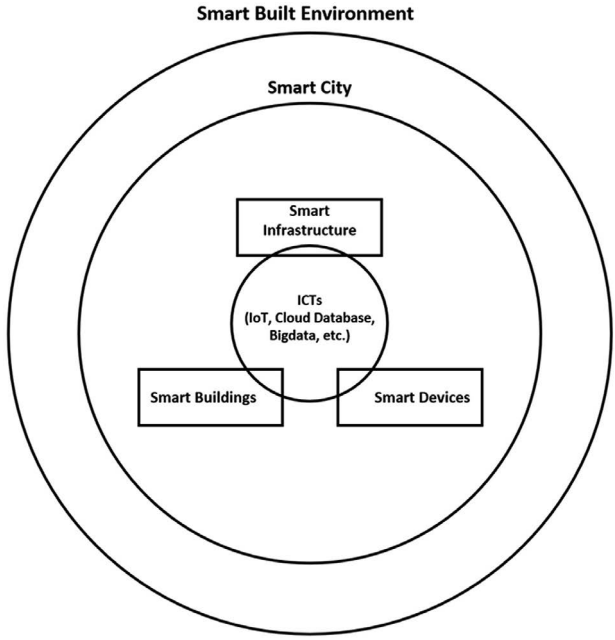

Fig. 7.1: Layers of smart built environment (adapted from Mohanty *et al*., 2016)

collaboration across entities and domains by infusing information into the cities physical infrastructure (Nam and Pardo, 2011). By utilizing the collected data and information-infused infrastructure, the cities can promote the quality of people's lives in the city in a more timely, effective, and energy-efficient way (Chamoso *et al*., 2020). Harrison *et al*. (2010) notes that in smart cities, the traditional concept of a physical city is extended to a virtual city, which utilizes ICT to physically impact people's lives. Not only are the ICT applications important for the definition of the smart city, but their impacts on the people's educational capital, social and relational capital, and environmental issues are also significant (Lombardi *et al*., 2012). Marsal-Llacuna *et al*. (2015) state, "*The smart cities initiative seeks to improve urban performance by using data, information and Information Technologies (IT) to provide more efficient services to citizens, to monitor and optimize existing infrastructure, to increase collaboration between different economic actors and to encourage innovative business models in both the private and public sectors*." Accordingly, in the smart city, people's quality of life, their decisions about their behavior, and their social life are directly linked to the ICT-applied city infrastructure, which means that cyber attacks on information in the infrastructure can result in severe physical attacks on the real lives of the people in the smart city.

7.2.2 Existing Cyber-Physical Security Risks and Solutions for Smart Cities

As the operation of smart cities heavily depends on ICTs, the cities are vulnerable to cyber attacks, which may lead to significant losses (Vitunskaite *et al*., 2019). The cyber attacks against data that is processed and shared within the city, and any attack can cause problems closely related to people's lives, such as financial loss and private data theft (Chauhan *et al*., 2016). Accordingly, many studies have investigated the cyber security of smart cities in order to prevent or mitigate cyber attacks against the cities.

Wang *et al*. (2015) have proposed a security threat assessment model that can be used to create risk mitigation strategies against cyber intrusions into smart city systems. To develop the assessment model, the authors established a threat model by collecting and analyzing security-associated information in the network and system architecture, operating systems and updates, components and configurations of applications, data and data storage, database schemas, services and roles, and encryptions and external dependencies. From the threat model, the authors generated a list of threats and associated risks, which were combined with an algorithm to calculate the threat factors. They then used these factors to assess the security threats and provide appropriate mitigation strategies. Wang *et al*. (2015) also verified that the mitigation strategies through threat assessment can improve the security of the smart city systems in case-based experiments. However, their study was limited to risk assessment and countermeasures based on assessment. They did not provide a preventive way to protect the smart city systems from cyber attacks. Furthermore, they concluded that their lifecycle threat assessment was too long as in that the second round of assessment and mitigations took three months, which meant the systems would have been exposed to the risks over an unrealistically long time period.

Another study for cyber security risks and solutions was conducted by Baig, Szewczyk *et al*. (2017) to investigate the security threats of data acquired from and stored in the smart city components (i.e. smart grids, BAS, unmanned aerial vehicles (UAV), smart vehicles), which utilize IoT sensors and a cloud-data-storage platform. To mitigate the threats, they highlighted the importance of digital forensic investigation on data. The digital forensic restores and analyzes the data for tracing the data use and identifying the evidence of criminal proceedings (Tully *et al*., 2020). The digital forensic can be especially useful for improving the security of cloud storage, since the storage is connected to internet, which is vulnerable to cyber attacks (Chung *et al*., 2012). Baig *et al*. (2017) found that the forensic investigation on smart cities components that use cloud

storage can help the investigator deeply comprehend the cyber attacks and prevent the resulting negative event. One question that Baig *et al.* (2017) did not address, however, was how integrity of the data in the forensic investigation process can be confirmed and maintained so that it is not tampered with or leaked. Even though the researchers pointed out that the data should be kept tamper-proof for effective forensic investigations, they did not propose how to do this. One limitation of digital forensics is that it is not a proactive means for preventing cyber attacks to smart city components. More research to address proactive and preventive means is required.

The cyber security risks and solutions are also discussed by Zang *et al*. (2017). The article revealed that data can be damaged or corrupted in cloud storage of smart cities unless it has security-enhanced remote data auditing (RDA) protocols. These protocols protect cloud users from deceitful cloud servers, which may hide data loss incidents or delete data intentionally for illicit purposes (Zang *et al*., 2017). The study improved RDA protocols compared to the RDA protocols of Sookhak (2015), which was vulnerable to two *replace*-and-*replay attacks.* A *replace attack* occurs when the server replaces damaged files with undamaged ones, and a *replay attack* occurs when the server deploys previous proofs and associated information to forge a valid proof for a new challenge (Zang *et al*., 2017). The study verified that the proposed RDA protocol can effectively prevent those attacks, something which the previous RDA protocol could not do. Even though the improved protocol can protect cloud users from deceitful cloud servers, the cyber-physical attacks in smart cities can't be completely eliminated because the cyber attacks exist not only in the cloud servers but also in devices, networks, and computational resources (Delgado-Gomes *et al*., 2015).

Some studies addressed the cyber-physical security risks from the aspects of risk cognition and information security management (ISM). Chatterjee *et al*. (2018) quantitatively verified that it is the risk cognition on the cyber security of smart cities that motivates people to use preventive technology against cyber threats in cities. The study also found that the cognition can be effectively achieved through social media, word of mouth, and official organization (e.g. banks, post offices, and financial institutions). These findings emphasize that the awareness of cyber attacks is important for people to prevent them and improve security by providing effective ways to increase awareness. Hasbini *et al*. (2018) investigated the role of ISM in smart city organizations. The study identified organizational factors, which enhance ISM in smart cities, highlighting the importance of information security governance. The identified factors can be utilized to establish an effective organization for smart cities to enhance information security.

