

## A critical review of digital twin confidentiality in a smart city

Item Type	Conference contribution
Authors	Kismul, Alex;al-Khateeb, Haider;Jahankhani, Hamid
Citation	Kismul, A., Al-Khateeb, H., Jahankhani, H. (2023). A Critical Review of Digital Twin Confidentiality in a Smart City. In: Jahankhani, H. (eds) Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications. Springer, Cham, pp 437–450. <a href="https://doi.org/10.1007/978-3-031-20160-8_25">https://doi.org/10.1007/978-3-031-20160-8_25</a>
DOI	<a href="https://doi.org/10.1007/978-3-031-20160-8_25">10.1007/978-3-031-20160-8_25</a>
Publisher	Springer
Download date	2026-03-10 03:54:10
Link to Item	<a href="http://hdl.handle.net/2436/624983">http://hdl.handle.net/2436/624983</a>

# A critical review of Digital Twin Confidentiality in a Smart City

Alex Kismul<sup>1</sup>, Haider Al-Khateeb<sup>2,\*</sup>, and Hamid Jahankhani<sup>1</sup>

<sup>1</sup> Northumbria University London Campus, UK

<sup>2</sup> School of Engineering, Computing and Mathematical Sciences, University of Wolverhampton, UK

\* Correspondence: [H.Al-Khateeb@wlv.ac.uk](mailto:H.Al-Khateeb@wlv.ac.uk)

**Abstract**— Digital twin technology is used to enable businesses to create efficiencies by modelling their physical counterparts. Use cases include modelling a physical device through its lifecycle to perform predictive maintenance, product training, future product development, product performance enhancement, or using the digital twin to control its physical counterpart to perform tasks on IoT or other connected devices. A digital twin leads to less downtime on a physical device as all the modelling or testing is conducted in a virtual environment meaning the physical device can continue to perform the tasks required of it. The digital twin and its physical counterpart are linked and synchronised through heterogeneous network connections. This poses a cyber security question of whether there is a risk of using a digital twin within a smart city. This paper aims to critically examine the confidentiality requirements for a digital twin in a smart city by performing a critical analysis of current literature.

**Keywords:** Digital Twin, Smart City, Cyber-Physical Systems, Confidentiality, Privacy, Data Protection.

## 1 Introduction

A digital twin (DT) can communicate bidirectionally with a physical entity (e.g., Internet of Things (IoT)) by use of network connectivity between the operational device and the DT (Singh et al., 2021), (Voas et al., 2021). This connectivity extends the data held within the physical entity to the DT and reciprocally the DT can send instructions to the physical entity. This brings a form of network convergence between Information Technology (IT) and Operational Technology (OT) systems.

These factors may introduce contemporary and novel cyber security threats to the DT and its physical counterpart by connecting systems that historically are separate operational and information system networks. This research critically evaluates confidentiality threats to DTs in a smart city as they are likely to contain sensitive data that must be protected. The study will offer a critical review and assess the use of DT technology that processes information from a physical entity in a smart city and how it may pose a significant confidentiality and cybersecurity risk. A thematic narrative literature review is presented which identified numerous contemporary and novel threats by connecting a DT to a physical operational entity.

## 2 Background and related work

The literature review examines the evolution of DTs for contextual awareness. It also examines the uniqueness of smart cities in terms of searching for specific ethical requirements such as privacy, and citizen safety.

### 2.1 Digital Twin Computing Background

Cyber-Physical Systems (CPS) are created through digital transformation strategies which are predominantly associated with Industry 4.0 initiatives (Fuller et al., 2020). Connected physical assets such as the Internet of Things (IoT) devices, and big-data computing processing via heterogeneous network connectivity methods allow for the creation of CPS. CPS enables organisations to enhance business process efficiencies through the analysis of readings from the physical assets data outputs (e.g., sensor and actuator outputs) to greater understand asset performance and to make efficiencies through the asset's lifecycle.

A DT is a virtualised replica of a physical entity. This can be a digital replica of an IoT device, an engine, a human (e.g., transplanted organ), a city, or any physical thing that can be replicated in a digital form (Fuller et al., 2020). A DT can communicate in real time with the physical entity it replicates. Effectively, it can model the physical counterpart by receiving and processing data from the physical entity and send communication signals such as instructions to the physical device. The state of the physical twin can be changed by altering the state of the DT and vice-versa, (Singh et al., 2021).

