Understanding Security in Smart City Domains
From the ANT-Centric Perspective

Jiani Fan, Wenzhuo Yang, Ziyao Liu, Jiawen Kang, Dusit Niyato, Fellow, IEEE, Kwok-Yan Lam, Senior Member, IEEE, and Hongyang Du, Graduate Student Member, IEEE

Abstract—A city is a large human settlement that serves the people who live there, and a smart city is a concept of how cities might better serve their residents through new forms of technology. In this article, we focus on four major smart city domains according to Maslow’s hierarchy of needs: smart utility, smart transportation, smart homes, and smart healthcare. Numerous Internet of Things (IoT) applications have been developed to achieve the intelligence that we desire in our smart domains, ranging from personal gadgets, such as health trackers and smart watches to large-scale industrial IoT systems, such as nuclear and energy management systems. However, many of the existing smart city IoT solutions can be made better by considering the suitability of their security strategies. Inappropriate system security designs generally occur in two scenarios: first, system designers recognize the importance of security but are unsure of where, when, or how to implement it and second, system designers try to fit traditional security designs to meet the smart city security context. Thus, the objective of this article is to provide application designers with the missing security link they may need in order to improve their security designs. By evaluating the specific context of each smart city domain and the context-specific security requirements, we aim to provide directions on when, where, and how they should implement security strategies and the possible security challenges they need to consider. In addition, we present a new perspective on security issues in smart cities from a data-centric viewpoint by referring to the reference architecture, the activity-network-things (ANT)-centric architecture. This architecture is built upon the concept of “security in a zero-trust environment,” to achieve end-to-end data security. By doing so, we reduce the security risks posed by new system interactions or unanticipated user behaviors while avoiding the hassle of regularly upgrading security models.

Index Terms—Cryptography, Internet of Things (IoT), IoT security, privacy, smart cities, survey, wireless communication.

I. INTRODUCTION

SMART city is a new paradigm that utilizes various advanced technologies, especially artificial intelligence, to improve urban conditions and make urban life more convenient. At this moment, there is no clear concept of what a smart city should look like, but we can imagine its potential in every possible way. After all, every smart city is the result of the joint choice and vision of all parties involved. According to Maslow’s hierarchy of needs [1], the basic needs of human includes food, water, warmth, rest, safety, and security, which form the basic layout of cities. In any smart city, smart utility systems are required for the efficient provision of power and to enable the operation of other smart systems; smart transportation systems are in charge of distributing resources quickly across cities; smart homes are intended to provide warm, comfortable shelters for city dwellers; and smart healthcare systems are responsible for providing adequate health security. Thus, we focus on four major smart city domains in this article: 1) smart utility; 2) smart transportation; 3) smart homes; and 4) smart healthcare. Nevertheless, all smart city domains will be empowered through the deployment of extensive Internet of Things (IoT) device networks.

IoT refers to the network of interconnected devices that enables cyberspace to interact with the environment and infrastructure [2]. The wireless characteristics of data communication in most IoT applications, as well as its ease of implementation, have accelerated the adoption of IoT systems in recent years. According to Statista [3], the number of IoT devices is expected to reach 30.9 billion by 2025, triple the number of non-IoT devices by then. With the support of IoT technologies and wireless communication protocols, our cities are capable of building extensive data networks that incorporate a large number of heterogeneous devices that participate in the data collection and decision-making process. This massive data backbone formed by IoT devices allows systems to perform real-time environmental monitoring and actuating. With such capabilities, our cities will be able to generate service intelligence and provide a higher standard of living without jeopardizing sustainability.

Numerous IoT applications have been developed to achieve the intelligence required for our smart cities, ranging from personal gadgets, such as health trackers and smart watches to large-scale industrial IoT systems, such as public transportation and energy management systems. However, many of the
existing smart city IoT solutions must be carefully designed by considering the security strategies. Inappropiately system security designs generally occur in two scenarios: first, the system designers recognize the importance of security but are unsure of where, when, or how to implement it. Second, the system designers try to fit traditional security designs to meet the smart city security context without taking specific characteristics of the smart city applications and IoT systems into account. The former necessitates a close examination of the specific security requirements on a context-by-context basis, which will be elaborated further in Section IV. Moreover, the latter requires a thorough understanding of the characteristics of smart city applications and their security challenges.