Laufs *et al*. (2020) pointed out that the security and privacy issues of smart city systems are relatively neglected when considering that smart technologies increasingly address urban challenges directly affecting people's lives. The authors asserted that the privacy rights and data protection should be considered in the smart city planning processes. Even though the smart technologies generate more efficient city services or effectively mitigate crimes, the people might feel less secure when there is a chance for an unpermitted entity to control their life by using the technologies or to steal and exploit their private data (Laufs *et al*., 2020). While afore-mentioned several articles studied cyber security risks and countermeasures in smart cities, more future research on data ownership and privacy rights are still required.

7.2.3 What is Smart Grid?

The smart grid is a power network enabling a two-way delivery of energy and information, which allows the power industry to optimize energy delivery and help consumers to optimally manage their energy usage (Delgado-Gomes *et al*., 2015; Dileep, 2020; Vaccaro *et al*., 2020). According to the National Institute of Standards and Technology (NIST), the smart grid can be established when the electrical grid domains, such as the generators, distributors, consumers, and operators, are connected and communicate with one another to efficiently deliver sustainable, economic, and secure electricity (SmartGrids, 2012). In this setting, the exchange of data or information among the domains should be secured and transparent so that each domain utilizes them in the intended way to provide smart power services (Vaccaro *et al*., 2020). The operation of a smart grid relies on the information exchange between the energy provider and consumer through the energy data collection and process (Raut *et al*., 2016). Deploying the data, the smart grid maximizes energy efficiency and minimizes energy loss (Mo *et al*., 2011; Kimani *et al*., 2019). To collect and process data, the system utilizes diverse smart devices based on IoT technology (Bekara, 2014; Kimani *et al*., 2019; Gunduz and Das, 2020). Such strong dependencies on digital communication technology make the smart grids more vulnerable to cyber attacks (Gunduz and Das, 2020; Moghadam *et al*., 2020). The data collected and processed from smart devices can critically impact people's lives because our lives are closely associated with city facilities and services consisting of a great number of electrical devices. Cyber attacks on these data can lead to breaks in national security, disruption of public order, and loss of life or large-scale economic damage (Vitunskaite *et al*., 2019; Gunduz and Das, 2020). Consequently, the cyber security risks of the smart grid can be considered as risks to the physical world.

7.2.4 Existing Cyber-Physical Security Risks and Solutions for Smart Grids

The function of smart grids depends significantly on IoT technologies, which make the grids vulnerable to cyber attacks (Gunduz and Das, 2020; Moghadam *et al*., 2020). This is because the components of smart grids (e.g. smart meters and smart appliances), which are connected with one another, allow cyber-attackers to easily achieve unpermitted access to the smart grid network (Mo *et al*., 2011). Cyber attacks against smart grids can lead to security, economic, and even safety problems because grids are closely associated with every aspect of people's lives as they reliably, securely, and economically transmit electricity throughout the city (Vitunskaite *et al*., 2019; Gunduz and Das, 2020). Because of the vulnerability of smart grids and the way they link people's lives, many studies address the need for improved cyber security for smart grids.

Mo *et al*. (2011) pointed out that not only cyber approaches but also physical approaches are required for improving smart grid security which can be compromised by cyber attacks and physical attacks (e.g. using compromised sensors, a shunt to bypass sensors, etc.). Physical attacks can be mitigated through *system theory*, which addresses the properties of the physical system, such as performance, stability, and safety (Mo *et al*., 2011). They classify the attacks on cyber-physical systems in smart grids according to both cyber and physical aspects. Based on these classifications, they proposed a system-theoretic approach by considering the physical aspects in more detail than traditional security and cryptographic approaches, which traditionally focus on cyber attacks. The authors developed detection algorithms and countermeasures to prevent physical attacks against smart grids. These algorithms and countermeasures can be used to complement the traditional cyber-security approaches for an additional layer of protection. This article verified that combining cyber security and system theory can effectively mitigate the cyber-physical risks in smart grids.

Liu *et al*. (2012) systemically analyzed the cyber vulnerabilities of smart grids in two points of view: c*yber security issues* and *privacy issues*. The study classified c*yber security issues* into five topics (i.e. device, networking, dispatching, and management, anomaly detection, others) and provided possible solutions for the problems in each topic through literature reviews. Regarding the *privacy issues,* the article suggested that private information about where the people were and when and what they were doing may be stolen when energy-related data in smart grids are not properly protected. The article also defined what personal information is, investigated privacy concerns, and provided recommendations for addressing the concerns. However, the article is limited to the overview of cyber security and privacy issues and the recommended possible

solutions, but did not verify the effectiveness of the solution-applied systems or theories.

Ashok *et al*. (2014) revealed the increased security risks in the technical initiatives supporting smart grids (e.g. Advanced Metering Infrastructure (AMI), Demand Response (DR), Wide-Area Monitoring, Protection and Control Systems (WAMPAC) based on Phasor Measurement Units (PMU), etc.). The article affirmed that AMI and WAMPAC are more vulnerable to cyber attacks because they heavily depend on cyber infrastructure and its data transfer through several communication protocols to utility control centers and consumers. The article focused on the security of the WAMPAC system because cyber attacks on it can easily cause critical damage to people's lives since the attacks on WAMPAC can impact bulk power system reliability, unlike the attacks on AMI. To protect the Cyber-Physical Security of the WAMPAC system from various coordinated cyber attacks, the article proposed a game-theoretic approach. This approach enables modeling dynamic cyber-attack scenarios, which are useful for obtaining appropriate solution strategies to improve security. However, the article didn't verify how much the solution strategies obtained from this approach mitigate the impact of cyber attacks. To demonstrate the effectiveness, case studies or simulations are required to implement and analyze.

Shapsough *et al*. (2015) discuss four cyber security challenges in smart grids. The challenges contain *connectivity*, *trust*, *customer's privacy*, and *software vulnerabilities*. The *connectivity* issue concerns the fact that numerous devices are connected with one another in the grids and that cyber attacks on smart grids might lead to significant damage to people's lives. The *trust* issue concerns with the possibility of users intentionally damaging the smart meter to falsify energy data for their benefit. The *customer's privacy* concerns with the user's critical private information in smart grids that could potentially be exploited by criminals. The *software vulnerabilities* concerns with software used in the smart grids system that could potentially be vulnerable to malware and malicious update. To address these challenges, the authors validated existing security solutions by analyzing them from five aspects (i.e. network security, data security, key management, network security protocols, and compliance checks) and recommended a new conceptual security model for smart grids. The proposed model allows data in smart devices and systems to be directly transmitted to the application layer through WiFi or 4G internet without going through multiple devices or networks.