DTs can be created and used in sectors such as smart cities, healthcare, aviation, automotive, or any sector where there is a benefit in creating a digitised replica of a physical asset. Use cases include product design, device lifecycle planning, and optimisation of process controls. These use cases lead to improved business efficiencies, and cost reductions through strategies such as predictive maintenance (Singh et al., 2021). A DT is not a standalone entity in software. Often DTs will be used in conjunction with Artificial Intelligence (AI), Machine Learning (ML), and Augmented Reality (AR). For example, the DT could pair a person's unique physical artefacts with digital models reflecting their status in real-time for analysis and representation within virtual and augmented reality systems (Ahmadi-Assalemi et al., 2020).

There are niche companies providing DT technology, either as a consumer service (SaaS, PaaS, etc), or through providing bespoke services that are created based on the specific physical entity technology and its required use case. Often these services are provided on cloud-based locations away from the operational physical entity to enable cost savings through economies of scale. DTs can be deployed using open-source software or proprietary vendor provided solutions (Mylonas et al., 2021). Along with other types of CPS, the concept of a DT introduces a form of convergence by connecting an operational physical asset to a digital replica over a shared network connection (Holmes et al., 2021). This literature review will concentrate on DTs within smart cities.

## *2.2 Smart City Background and Digital Twin Relevance*

A connected place or smart city is defined by UK National Cyber Security Centre (NCSC) as “a community that integrates information and communication technologies and IoT devices to collect and analyse data to deliver new services to the built environment and enhance the quality of living for citizens” (NCSC., 2021)(a). Smart city services include CCTV, traffic light management, waste management, street lighting management, transport services and other public services such as healthcare and emergency services (NCSC., 2021)(a).

Basic building blocks for a smart city are instruments (e.g., sensors, cameras, consumer devices, and other specific city digital devices), connectivity, and intelligent services used for analysis and decision making (Ibm.com., 2009). Smart city infrastructure is built by using technologies such as IoT, big data analytics computing, and network connectivity over existing (wired / wireless) and emerging deployment of network technologies (such as 5G / WIFI 6). IoT Sensors collect the data and stream it to computing data processors for a variety of applications such as Real-time reporting in Smart Homes (Singh et al., 2021).

DTs can play a role in smart cities, for example, planning decisions within built environments can benefit from using near real-time 3D modelling. Collecting vast amounts of data can lead to the creation of modelling to enable smart city planners to adaptively change how the smart city operates (Deren et al., 2021).

## *2.3 Digital Twin Integration with Smart Cities*

Deren et al., (2021) assert there are two fundamental aspects to creating a DT city, a data foundation, and a technical foundation. The data foundation is created by the transmission of data from sensors, cameras, and other digital data collection devices. The technical foundation is the IoT, network transmission technologies (wired/ wireless), cloud, fog services, big data processing, and integrated intelligence (e.g., AI) (Deren et al., 2021).

This raises two important considerations – the coexistence of multiple entities (service providers, city technology infrastructure, and consumer devices), and the convergence of data and information between operational networks and DTs likely located on separate networks (e.g., cloud infrastructure).

Elmaghraby, et al., (2014) previously investigated cyber security concerns with smart cities and concluded that the smart city building blocks need to be protected using the Confidentiality, Integrity, and Availability (CIA) triad (and authenticity), adherence to privacy laws, and consideration of the democratic social concept of the right to privacy (Ahmadi-Assalemi et al., 2020). The social right to privacy is a complex subject and is taken to account

within this document as a concept based on citizen trust and confidence, rather than examining various specific legal statutes (Benedik and Al-Khateeb, 2021)

Traditional industrial network hierarchical models such as IEC 62443 (Iec.ch., (2021), Sans.org., (n.d)) used in industrial zones is less relevant for connected places. The network is no longer hierarchical in the traditional sense of layers of rigid zones from the sensor to the application server. Emerging digital technologies such as multi-access edge computing (MEC), fog computing, and cloud computing will become the standardised technology stacks within smart cities. High speed, low latency connectivity will be critical for real-time representation as the technology use cases grow.

Cyber security considerations of the DT, physical twin, data flow, and the types of technology used need to be considered holistically when planning DT deployments. By processing potentially sensitive personal data, the risks and threats increase and could become uncontrolled. The risk of connecting DTs to their physical counterparts is if one of them is compromised by an attacker it could compromise the other.