For example, a common characteristic of smart city applications is being data-driven and rely on constant ubiquitous sensing of the environment. This creates a significant concern regarding compatibility issues with big data due to the high volume, velocity, and variety of data flow [4]. Maintaining data integrity and confidentiality on such a massive scale needs a large amount of computation and storage resources, and failing to do so will have disastrous consequences for the usability of smart systems. Thus, how to best implement adequate data security protection for various types and stages of data is a difficult challenge that smart city applications must address.

Another common characteristic of smart city applications is user-centric. Besides common objectives, such as optimizing resource utilization and system efficiency, improving user experience is a main objective for standard smart city applications. A large amount of sensitive private data is collected to understand user preferences and behavior to provide personalized service and designs [5]. This has raised significant privacy concerns about the use of private data. Any smart city application dealing with such data will require substantial efforts to protect and regulate them.

Furthermore, a common smart city application is expected to deal with devices of varied capabilities and resource constraints and frequent data interchange inside the system and with third parties, imposing high interoperability requirements on the smart city application. This has created a new security context for smart city applications. By a security context, we mean the scope of responsibility that the security mechanism must protect. For example, conventional system security solely protects IT components, such as the software system and servers. However, IoT security in a smart city may also have to safeguard operational components, such as sensors and actuators that are physically installed [6]. Common security challenges include integrity, confidentiality, availability, decentralization, authentication, secure communication, end-to-end security, identity management, access control, privacy, system resilience, scalability, and interoperability [7], [8]. With a changing security context, we will face new security challenges that we may not have anticipated. For example, we have to consider the different wireless communication protocols adopted by IoT devices, where incompatibility between different protocols can lead to serious communication security flaws; and the deployment environment, in which IoT devices may operate in uncontrolled environments, such as public and open spaces, as opposed to the controlled environments in which they have previously operated. Thus, establishing security mechanisms based on a “zero-trust” environment is essential for securing heterogeneous interactions. As a result, conventional system security designs may not be appropriate to be directly applied to smart city applications.

Hence, the objective of this article is to provide application designers with the missing security link they may need in order to improve their security designs. By evaluating the specific context of each smart city domain and the context-specific security requirements, we aim to provide directions on when, where, and how they should implement security strategies and the possible security challenges they need to consider.

In this article, we look at the cybersecurity requirements and challenges for the smart cities from a data-centric perspective by referring to a security reference architecture, i.e., the activity-network-things (ANTS)-centric architecture [9]. The “Activity-centric” view establishes the system context and highlights critical nodes in the system where sensitive data is stored and processed. The “Network-centric” view investigates the connectivity between heterogeneous system components and the sensitive data flow. The “Things-centric” view aids in determining whether the capabilities of end-devices or physical things in terms of communication, computation, and energy are adequate for the execution of adequate cryptographic operations.

There are many benefits of adopting this approach. First, this architecture is built on the notion of “security in a zero-trust environment,” identifying and assessing all attack surfaces under the complex heterogeneous smart city IoT systems, ranging from the data source to its communication agent and extend beyond its own stakeholders. Many traditional security approaches are reliant on the central agent’s or a trusted third party’s ability to act in an appropriate manner, i.e., protect data confidentiality and authenticity. However, there have been numerous instances where the trusted agent has been used for malicious purposes by internal or external parties. On the other hand, when we embrace the ANT-centric view and adapt to the idea of a “zero-trust environment,” there is less reliance on the involvement of trusted agents, lowering the danger of insider attacks and taking into account data protection in the broader system. Furthermore, unlike traditional architecture, ANT-centric architecture is centered on the concept of end-to-end data security, in which we attempt to safeguard sensitive data flows and their interactions rather than bounded system components. This is different from traditional systems where each component is evaluated separately or only in relation to its subordinates. For instance, the vehicle’s conventional cybersecurity depends on the reliability of its digital systems, which include its operating, onboard stereo, Bluetooth multimedia, and visual systems. According to the ANT-centric perspective, we have to evaluate every stage of the data life cycle, including data collection, communication, processing, and storage. By doing this, we can offer complete data protection while avoiding the hassle of having to massively update the security models on a regular basis when new system interactions and functionalities are added, since we have tailored our protection based on the data life cycle by meeting the ANT-centric security requirements listed in Section IV. In addition, with this...
security reference architecture, we can identify critical components of the system that handle sensitive data and understand the data interactions with system components. This provides a means for us to determine the sensitivity of data as well as the criticality of activities evolving around this data. Finally, we chose the ANT architecture also because of its flexibility to suit any IoT system and its comprehensive representation of the IoT systems from the architectural perspectives of device, Internet, and semantic. Thus, security requirements developed using this security reference architecture can be easily applied across smart city applications.