Gunduz and Das (2020) classified the security threats against IoT-based smart grids and investigated the potential security solutions for each threat type. They investigated the existing cyber attacks from the aspects of confidentiality, integrity, and availability (CIA) and network layers. Based on the evaluation, the research discussed and examined network

vulnerabilities, attack countermeasures, and security requirements. However, the article is limited to classifying the solutions with the threat types and frame-working the security threats analysis. Although the classification and framework help understand the cyber attacks against smart grids and identify appropriate solutions for them, the limitations of the solutions need to be examined, and a novel approach that can complement the limitation should be proposed.

As another solution for the security issue of smart grids, Moghadam *et al*. (2020) proposed a security-enhanced protocol for communication between substations and a data center in the smart grid network, which is based on hash and private key to overcome the security weakness associated with the International Electrotechnical Commission (IEC) 62351 standard. IEC 62351 is an industry standard for security in automation systems in the power supply system domain (Schlegel *et al*., 2017). In their study, the enhanced security of the proposed protocol is verified with AVISPA software.

All the afore-mentioned studies agree that lack of security in smart grids negatively impacts people's lives by interrupting the power system's operation. Even though the studies proposed several solutions for improving the security, more future research on data authenticity and immutability in the smart grid network is still necessary.

7.2.5 What is Smart Building?

The definition of smart building is evolved from the preliminary definition focusing on the technological aspects to the definition focusing more on the interrelationships between occupants and building systems (Martins *et al*., 2012). According to Linder, Vionnet *et al*. (2017), smart buildings are buildings where the owners, operators, and facility managers can utilize building technology systems (e.g. building management system) connected to a variety of sensors, actuators, and networks with IoT technology in order to improve the reliability and performance of building assets. These systems enable automation control of building systems, promote occupant safety, and facilitate operation management (Sinopoli, 2009). The building technology systems monitor and collect the data of occupants, such as energy usage, user location, and behavior pattern and process the data to generate information that can be used to optimize building services. In this setting, the systems can support people's lives in various ways: inhabitants' comfort, energy savings, time-saving, safety, health and care (Batov, 2015). However, these advantages are accompanied with a risk of cyber attacks that can be extended to the physical world (Tankard, 2016). The building technology systems mainly depend on IoT devices, which are installed all over the smart building (Casado-Vara *et al*., 2020). Given that IoT devices are vulnerable to risks of cyber security attacks (Bertino,

2016; Qian *et al*., 2018; Hassan 2019; Amanullah *et al*., 2020; Waraga *et al*., 2020), the risks can be substantial to people's lives.

7.2.6 Existing Cyber-Physical Security Risks and Solutions for Smart Buildings

The AECO industry is advancing towards the smart building paradigm in which IoT devices and networks are used to improve occupants' comfort, reduce lifecycle costs, and optimize the operation of building systems (Gao and Pishdad-Bozorgi, 2019a; Gao and Pishdad-Bozorgi, 2019b; Gao *et al*., 2019; Tang *et al*., 2019). As the building managers are moving away from the older proprietary systems of the past and adopting new data-intensive, comprehensive building automation and control solutions, there is a desire to gather as much data as possible with lower cost sensors – both wired and wireless (O'Brien, 2019). It is envisioned that in future each building will be 'smart' enough to provide a certain amount of data to the city IoT network in real-time, and the city will provide services in return, such as security, emergency assistance, data connection, and automated operation and maintenance (Gao *et al*., 2019; Pishdad-Bozorgi *et al*., 2020). Although the advantages of this trend are undeniable, this substantial change from traditional, isolated, single-function building systems to a ''system of systems'' integration with existing IoT infrastructures –the Internet and innovative automation devices – exposed smart buildings to significant cyber threats. Moreover, smart buildings are not only subject to known ICT system attacks, but also to a new breed of cyber-physical attacks (Siaterlis *et al*., 2013).

Cyber attacks on smart buildings alone can have many negative impacts that may pose risks to human safety (O'Brien, 2019). Cyber attacks can impact one or multiple smart building cyber security goals, involving confidentiality, authenticity, integrity, authorization, and availability, non-repudiation (Komninos *et al*., 2014; Radanliev *et al*., 2020; Sharma, 2020). Cyber attacks can be classified into passive attacks, which attempt to utilize the data housed in building systems without affecting the operation of systems , or active attacks, which attempt to interrupt system operation or alter its resources (Qi *et al*., 2017).

In cases of passive attacks, the compromised cyber security of a smart building will lead to data leakage, which may result in occupants' behavior being monitored by the malicious party and/or identity theft. For example, if the attackers have access to data regarding the thermostat setting or occupancy history, with enough time-series data, they can use machine learning techniques to identify the occupants' behavior patterns and thus, know when the occupants will be in the building (or a particular room). Another example is the hack at the target retail chain (Wallace, 2013), in which case the remote access privileges of the HVAC system

were exploited to gain access to the target's financial systems, and led to a leak of over 40 million people's credit card information (O'Brien, 2019).

Active attacks tend to disrupt the physical processes and jeopardize the safety properties in the physical world more directly (Wang *et al*., 2017). If a malicious party hacks into the smart building's security system and turns off the security cameras and intrusion alerts, the physical security of the building will also be compromised. Moreover, if a malicious party can take over the access control system, the building will be completely exposed to physical threats. On the other hand, physical security has always been an important part of cyber security – if adversaries can physically access the building system server, equipment, and even some routing devices, the building's cyber security may be in jeopardy. Therefore, in the smart building domain, the cyber security issues and physical security issues are converging into one critical issue that requires extensive research and innovative solutions.

A limited number of research studies have been conducted to improve the Cyber-Physical Security of smart buildings. An effective approach is to enhance the security of building systems; for example, Wang *et al*. (2017) use a security-enhanced, microkernel architecture to ensure the BAS's security in a hostile cyber environment. Another research trend is to create testbeds to simulate smart buildings for cyber-security experimentation (Mekikis *et al*., 2013; Tong *et al*., 2014). Such testbeds are capable of 1) enabling users to specify the building-area network topology, communication protocols and appliances, and developing security mechanisms, such as information flow tracking (Tong *et al*., 2014), and 2) detecting and localizing events (such as water leakages and system failure) in smart buildings (Mekikis *et al*., 2013).

The Cyber-Physical Security of smart buildings is an innovative, interdisciplinary topic. Many issues have emerged but not been thoroughly investigated yet, such as the existing and potential attack models, the risk assessment criteria, and countermeasures under different circumstances. Two major research gaps exist in this area – first, the deployment of smart building applications requires increased cyber-physical interdependencies, hence security issues in smart buildings cannot be fully addressed only by considering the cyber layer (Qi *et al*. 2017). There is yet a framework or testbed to examine the joint effects of cyber attack and physical attack, considering the smart building systems and devices, as well as the building layout. Second, humans tend to be the weak link of the Cyber-Physical Security of smart buildings. Studies on the human-building interaction from a security perspective are in need.