A further complication occurs due to identifying the ownership of specific data and information. If a smart city is compared to a manufacturing business that uses DTs it can be assumed the intellectual property of the data belongs to the manufacturing business owner or stakeholders, in a smart city there are numerous groups of service providers, individual citizens, and civil departments. As smart cities grow, collaboration requirements will also grow and networks will continue to converge (Mylonas et al., 2021). Data and information must be identified and categorised whether it is in the public domain, a closed domain, and is governed under a specific set of regulations (e.g., if defined as critical infrastructure or is an essential service). A further consideration is cloud servers storing and processing data (e.g., GDPR compliance). Cloud servers may not be in the jurisdictional areas required for compliance (Sookhak et al., (2019)). These considerations outline the importance of information governance for a smart city using CPS (Ahmadi-Assalemi et al., 2020).

Much work has been conducted to highlight a general requirement for cyber security and information security guidance or frameworks for using IoT and Smart Cities. Sookhak et al., (2019) and Montasari et al., (2021) discuss the security and privacy of smart city requirements based on IoT security and cloud security. Relevance is paid to security and privacy issues that should be considered when designing smart city frameworks.

Vitunskaitė et al., (2019) highlight the smart city threat landscape in their research. This is based on malicious activity and accidental activity. They discuss the risks to smart cities regarding third-, fourth- and fifth-party access. Of concern is connecting IoT devices which are not built with security in mind or by design. In addition, they discuss the lack of roles and responsibilities documented in standards concerning emerging smart city development and deployment of technology. Other key findings are requirements for maintaining the trustworthiness of data, malware mitigation (i.e., targeting IoT devices and connected application servers), and the impact of a Distributed Denial of Service (DDoS) attack. A key conclusion from their report is security by design is a major factor in ensuring secure and resilient smart cities. This is especially applicable when connecting DTs to smart city network infrastructure.

Vitunskaitė et al., (2019) report that threats to smart cities can be intentional or accidental. Of specific interest to the protection of confidentiality are eavesdropping and unauthorised access threats. However other threats can relate to the loss of confidentiality (e.g., malware resulting in data theft).

There is a common theme in literature for smart cities in terms of IoT protection, cloud computing protection, and secure network connectivity using encryption techniques. Limited information is currently available specifically aimed at DTs within smart cities. There are relevant similarities in terms of CPS and should be taken into consideration.

#### *2.4 Relatable Standards and Guidance for Smart City Digital Twins*

The European Union Agency for Cybersecurity (ENISA) provides guidance for “The Good Practices for Security of IoT” (European Union Agency for Cybersecurity, (2019)) which focuses on the secure development Lifecycle of IoT and “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures” (European Union Agency for Cybersecurity, (2017)) which focusses on IoT in mission-critical environments. This provides strong technical and procedural guidance to understand the IoT threat landscape, attack types, and mitigation techniques.

ENISA has produced a tool for smart environments (IoT, Smart Cities, Industry 4.0, Smart Cars, Smart Hospitals and more) that can be downloaded and used as guidance (Enisa.europa.eu., (n.d.)), this is broadly similar to control frameworks such as ISO2700 series controls, NIST CSF, and other good practices.

The UK NCSC has put together a set of principles for connected places (smart cities), that is based upon three guiding principles:

- Understanding the connected place
- Designing the connected place
- Managing the connected place

These principles are broadly based on regulatory requirements such as the Network and Information Systems (NIS) and General Data Protection Regulation (GDPR) in collaboration with the UK Centre for Protection of National Infrastructure (CPNI) (with relevance to critical infrastructures). CPNI has also provided guidance under a specification entitled PAS185:2017 for the development and operation of connected places (NCSC., (2021)(b), Cpni.gov.uk., (2021), Cpni.gov.uk., (2022)).

The US Government has legislated “The Internet of Things Cybersecurity Improvement Act”. This regulatory requirement overseen by the US NIST institute mandates US federal agencies are required to comply with the guidance published by NIST (Congress.Gov., (2020), NIST., (2020)(a)). This guidance is specifically intended to work with existing NIST frameworks (NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations) to tighten up cyber security for IoT. It also enables a baseline set of standards for manufacturers to comply with when developing and building IoT devices. It has some limitations as the regulatory framework only mandates US federal organisations to comply, others may do so on a voluntary basis. Additionally, its primary focus is securing IoT, rather than considering DT technology.

Applicable standards such as NIST 800-53 (NIST., 2020)(b), and ISO 27001 (Bsigroup.com., (n.d.)) have relevance. Applicable sections of ISO 27001 include segregation of duties, access controls, user training and awareness, asset management, information classification, user access management (including privileged account management), user responsibilities, cryptographic controls, malware and vulnerability prevention, security in development, supplier relationships and legal and contractual requirements (including accessing and handling PII and IP). Whilst these controls are generic, they provide guidance to ensure access controls are robust and are used to protect business information (including PII). This requires an up-to-date inventory of assets and a solid understanding of the business information held within them.

### *2.5 Legal Requirements to Protect Private Data*

Data protection is a regulatory requirement in most modern economies. The data protection act (DPA) in the European Economic Area (EEA) is GDPR (the UK has also adopted this DPA after leaving the bloc). This law applies anywhere to anyone who targets or collects personal data of a citizen in the European Union (EU) (European Commission, Directorate-General for Justice and Consumers., (2018)).

GDPR Article 25 states data protection must be by design and by default (European Commission, Directorate-General for Justice and Consumers., (2018)). Data protection by design is a requirement for organisations to design privacy handling requirements into new systems that process personal data. This includes technical and organisational requirements. This principle is designed to reduce privacy risks and promote trust.

Data protection by default mandates an organisation to protect privacy technically by choosing the most protective settings. (European Commission, Directorate-General for Justice and Consumers., (2018)). Furthermore, only personal data that achieves the specific business purpose should be processed (Ico.org.uk., (n.d.)).

## **3 Organisations Concerned with the Development of Smart Cities**

The G20 of developed nations Smart Cities Alliance was formed in 2019 (Globalsmartcitiesalliance.org. (2020)) to bring together industrialised countries to work in a public-private sector partnership to enhance smart city standards through collaboration. This partnership is currently developing its standards. Currently released is a policy for cyber resilience based on the NIST Cybersecurity Framework (CSF) (Barrett (2018)), the NCSC Cyber Assessment Framework (CAF) (NCSC., 2019) aimed at critical infrastructures, or requirements for UK/ EU NIS compliance, or organisations associated with public safety. Other currently released policies include a Privacy

Impact Assessment (PIA) which takes into account legal and ethical considerations for data and information privacy and a Cyber Accountability Model.

At the time of writing this document, numerous policies on the roadmap are not yet released. It is still currently incumbent on the technology owners and local policymakers to ensure specific technical controls comply with the standards and frameworks within their region.

Whilst all these policies align with security good practice guidelines and standards, they are generic and high-level. From the examination of the standards and frameworks from the UK, EU, US and G20, there is a lack of maturity concerning specific technical cyber security controls that are relevant to DTs that connect and control their physical counterpart. The policies released are generally based on contemporary controls and do not take account of the novel threats and risks posed by introducing DTs into smart cities. This is where the current gap in knowledge exists.

#### 4 Current Considerations for Digital Twin Cyber Security

A key cyber security consideration for a DT is the synchronous bi-directional communication with its physical counterpart (Holmes, et al (2021)). The protection of information held within a DT, and resultant data flow between the CPS systems is paramount. Maliciously attacking a DT could result in loss of information such as intellectual property, privacy loss such as Personally Identifiable Information (PII), degrading the quality of service, or in extreme cases the safety of employees or citizens. Holmes et al., (2021) advocate the CIA triad as a method to secure DTs.

The Industrial Internet Consortium (IIC) outlined the requirement to protect the DT itself, (i.e., protect the intellectual property within), and to protect the physical asset(s) it connects to. When considering security controls, it must be done holistically and with consideration of the strength of the security of the IoT device, the network and any other connected device or system. Consideration needs to account that a compromise of the physical asset could lead to compromise of the DT, and conversely, compromise of the DT could lead to compromise of the physical asset. The article states there must be a security culture within an organisation that is led from the top. A secure by-design methodology is needed that is incorporated into a Software-Defined Lifecycle (SDLC). Software hardening should occur, and encryption to protect data at rest and in transit (Hearn et al., 2019).

A publication by the consulting firm Royal HaskoningDHV (Lomax Thorpe., (n.d.)) highlights four contemporary cyber security risks to DTs that directly impact the confidentiality and integrity of a DT. This is summarised in Table 1.