7.2.7 What is Smart Device?

The afore-mentioned smart built environments (i.e. smart city, smart grid, and smart building) should collect and process data from the

physical world and exchange the data across the systems or devices for operation of the smart built environments. This can be achieved by smart devices. Smart devices perceive information from the environment through sensors; process the information automatically without the direct command of the user; and enable the exchange of information among the systems (Silverio-Fernández *et al*., 2018). Silverio-Fernández *et al*. (2018) have defined the smart device as follows: "*A smart device is a context-aware electronic device capable of performing autonomous computing and connecting to other devices wire or wirelessly for data exchange*." The data exchange among smart devices is enabled by IoT technology (Miller, 2015). In addition, the IoT technology enables the systems to sense and control objects, which facilitate integration between the physical world and computer-based systems (Bertino, 2016). However, on the other side, the IoT technology is vulnerable to risks of cyber security attacks (Bertino, 2016; Qian *et al*., 2018; Hassan, 2019; Amanullah *et al*., 2020; Waraga *et al*., 2020). Given that IoT technology is one of the main components for smart built environments (Zanella *et al*. 2014; Waraga *et al*., 2020), the vulnerability can be a serious threat to people's lives in the smart built environments. Therefore, reliable and foolproof solutions need to be developed by creating new technologies or combining existing technologies to address the security issues (Amanullah *et al*., 2020).

7.2.8 Existing Cyber-Physical Security Risks and Solutions for Smart Devices

The security requirements of IoT devices involve: 1) identifying the device itself and its administrative entities, such as a gateway, 2) protecting device hijacking, and 3) protecting the information flow between devices and their administrative entities (Minoli *et al*., 2017; Radanliev *et al*., 2020). As new IoT devices are being invented and implemented for smart building solutions, these new technologies coexist with legacy building systems, such as HVAC, energy management systems, lighting control systems, video surveillance systems, access control systems, elevator control systems that must be managed, maintained, and gradually modernized. The coexistence of new IoT devices and legacy devices creates a mixed-criticality environment in which new attack vectors are introduced (Wang *et al*., 2017).

A study showed how an attacker can obtain full control over some smart building devices by injecting arbitrary audio signals into their microphones via light commands (laser) (Sugawara *et al*.). The researchers breached the security measures of some popular voice assistants, such as Amazon Alexa, Apple Siri, Facebook Portal, and Google Assistant, and showed that user authentication of these devices is often lacking or non-existent, allowing the attacker to unlock the target's smart lock-

protected front doors, open garage doors, shop on e-commerce websites at the target's expense, or even locate, unlock, and start various vehicles (e.g. Tesla and Ford) that are connected to the target's account. The study revealed several vulnerabilities in today's smart building devices besides highlighting lack of an efficient approach to measure and mitigate the impact of cyber threats on both the cyber and the physical parts of smart buildings.

The cyber-security challenge has always been an obstacle to the popularization of IoT technologies in smart buildings. Minoli *et al*. (2017) summarized the IoT-related challenges in the building sector. Those related to the cyber risks of devices are:

Intrinsic IoT security issues: Most of the software codes in the IoT ecosystems have exploitable vulnerabilities. Moreover, if a device is not protected physically, adversaries can access the device via physical attacks, and the rest of the IoT ecosystem.

Low-complexity devices: Limit the amount of computing power needed for encryption, firewalling, and deep packet analysis.

Limited on-board power: Limits the amount of computing needed for security algorithms.

Accessibility: Devices may be in an open environment, where they can be physically tampered with or stolen.

Device mobility: Portable devices may be placed in some 'foreign' network of unknown security status.

Active system: IoT devices are always connected; hence they are more susceptible to cybersecurity attacks.

System size: Scalable solutions are in need to incorporate a large number of IoT devices in the 'system'.

Many devices and access points are required in smart building deployments, and this presents additional cyber risks because of the devices operating outside the traditional facilities management domain. To solve this problem, enhanced attack prevention, detection, and mitigation approaches should be implemented at both the cyber and physical layers (Qi, Kim *et al*., 2017). Threats and risks of cyber attacks can be effectively mitigated with the blockchain technology.

Blockchain can generate a data platform for IoT systems in which data theft and tampering are basically impossible with its hash function, consensus mechanism, and capability of distributing the data transaction records to every participant (Samaniego and Deters, 2016). These benefits enable the smart devices to provide additional security to people living in smart built environments.

7.3 Blockchain Technology for Cyber-Physical Security of Smart Built Environments

This section discusses what the blockchain technology (blockchain) is and how it can enhance Cyber-Physical Security of smart built environments. The section provides an explanation of the two main features of blockchain – decentralized network and tamper-proof digital storage, and examines how these two features can enhance the security. It also reviews various studies on blockchain-based security enhancement of the smart built environments.

7.3.1 What is Blockchain Technology and How It can Enhance Cyber-Physical Security on Smart Built Environments?

Blockchain is a database that enables peer-to-peer data transactions in a tamper-proof environment through two main features – *decentralized Network with timestamp* and *linked data list through hash function in conjunction with consensus protocol.*

7.3.2 Decentralized Network with Timestamp

Unlike traditional databases, blockchain doesn't have a single entity that manages and stores data transaction records (Abeyratne and Monfared, 2016; Aung and Tantidham, 2017). Instead, in the blockchain network, all the nodes in the network will be the actual users, whose records blockchain replicates with timestamps of each transaction and then stores them in every node in the network (Fig. 7.2). All the users of this network can see every transaction record with the timestamp. This is the reason why blockchain is called a decentralized (or distributed) ledger. In this ledger, no individual record can be removed unless all the records in all the nodes are removed (Aung and Tantidham, 2017). This prevents the two biggest weaknesses of traditional database: data loss (Jiang *et al*., 2017; Gatteschi *et al*., 2018; Saraf and Sabadra, 2018) and single point of failure (Wang *et al*., 2018; Xiong *et al*., 2018; Yakubov *et al*., 2018).

7.3.3 Linked Blocks with Hash and Consensus Protocol

Despite the advantages of decentralization, it cannot ensure complete data integrity and authenticity (Oh, 2017). To achieve data integrity and authenticity, blockchain leverages a *hash function* in conjunction with a *consensus protocol.* The *hash function* is used to convert data into a hash value, which is a random combination of numbers and letters. Any small change in data will give the data a completely different hash value. This feature ensures data integrity and authenticity. For instance, users will see when the existing data have been tampered with (integrity destruction)

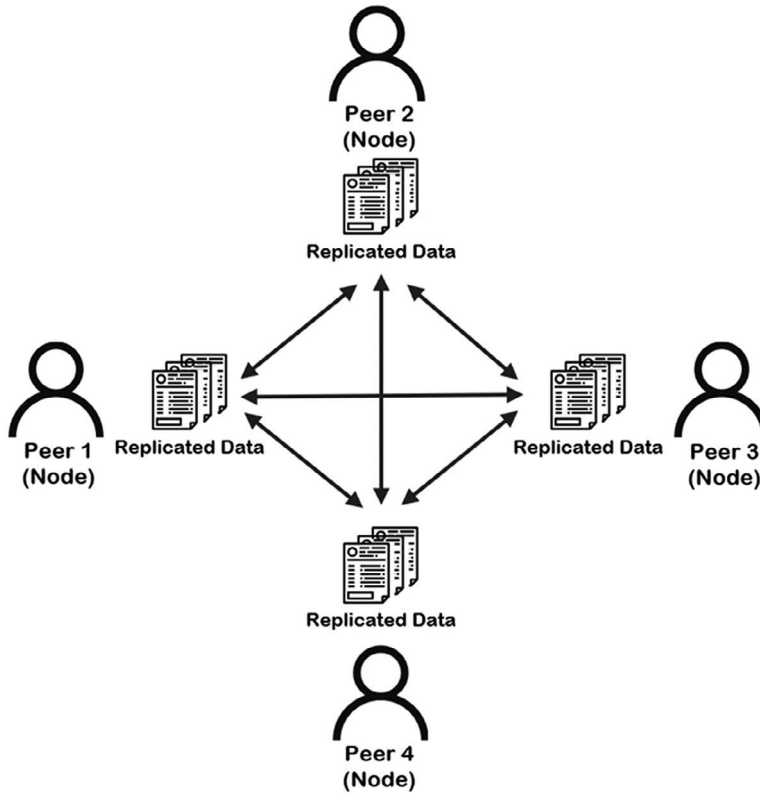

Fig. 7.2: Peer-to-peer transaction-based distributed ledger

or the counterfeited data are newly added (authenticity destruction), as the hash value of the block containing the data will change. The users can verify the integrity and authenticity of the block by comparing the original hash value with the changed hash value. In blockchain, the hash values link blocks with each other. Each block has its own hash value, which is computed of the hash value of the transaction data in the current block, the hash value of the previous block, timestamp, and nonce, which is an arbitrary number. This creates the link between blocks (Fig. 7.3), which makes it much more difficult for anyone to tamper with the transaction data in the blocks (Lisk, 2019).

If an attacker changes any of the data in one block, the attacker must also create a corresponding change in the next block, which includes the changed hash value of the attacked block. However, to create the next new block, the attacker must satisfy the consensus protocol, such as proof-of-work (Mougayar, 2016). The proof-of-work is a process to find out the proper nonce for creating the hash value of the new block (Whittle, 2018).

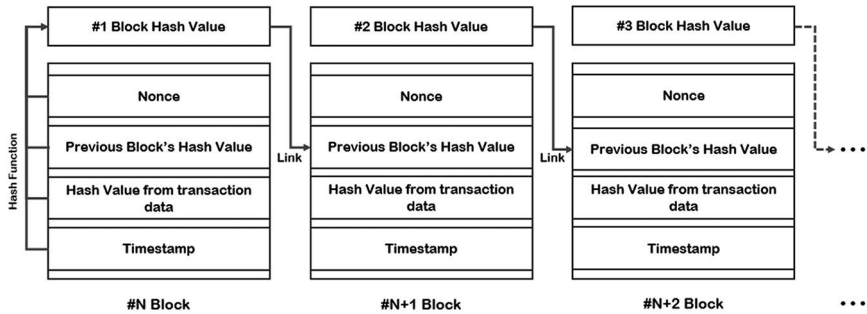

Fig. 7.3: Linked blocks with hash

Even though the attacker can create the new blocks by identifying the proper nonce, the falsified blockchain should be longer than the original blockchain in order to be considered an official blockchain (Fig. 7.4). Because the proof-of-work needs substantial computing power and processing time, it is nearly impossible that the attacker gets falsified blockchain to be the official one by being longer than the original blockchain in which other nodes are continually creating authenticated blocks. In conclusion, in the blockchain network, either tampering with the existing data or adding unauthenticated data is nearly impossible.

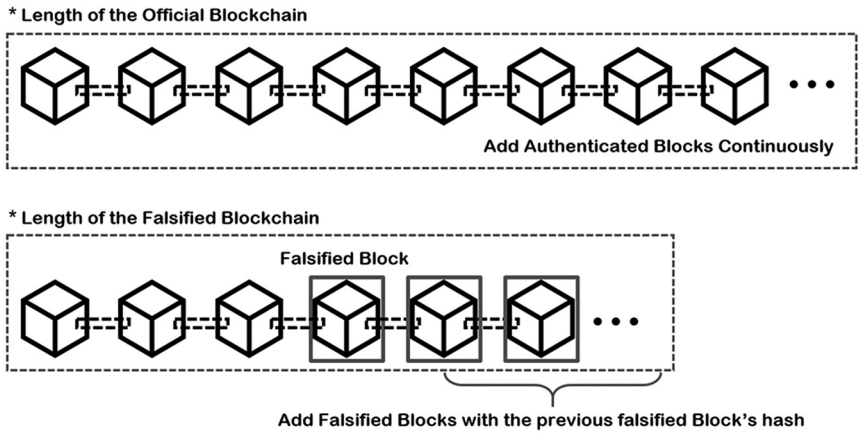

Fig. 7.4: Selecting process for an official blockchain

7.3.4 Enhancing Cyber Security and Privacy of Smart Built Environments through Blockchain

As discussed in previous sections, smart built environments are very vulnerable to cyber attacks, which can lead to significant risks to people's lives. A major reason for vulnerability stems from the two main characteristics of the environment: 1) *cloud database utilization* and 2) *IoT-*

and ICT-based devices application. The cloud database employment causes risks, such as a single point of failure, data loss and breach, and data integrity and authenticity destruction (Xie *et al*., 2020). The IoT- and ICT-based devices' application causes risks, such as data loss and breach, data integrity and authenticity destruction, and physical attacks on devices. While these risks are the focus of a growing debate about cyber security of smart built environments, a preventive way to eliminate these Cyber-Physical Security risks is often neglected.

The majority of these risks can be eliminated or substantially mitigated by two aforementioned features of blockchain (i.e. *decentralized network* and *linked blocks by hash and consensus protocol*), and this will enhance the Cyber-Physical Security of smart built environments.

The data decentralization of blockchain can effectively prevent the single point of failure and data loss and breach (Xie *et al*., 2020). Although decentralization is not proper for preventing the data breach because all the data in blockchain should be replicated and shared with every user, this drawback can be complemented by establishing private blockchain with data encryption technology (e.g. the hash function). Furthermore, data links by hash and consensus protocol of blockchain can strongly protect data integrity and authenticity. This can help prevent the destruction of data integrity and authenticity in the operating systems of smart built environments. Despite these two countermeasures from blockchain applications, the smart built environments still face the risk of physical attack on the devices which are used for operating the environment. These findings are summarized in Fig. 7.5.