*Table 1. Digital Twin Risks.*

<b>Risk</b>	<b>Summary</b>	<b>Aspect of CIA Triad</b>
System Access	The unauthorised access or unauthorised elevation of privileges could lead to IP theft, non-compliance, and loss of information integrity	Confidentiality / Integrity
IP Theft	Theft of IP (i.e., theft of business information, PII) enabling an attacker to sell on IP, or use to reproduce the DT for further malicious activity	Confidentiality
Non-Compliance	Compromise of the DT could lead to loss of privacy compliance requirements such as DPA's (e.g., GDPR). Resulting in fines or reputational loss.	Confidentiality / Integrity
Information Integrity	If information integrity is compromised, the DT could compromise the physical counterpart (e.g., degrade service, produce unexpected results, endanger safety, compromise privacy)	Integrity

Lomax Thorpe., (n.d.) asserts the risks covered in Table 1 should be understood by the business and governed by an enforceable policy.

Nonetheless, the US federal standards organisation NIST recently produced a draft guidance of cyber security considerations concerning DTs (Voas et al., 2021). This literature states there is a requirement to address novel threat considerations that DTs introduce when connecting CPS. Confidence in DTs is of paramount importance, especially to ensure information and data privacy is maintained. Fundamentally, connecting DTs introduces novel

threats which may not be fully addressed by existing contemporary controls. Table 2 illustrates the threat considerations posed in the NIST document.

Table 2. Novel Cybersecurity Challenges (Source – Voas, J., et al (2021)). Novel Threat – “NIST Draft NISTIR 8356 Considerations for Digital Twin Technology and Emerging Standards”

Statement	Summary Consideration from Document
“Massive instrumentation of objects (usually IoT technology)”	<p>Vulnerabilities in IoT devices</p> <p>Low-level computing capability of IoT technology combined with limited upgradeability or patching of vulnerabilities</p> <p>Trusted sourcing and deployment of IoT devices</p> <p>Remote control of IoT devices at a mass scale and within different environments (e.g., botnet attack)</p> <p>IoT device secure communication (e.g., PKI, symmetric/ asymmetric encryption of link)</p>
“Centralization of Object Measurements”	<p>Containment of potentially sensitive information within a central location</p> <p>Unauthorised system access compromise could lead to loss of IP from all data collated from sensors sent to the DT (e.g., information theft, ransomware)</p> <p>A large volume of technology (IoT and DTs to protect) where a vulnerability in one could lead to compromise of the other</p> <p>Taking control of DT leads to control of physical devices</p> <p>Interconnected system vulnerabilities</p>
“Visualization/Representation of Object Operation”	<p>Manipulation of how information is presented through malicious access to the DT</p> <p>Loss of data integrity leading to system integrity loss (including connected systems)</p>
“Remote Control of Objects”	<p>Compromise of the physical objects a DT remotely controls</p> <p>Presentation of false readings</p> <p>Safety of sensor, human safety</p> <p>Loss of IP/ data theft</p>
“Standards for Digital Twin Definitions”	<p>Removes the proprietary aspects of the technology</p> <p>Enables attackers to build their own DT definitions (also consider phishing techniques)</p> <p>Could become part of an attacker toolkit</p>

The document produced by Voas et al., (2021) refers to numerous NIST standards that exist as potential frameworks that can be used. These suggestions follow IoT-specific controls, standard risk controls, privacy considerations, the NIST CSF, encryption at rest and in transit, strong authentication, physical security controls, and fault tolerance. A Zero Trust approach is also suggested (Voas et al (2021)).

## 5 Risks and Architectural Requirements

Overall, the question around the protection of the DT in a smart city requires further consideration. For example, the inclusion of techniques and controls such as privacy by design, privacy enhancing technologies (PETs) and other techniques discussed earlier above (Holmes et al (2021)), (Lomax Thorpe., (n.d.)), (Voas et al., 2021). As a smart city grows so will the convergence and coexistence of different technology and data. Fundamentally the specific types of technology, usage of the technology and the sensitivity of the information should drive the specific controls (i.e., through a risk-based methodology). Continuous development of controls to counter contemporary and novel threats will enable a future framework of controls that will be state-of-the-art.

The protection of data and information must be included when designing and deploying DTs to ensure it is not subject to theft, accidental loss, or misuse. This is especially important when privacy is a requirement. Technology, processes and authorised people need to be identified to ensure correct cyber security governance is in place. This is an especially difficult undertaking. For example, a smart CCTV system will capture multiple thousands of

people in a city per day. One of the most important undertakings is ethically protecting the right to privacy, whilst still fulfilling the purpose of the system.

Examining the confidentiality perspective (of the CIA triad) and making consideration for the privacy requirement of citizens' data is closely linked to data protection regulations (Benedik and Al-Khateeb, 2021). Information anonymisation or encryption may be a regulatory requirement to protect privacy where a sensor has retrieved Personally Identifiable Information (PII) which is processed in a DT or connected system. Business intellectual property information is also highly likely to be contained within a DT and its physical counterpart and requires protection. To promote confidence and trust in the use of DT technology, data and information must be used ethically. The benefits of using DTs should be clearly defined to ensure it is not perceived as an information gathering service of citizen data (e.g., for unethical surveillance purposes (Mehta, 2022)).

Some work has commenced on the creation of a framework required to protect DTs and their physical counterparts in the industry. Gehrman et al., (2020) has produced a set of requirements (Table 3) that address aspects of system security, performance, and accuracy of the data exchange between DTs and dependant devices for industrial automation and control system security. The table below summarises the findings.

*Table 3. Architectural Requirements for Industrial Digital Twins (Source - Gehrman, C. et al., (2020))*

<b>Requirement</b>	<b>Summary Consideration</b>
“Synchronization security”	The starting state and idle state between the DT and its counterpart are always in alignment  The DT provides confidentiality protection  The DT provides synchronisation protection
“Synchronization latency”	Message exchanges between the DT and physical twin must not affect time-critical control functions
“Digital twin external connections protection”	Authentication of connections between the DT and any external entities must occur to protect confidentiality and integrity
“Access control”	Access controls are applied to the DT and any entity that requests access to the DT. Includes third parties and information exchanged with other DTs
“Software security”	The physical twin software should be trustworthy and must be resilient to zero-day attacks (e.g., a backup available)
“Local factory network isolation”	Network controls are required to be in place to ensure only valid synchronisation traffic is permitted and can mitigate against DoS attacks on the physical twin
“Digital twin Denial-of-Service (DoS) resilience”	The DT should be protected from DoS attacks, whilst ensuring this doesn't restrict synchronisation between the DT and the physical counterpart (see “Synchronization latency”)

From a smart city perspective, these requirements in the table above are valid and comparable. A smart city has a strong mandate to protect citizen safety and keep mission-critical services running for many people. Numerous high-profile attacks have recently occurred against city services (and utility providers providing critical services). Furthermore, the protection from supply chain attacks must also be mitigated to ensure the propagation of malware (Irshad et al., 2018) is limited throughout the smart city digital infrastructure. A recent global supply chain attack in 2020 illustrated the threat by using techniques including infiltration, lateral movement across systems, and implemented malware to eventually steal information (Mandiant.com., (2020)).

## 6 Conclusion

Any digital replica of a physical entity that can communicate and control its physical counterpart could be prone to the contemporary and novel threats discussed earlier, either accidentally or maliciously. This could result in defects, IP theft, or even threaten human life. Therefore, the protection of the DT is at least of equal importance to protecting the connected operational physical assets.

Key considerations for DTs within smart cities are citizen safety and privacy are of paramount importance, and the protection of intellectual property is also of key importance. What is required is a specific framework to protect

the DT that takes account of novel threats and that understands the risk landscape for a DT within a smart city (and other related sectors). Consideration should be made to the protection of data and information. Where feasible technical controls should be state-of-the-art to build on existing contemporary controls.

All the considerations here are valid and critical; however, they are generally based on generic contemporary controls, rather than specifically targeting the protection of a DT with the novel risks and threats it may encounter (including the environment it is used in). The considerations above are predominantly related to IoT and CPS. This highlights there is a gap in the literature concerning the protection of confidentiality of data and information for a DT in a smart city.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