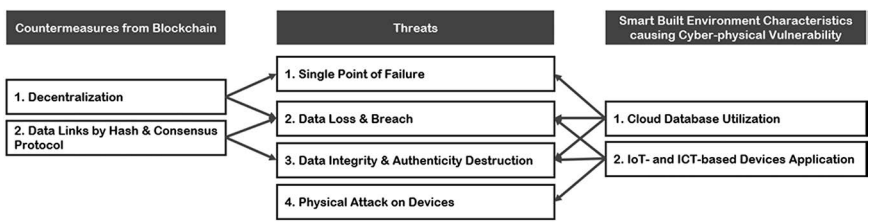

Fig. 7.5: Threats and countermeasures of cyber-physical risks in smart built environments

7.3.5 Literature Reviews on Blockchain Application to Smart Built Environments

Multiple studies have found that blockchain applications effectively address cyber security threats in smart built environments (Biswas and Muthukkumarasamy, 2016; Aung and Tantidham, 2017; Dorri *et al*., 2017; Mylrea and Gourisetti, 2017; Pop *et al*., 2018; Qu *et al*., 2018; Minoli, 2019;

Agung and Handayani, 2020; Makhdoom *et al*., 2020, Qashlan, Nanda *et al*., 2020).

Biswas and Muthukkumarasamy (2016) and Makhdoom *et al*. (2020) pointed out that the data collected and processed by IoT systems in smart cities are vulnerable to availability, integrity, and privacy threats. As a countermeasure to the threats, these studies proposed a blockchain-based security framework, which enables users to engage in privacy-preserving and secure IoT data sharing in smart city environments. Other studies (Mylrea and Gourisetti, 2017; Pop *et al*., 2018; Agung and Handayani, 2020) utilized *smart contract*, which can be implemented by blockchain, to build a more secure and reliable smart grid system against security threats. A *smart contract* is a computer protocol intended to digitally facilitate or enforce automatic data-transaction processes by providing rules and penalties (Rosic, 2016). With a *smart contract*, the data satisfying the rules for transaction can be automatically processed in the system. This can help smart grids to automatically balance energy demand with energy production (Pop, Cioara *et al*., 2018). The reason why this protocol can function is that the transaction data in blockchain are trustworthy since the blockchain guarantees the integrity and authenticity of the data. In smart grids, blockchain can keep energy transaction data secured and simultaneously can supply reliable electricity more efficiently (Mylrea and Gourisetti, 2017; Pop *et al*., 2018; Agung and Handayani, 2020). Blockchain application also has the potential to improve the security of smart homes that use IoT devices. Examples can be found in several studies (Aung and Tantidham, 2017; Dorri *et al*., 2017; Minoli, 2019; Qashlan *et al*., 2020). Aung and Tantidham (2017) found that private blockchain can improve security and protect the privacy of the IoT device-based data against cyber-attacks. Dorri *et al*. (2017) proposed lightweight instantiation of a blockchain application system for IoT devices in smart homes and verified that the overhead incurred by the proposed system is insignificant when compared with the benefits of security and privacy. Qashlan *et al*. (2020) developed a private blockchain-based smart security solution for smart homes in which only the home owner could access and monitor home appliances, by utilizing ethereum smart contract. The study designed simple smart contracts to enable smart devices to communicate without the need for trusted third party. Qu *et al*. (2018) noted that the existing blockchain is not proper for IoT devices in smart homes, which have less energy and memory. To overcome this limitation, the study proposed a hypergraph-based blockchain model, which can provide more efficient network storage than the traditional blockchain network did, so that the IoT devices can obtain the security and privacy benefits from blockchain.

Even though the benefits of these blockchain applications are understood and accepted, few studies have investigated what type of physical risks can be caused by the security and privacy threats from

cyber attacks against smart built environments or how the blockchain applications, which enhance cyber security and privacy, mitigate the physical risks and enhance people's safety in smart built environments. Future research in this area is necessary to investigate if blockchain can be one of the most effective ways to enhance Cyber-Physical Security. Also necessary is future research regarding the assessment parameters and the testbed framework.

7.4 Conclusion

As smart built environments are continually growing and evolving, so do cyber-physical risks. These risks can negatively impact people's lives. Cyber attacks against smart built environments can lead to city service malfunction, energy supply failure, private data breach, building operation system misuse, etc. Despite these significant impacts, most current research has focused on cyber security. Relatively few studies have investigated cyber-physical threats and risks in smart built environments or proposed proper countermeasures for preventing them.

One effective countermeasure can be blockchain, which has the potential to serve as a data platform for IoT systems in which data theft and tampering are basically impossible because of its hash function, consensus mechanism, and capability of distributing the data transaction records to every participant (Samaniego and Deters, 2016). These benefits can enhance cyber security of smart built environments. Multiple studies have demonstrated that blockchain applications effectively address cyber security threats in smart built environments. Nevertheless, the studies on physical risks caused by the cyber attacks are still missing, and few studies have addressed how the cyber security achieved by blockchain can extend to people's lives in smart built environments.

This chapter contributes to the body of knowledge on Cyber-Physical Security by discussing the definition of each layer of smart built environment and reviewing the relevant literature regarding the cyber-physical risks. The literature reviews investigate risks and explore the existing solutions for mitigating the risks. Through these reviews, this chapter demonstrates that more studies on cyber-physical risks and threats are required to develop proper countermeasures. This chapter also includes reviews of existing literature on blockchain for the smart built environments. It demonstrates that blockchain technology can enhance the Cyber-Physical Security in smart built environments through its security-enhancing system. However, more studies involving use cases are required to demonstrate how blockchain enhances cyber security and impacts people's lives.

References

Abeyratne, S.A. and Monfared, R.P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9): 1-10.

Agung, A.A.G. and Handayani, R. (2020). Blockchain for smart grid. *Journal of King Saud University - Computer and Information Sciences*. (In Press)

AlDairi, A. (2017). Cyber security attacks on smart cities and associated mobile technologies. *Procedia Computer Science*, 109: 1086-1091.

Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M. and Imran, M. (2020). Deep learning and big data technologies for IoT security. *Computer Communications*, 151: 495-517.

Ashok, A., Hahn, A. and Govindarasu, M. (2014). Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *Journal of Advanced Research*, 5(4): 481-489.

Aung, Y.N. and Tantidham, T. (2017). Review of Ethereum: Smart home case study. 2017 2nd International Conference on Information Technology (INCIT), IEEE.

Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnston, M., Kerai, P., Ibrahim, A. and Sansurooah, K. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22: 3-13.

Batov, E.I. (2015). The distinctive features of 'smart' buildings. *Procedia Engineering*, 111: 103-107.