- A. Elmaghraby, and M. Losavio, 2014. "Cyber security challenges in Smart Cities: Safety, security and privacy". Journal of Advanced Research, [online] 5(4), pp.491-497. DOI:10.1016/j.jare.2014.02.006.
- A. Fuller, Z. Fan, C. Day and C. Barlow, 2020 "Digital Twin: Enabling Technologies, Challenges and Open Research," in IEEE Access, vol. 8, pp. 108952-108971, 2020. DOI: 10.1109/ACCESS.2020.2998358.
- D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal and H. Janicke, "Digital Twins and Cyber Security – solution or challenge?," 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2021, pp. 1-8. DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277.
- G. Ahmadi-Assalemi, H. M. Al-Khateeb, G. Epiphaniou and C. Maple, "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review", Smart Cities, 2020, 3, 894-927. DOI: 10.3390/smartcities3030046.
- G. Ahmadi-Assalemi, H. M. al-Khateeb, C. Maple, G. Epiphaniou, Z. A. Alhaboby, S. Alkaabi, and D. Alhaboby, "Digital Twins for Precision Healthcare", in Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Sciences and Technologies for Security Applications, H. Jahankhani et al., Ed. Cham: Springer International Publishing, 2020, pp. 133-158, ISBN: 978-3-030-35746-7. DOI: 10.1007/978-3-030-35746-7\_8.
- G. Mylonas, A. Kalogeras, G. Kalogeras, C. Anagnostopoulos, C. Alexakos and L. Muñoz, "Digital Twins From Smart Manufacturing to Smart Cities: A Survey," in IEEE Access, vol. 9, pp. 143222-143249, 2021. DOI: 10.1109/ACCESS.2021.3120843.
- J. Voas, P. Mell, V. Piroumian, 2021. (Draft) Considerations for Digital Twins Standards. NIST Database, [online] (Draft). Available at: <<https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8356-draft.pdf>>.
- L. Deren, Y. Wenbo, S. Zhenfeng, 2021, Smart city based on digital twins. Comput.Urban Sci. 1, 4 (2021). DOI: 10.1007/s43762-021-00005-y
- M. Irshad, H. M. Al-Khateeb, A. Mansour, A. Ashawa, and M. Hamisu, "Effective methods to detect metamorphic malware: A systematic review", International Journal of Electronic Security and Digital Forensics, vol. 10, no. 2, pp. 138–154, 2018, ISSN: 1751-9128. DOI: 10.1504/IJESDF.2018.090948.
- M. Singh, E. Fuenmayor, E. Hinchy, Y. Qiao, N. Murray, and D. Devine, "Digital Twin: Origin to Future," Applied System Innovation, vol. 4, no. 2, p. 36, May 2021. DOI: 10.3390/asi4020036.
- M. Sookhak, H. Tang, Y. He and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Secondquarter 2019. DOI: 10.1109/COMST.2018.2867288.
- M. Vitunskaitė, Y. He, T. Brandstetter, & H. Janicke, (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. DOI: 10.1016/J.COSE.2019.02.009.
- R. Singh, H. M. Al-Khateeb, G. Ahmadi-Assalemi, and G. Epiphaniou "Towards an IoT Community-Cluster Model for Burglar Intrusion Detection and Real-Time Reporting in Smart Homes", in Challenges in the IoT and Smart Environments, A Practitioners' Guide to Security. Advanced Sciences and Technologies for Security Applications, R. Montasari et al., Ed. Cham: Springer International Publishing, 2021, pp. 53-73, Print ISBN: 978-3-030-87165-9, Electronic ISBN: 978-3-030-87166-6. DOI: doi.org/10.1007/978-3-030-87166-6\_3.

R. Benedik, and H. M. Al-Khateeb, “Digital Citizens in a Smart City: The Impact and Security Challenges of IoT on citizen’s Data Privacy”, in Challenges in the IoT and Smart Environments, A Practitioners' Guide to Security. Advanced Sciences and Technologies for Security Applications, R. Montasari et al., Ed. Cham: Springer International Publishing, 2021, pp. 93-122, Print ISBN: 978-3-030-87165-9, Electronic ISBN: 978-3-030-87166-6. DOI: 10.1007/978-3-030-87166-6\_5.

R. Montasari, H. Jahankhani, H. M. Al-Khateeb, Challenges in the IoT and Smart Environments - A Practitioners' Guide to Security, Ethics and Criminal Threats. Advanced Sciences and Technologies for Security Applications, Ed. Springer International Publishing, 2021. Print ISBN: 978-3-030-87165-9. Electronic ISBN: 978-3-030-87166-6. DOI: 10.1007/978-3-030-87166-6.