Bekara, C. (2014). *Security Issues and Challenges for the IoT-based Smart Grid*. FNC/MobiSPC.

Bertino, E. (2016). *Data Security and Privacy in the IoT*. EDBT.

Biswas, K. and Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE.

Casado-Vara, R., Martin-del Rey, A., Affes, S., Prieto, J. and Corchado, J.M. (2020). IoT network slicing on virtual layers of homogeneous data for improved algorithm operation in smart buildings. *Future Generation Computer Systems*, 102: 965-977.

Chamoso, P., González-Briones, A., De La Prieta, F., Venyagamoorthy, G.K. and Corchado, J.M. (2020). Smart city as a distributed platform: Toward a system for citizen-oriented management. *Computer Communications*, 152: 323-332.

Chatterjee, S., Kar, A.K., Dwivedi, Y.K. and Kizgin, H. (2018). Prevention of cyber crimes in smart cities of India: From a citizen's perspective. *Information Technology & People*, 32(5): 1153-1183.

Chauhan, S., Agarwal, N. and Kar, A.K. (2016). Addressing big data challenges in smart cities: A systematic literature review. *Info*, 18(4): 73-90.

Chung, H., Park, J., Lee, S. and Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital Investigation*, 9(2): 81-95.

Delgado-Gomes, V., Martins, J.F., Lima, C. and Borza, P.N. (2015). Smart grid security issues. 2015 9th International Conference on Compatibility and Power Electronics (CPE), IEEE.

Dileep, G. (2020). A survey on smart grid technologies and applications. *Renew. Energy*, 146: 2589-2625.

Do, Q., Martini, B. and Choo, K.K.R. (2018). Cyber-physical systems information gathering: A smart home case study. *Computer Networks*, 138: 1-12.

Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops), IEEE.

Gao, X. and Pishdad-Bozorgi, P. (2019). BIM-enabled facilities operation and maintenance: A review. *Advanced Engineering Informatics*, 39: 227-247.

Gao, X. and Pishdad-Bozorgi, P. (2019). A framework of developing machine learning models for facility lifecycle cost analysis. *Building Research & Information*, 1-25.

Gao, X., Pishdad-Bozorgi, P., Shelden, D. and Tang, S. (2019). A Scalable Cyber-Physical System Data Acquisition Framework for the Smart Built Environment. The 2019 ASCE International Conference on Computing in Civil Engineering, Atlanta, GA, ASCE.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. and Santamaria, V. (2018). To blockchain or not to blockchain: That is the question. *IT Professional*, 20(2): 62-74.

Gračanin, D., Matković, K. and Wheeler, J. (2015). An approach to modeling internet of things based smart built environments. 2015 Winter Simulation Conference (WSC), IEEE.

Gunduz, M.Z. and Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*: 107094.

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J. and Williams, P. (2010). Foundations for smarter cities. *IBM Journal of Research and Development*, 54(4): 1-16.

Hasbini, M.A., Eldabi, T. and Aldallal, A. (2018). Investigating the information security management role in smart city organisations. *World Journal of Entrepreneurship, Management and Sustainable Development, Info*, 18(4): 73-90.

Hassan, W.H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, 148: 283-294.

Jia, M., Komeily, A., Wang, Y. and Srinivasan, R.S. (2019). Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications. *Automation in Construction*, 101: 111-126.

Jiang, P., Guo, F., Liang, K., Lai, J. and Wen, Q. (2017). Searchain: Blockchain-based private keyword search in decentralized storage. *Future Generation Computer Systems*, 107: 787-792.

Kimani, K., Oduol, V. and Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25: 36-49.

Komninos, N., Philippou, E. and Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4): 1933-1954.

Laufs, J., Borrion, H. and Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, 102023.

Linder, L., Vionnet, D., Bacher, J.-P. and Hennebert, J. (2017). Big Building Data – A Big Data platform for smart buildings. *Energy Procedia*, 122: 589-594.

Lisk. (2019). What is Blockchain? https://lisk.io/what-is-blockchain

Liu, J., Xiao, Y., Li, S., Liang, W. and Chen, C.P. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys and Tutorials*, 14(4): 981-997.

Lombardi, P., Giordano, S., Farouh, H. and Yousef, W. (2012). Modelling the smart city performance. *Innovation: The European Journal of Social Science Research*, 25(2): 137-149.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J. and Ni, W. (2020). Privy Sharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers and Security*, 88: 101653.

Marsal-Llacuna, M.-L., Colomer-Llinàs, J. and Meléndez-Frigola, J. (2015). Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative. *Technological Forecasting and Social Change*, 90: 611-622.

Martins, J., Oliveira-Lima, J., Delgado-Gomes, V., Lopes, R., Silva, D., Vieira, S. and Lima, C. (2012). Smart homes and smart buildings. 2012 13th Biennial Baltic Electronics Conference, IEEE.

Mekikis, P.-V., Athanasiou, G. and Fischione, C. (2013). A wireless sensor network testbed for event detection in smart homes. 2013 IEEE International Conference on Distributed Computing in Sensor Systems, IEEE.

Miller, M. (2015). *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World*. Pearson Education.

Minoli, D. (2019). Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. *Internet of Things*, 100147.

Minoli, D., Sohraby, K. and Occhiogrosso, B. (2017). IoT considerations, requirements, and architectures for smart buildings – Energy optimization and next-generation building management systems. *IEEE Internet of Things Journal*, 4(1): 269-283.

Mo, Y., Kim, T.H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A. and Sinopoli, B. (2011). Cyber-physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1): 195-209.

Moghadam, M.F., Nikooghadam, M., Mohajerzadeh, A.H. and Movali, B. (2020). A lightweight key management protocol for secure communication in smart grids. *Electric Power Systems Research*, 178: 106024.

Mohanty, S.P., Choppali, U. and Kougianos, E. (2016). Everything you wanted to know about smart cities: The internet of things is the backbone. *IEEE Consumer Electronics Magazine*, 5(3): 60-70.

Monostori, L. (2018). Cyber-physical systems. The International Academy for Production. *CIRP Encyclopedia of Production Engineering*: 1-7.

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons.

Mylrea, M. and Gourisetti, S.N.G. (2017). *Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security*, 2017 Resilience Week (RWS), IEEE.

Nam, T. and Pardo, T.A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times.

O'Brien, L. (2019). Cybersecurity for Smart Buildings. https://www.arcweb.com/blog/cybersecurity-smart-buildings.

Oh, M.W. (2017). "블록체인한번에이해하기 (Korean Title). https://homoefficio.github.io/2017/11/19/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%ED%95%9C-%EB%B2%88%EC%97%90-%EC%9D%B4%ED%95%B4%ED%95%98%EA%B8%B0/

Overman, T.M., Sackman, R.W., Davis, T.L. and Cohen, B.S. (2011). High-assurance smart grid: A three-part model for smart grid control systems. *Proceedings of the IEEE*, 99(6): 1046-1062.