NCSC, 2021., (a)., Connected Places Cyber Security principles. [online] NCSC. Available at: <<https://www.ncsc.gov.uk/collection/connected-places-security-principles>>.

Ibm.com., 2009. A vision of smarter cities. [online] Available at: <<https://www.ibm.com/downloads/cas/2JYLM4ZA>>.

Iec.ch. 2021., Understanding IEC 62443. [online] Available at: <<https://www.iec.ch/blog/understanding-iec-62443>>.

Sans.org. n.d., Introduction to ICS Security Part 2 | SANS Institute. [online] Available at: <<https://www.sans.org/blog/introduction-to-ics-security-part-2/>>.

European Union Agency for Cybersecurity, (2019) “Good practices for security of IoT : secure software development lifecycle”. European Network and Information Security Agency. ISBN 978-92-9204-316-2, DOI: 10.2824/742784

European Union Agency for Cybersecurity, (2017) “Baseline security recommendations for IoT in the context of critical information infrastructures”. European Network and Information Security Agency. ISBN: 978-92-9204-236-3, DOI: 10.2824/03228

Enisa.europa.eu., n.d. “ENISA Good practices for IoT and Smart Infrastructures Tool”. [online] Available at: <<https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Smart%20Cities>>.

NCSC. 2021., (b)., Connected Places Cyber Security Principles. [online] Available at: <<https://www.ncsc.gov.uk/files/NCSC-Connected-Places-security-principles-May-2021.pdf>>.

Cpni.gov.uk., 2021. Security-Minded approach to Open and Shared Data. [online] Available at: <<https://www.cpni.gov.uk/security-minded-approach-open-and-shared-data>>.

Cpni.gov.uk., 2022. Security-Minded approach to developing Smart Cities. [online] Available at: <<https://www.cpni.gov.uk/security-minded-approach-developing-smart-cities>>.

Congress.Gov., 2020. H.R.1668 - IoT Cybersecurity Improvement Act of 2020. [online] Available at: <<https://www.congress.gov/bill/116th-congress/house-bill/1668>>.

NIST., 2020., (a) NIST Releases Draft Guidance on Internet of Things Device Cybersecurity. [online] Available at: <<https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity>>.

NIST, 2020., (b)., Security and Privacy Controls for Information Systems and Organizations. [online] Available at: <<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>>.

Bsigroup.com., n.d. ISO 27001 - Information Security Management (ISMS). [online] Available at: <<https://www.bsigroup.com/en-GB/iso-27001-information-security/>>.

European Commission, Directorate-General for Justice and Consumers., (2018) The GDPR : new opportunities, new obligations : what every business needs to know about the EU’s General Data Protection Regulation. Publications Office. Print ISBN 978-92-79-79453-7 DOI:10.2838/6725. PDF ISBN 978-92-79-79430-8 DOI:10.2838/97649

Ico.org.uk. n.d., Data protection by design and default. [online] Available at: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>>.

Globalsmartcitiesalliance.org., 2020. About the Alliance – GSCA v2. [online] Available at: <[https://globalsmartcitiesalliance.org/?page\\_id=107](https://globalsmartcitiesalliance.org/?page_id=107)>.

Barrett, M. (2018)., Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, [online] Available at: <<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>>.

NCSC., 2019. NCSC CAF guidance. NCSC.  
Available at: <<https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance>>.

Hearn, M. and Rix, S., 2019. Cybersecurity Considerations for Digital Twin Implementations. [online] Iiconsortium.org.  
Available at: <<https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-Cybersecurity-Considerations-for-Digital-Twin-Implementations.pdf>>.

Lomax Thorpe, B., n.d. Risk mitigation in digital twins. [Blog] Available at:  
<<https://global.royalhaskoningdhv.com/digital/resources/blogs/risk-mitigation-in-digital-twins>>.

Mehta, A., 2022. Facial recognition technology 'will turn our streets into police line-ups', campaigners say. [online] Sky News. Available at: <<https://news.sky.com/story/facial-recognition-technology-will-turn-our-streets-into-police-line-ups-campaigners-say-12572433>>.

Gehrmann, C. & Gunnarsson, M., 2020. A digital twin based industrial automation and Control System Security Architecture. IEEE Transactions on Industrial Informatics, 16(1), pp.669–680. DOI: 10.1109/TII.2019.2938885

Mandiant.com., 2020. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | Mandiant. [online] Available at: <<https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor>>.