Paridari, K., Mady, A.E.-D., La Porta, S., Chabukswar, R., Blanco, J., Teixeira, A., Sandberg, H. and Boubekeur, M. (2016). Cyber-Physical-Security framework for building energy management system. 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), IEEE.

Pishdad-Bozorgi, P., Shelden, D. and Gao, X. (2020). Introduction to Cyber-Physical Systems in the Built Environment. Sawhney, Riley, M. and Irizarry, J. (Ed.). Construction 4.0: An Innovation Platform for the Built Environment. Taylor and Francis.

Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I. and Bertoncini, M. (2018). Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors*, 18(1): 162.

Qashlan, A., Nanda, P. and He, X. (2020). Automated ethereum smart contract for block chain based smart home security. pp. 313-326. *In:* Smart Systems and IoT: Innovations in Computing. Springer.

Qi, J.J., Kim, Y., Chen, C., Lu, X.N. and Wang, J.H. (2017). Demand response and smart buildings: A survey of control, communication, and cyber-physical security. *ACM Transactions on Cyber-Physical Systems*, 1(4): 1-25.

Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M. and Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering*, 72: 266-273.

Qu, C., Tao, M. and Yuan, R. (2018). A hypergraph-based blockchain model and application in Internet of Things-enabled smart homes. *Sensors*, 18(9): 2784.

Radanliev, P., De Roure, D.C., Nurse, J.R., Montalvo, R.M., Cannady, S., Santos, O., Burnap, P. and Maple, C. (2020). Future developments in standardisation of cyber risk in the Internet of Things (IoT). *SN Applied Sciences*, 2(2): 169.

Raut, M.M., Sable, R.R. and Toraskar, S.R. (2016). Internet of Things (IoT) based smart grid. *International Journal of Engineering Trends and Technology (IJETT)*, 34: 15-20.

Rosic, A. (2016). Smart Contracts: The blockchain technology that will replace lawyers. Retrieved from https://blockgeeks.com/guides/smart-contracts/

Samaniego, M. and Deters, R. (2016). Blockchain as a Service for IoT. 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (Smart Data), IEEE.

Saraf, C. and Sabadra, S. (2018). Blockchain platforms: A compendium. 2018 IEEE International Conference on Innovative Research and Development (ICIRD), IEEE.

Schlegel, R., Obermeier, S. and Schneider, J. (2017). A security evaluation of IEC 62351. *Journal of Information Security and Applications*, 34: 197-204.

Shapsough, S., Qatan, F., Aburukba, R., Aloul, F. and Al Ali, A. (2015). Smart grid cyber security: Challenges and solutions. 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), IEEE.

Sharma, A. (2020). Impact of cyber risks from Internet of Things. *TEST Engineering & Management*, 82: 2484-2487.

Siaterlis, C., Genge, B. and Hohenadel, M. (2013). EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. *IEEE Transactions on Emerging Topics in Computing*, 1(2): 319-330.

Silverio-Fernández, M., Renukappa, S. and Suresh, S. (2018). What is a smart device? A conceptualisation within the paradigm of the Internet of Things. *Vizualization in Engineering*, 6(1): 3.

Sinopoli, J.M. (2009). *Smart Buildings Systems for Architects, Owners and Builders*. Butterworth-Heinemann.

SmartGrids, E.T.P. (2012). SmartGrids SRA 2035 Strategic Research Agenda Update of the SmartGrids SRA 2007 for the needs by the year 2035. *Smart Grids European Technology Platform*: 74.

Sookhak, M. (2015). *Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing*. University of Malaya.

Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D. and Fu, K. (2020). Light commands: Laser-based audio injection attacks on voice-controllable systems. *In*: 29th {USENIX} Security Symposium ({USENIX} Security 20), 2631-2648.

Tang, S., Shelden, D., Eastman, C., Pishdad-Bozorgi, P. and Gao, X. (2019). A review of Building Information Modeling (BIM) and Internet of Things (IoT) devices integration: Present status and future trends. *Automation in Construction*, 101: 127-139.

Tankard, C. (2016). Smart buildings need joined-up security. *Network Security*: 1.

Tong, J., Sun, W. and Wang, L. (2014). A smart home network simulation testbed for cybersecurity experimentation. International Conference on Testbeds and Research Infrastructures. Springer.

Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R. and Watson, T. (2020). Quality standards for digital forensics: Learning from experience in England & Wales. *Forensic Science International: Digital Investigation*, 200905.

Vaccaro, A., Pepiciello, A. and Zobaa, A.F. (2020). Introductory chapter: Open problems and enabling methodologies for smart grids. Research Trends and Challenges in Smart Grids. IntechOpen.

Vitunskaite, M., He, Y., Brandstetter, T. and Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 83: 313-331.

Wallace, G. (2013). *Target Credit Card Hack: What You Need to Know*. https://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/

Wang, P., Ali, A. and Kelly, W. (2015). Data security and threat modeling for smart city infrastructure. 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), IEEE.

Wang, S., Zhang, Y. and Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, 6: 38437-38450.

Wang, X., Habeeb, R., Ou, X., Amaravadi, S., Hatcliff, J., Mizuno, M., Neilsen, M., Rajagopalan, S.R. and Varadarajan, S. (2017). Enhanced security of building automation systems through microkernel-based controller platforms. 2017

IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), IEEE.

Wang, X., Mizuno, M., Neilsen, M., Ou, X., Rajagopalan, S.R., Boldwin, W.G. and Phillips, B. (2015). Secure rtos architecture for building automation. Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy.

Waraga, O.A., Bettayeb, M., Nasir, Q. and Talib, M.A. (2020). Design and implementation of automated IoT security testbed. *Computers & Security*, 88: 101648.

Whittle, B. (2018). *What is a Nonce? A No-Nonsense Dive into Proof of Work*. https://coincentral.com/what-is-a-nonce-proof-of-work/

Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H.-N. and Imran, M. (2020). Blockchain for cloud exchange: A survey. *Computers & Electrical Engineering*, 81: 106526.

Xiong, Z., Zhang, Y., Niyato, D., Wang, P. and Han, Z. (2018). When mobile blockchain meets edge computing. *IEEE Communications Magazine*, 56(8): 33-39.

Yakubov, A., Shbair, W., Wallbom, A. and Sanda, D. (2018). A blockchain-based pki management framework. The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS, 2018, Tapei, Tawain. 23-27 April 2018.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1): 22-32.

Zang, L., Yu, Y., Xue, L., Li, Y., Ding, Y. and Tao, X. (2017). Improved dynamic remote data auditing protocol for smart city security. *Personal and Ubiquitous Computing*, 21(5): 911-921.

Zubizarreta, I., Seravalli, A. and Arrizabalaga, S. (2016). Smart city concept: What it is and what it should be. *Journal of Urban Planning and Development*, 142(1): 04015005.