The main contributions of this article are summarized as follows.

1) We present a new perspective on security issues in smart cities from a data-centric viewpoint by referring to the architecture. This aims to provide a different view toward approaching privacy and security issues in a smart city context.

2) We investigate the concept of smart city holistically, beginning with end applications to abstract shared properties, highlight potential privacy and security challenges. By doing so, we hope to broaden readers’ understanding of the background and characteristics of smart cities.

3) We evaluate the specific context of each smart city domain and the context-specific security requirements from the ANT-centric perspective. By doing so, we aim to provide application designers with the missing security link they may need in order to improve their security designs and directions on when, where, and how they should implement security strategies and the possible security challenges they need to consider.

4) From the ANT-centric standpoint, we present the set of challenges that current security solutions for smart city applications will encounter in meeting security requirements and provide a new research perspective toward the evaluation of security frameworks and design. These could also serve as future research directions where research can be aimed at fulfilling these challenges in existing frameworks or giving insights into future research.

5) We discuss the potential prospects for IoT and IoT security in smart cities, such as cognitive IoT and the adoption of machine learning and artificial intelligence.

The structure of this article is in accordance with the following. In Section II, we explain the ANT reference architecture and how to view security issues in smart cities from a data-centric perspective by referring to the architecture. In Section III, we study the concept of a smart city holistically and highlight some of the privacy and security challenges that smart city applications will face. In Section IV, we evaluate the specific context of each smart city domain and their security requirements from an ANT-centric perspective, presenting existing security proposals, and some of their shortcomings. In Section V, we investigate the challenges and gaps that current security solutions have to overcome to meet the set of security requirements from an ANT-centric perspective. In Section VI, we discuss the potential prospects for IoT and IoT security in smart cities, such as cognitive IoT and the adoption of machine learning and artificial intelligence. In Section VII, we conclude our work in this article. The organization of this article is also presented via Fig. 1.

II. ANT-CENTRIC: NEW WAY TO LOOK AT SMART CITIES AND ITS CYBERSECURITY CHALLENGES

In this section, we aim to give a new perspective on smart cities and their cybersecurity challenges to facilitate a deeper understanding of the security requirements needed for designing future smart city solutions. Most of the existing security survey papers for IoT-enabled smart cities consider the security and privacy challenges based on the device layer, network layer, and software layer to application layer [16]. A comparison of our work against some of the related work is provided in Table I. In this survey, we look at the cybersecurity requirements and challenges for the smart cities from a data-centric
table I

| Year | Reference | Contribution |
|------|-----------|--------------|
| 2019 | [10]      | Presented IoT attack vectors and summarize research according to the security technique used. |
| 2021, 2019, 2020, 2022 | [7], [11], [12], [13] | Surveyed IoT security threats, attacks, and vulnerabilities and risk mitigation methods. |
| 2019 | [14]      | Presented "IoT features" for representing IoT security challenges, relating each feature into IoT threat, challenge, and opportunity. |
| 2019 | [15]      | Surveyed IoT security from a data perspective, considering data life cycle. |
| 2018 | [16]      | Surveyed IoT security in smart city from the viewpoint of related disciplines such as cryptography, blockchain, biometrics, and machine learning. |
| 2019 | [17]      | Presented different types of attacks and techniques, broadly classification of security challenges into IoT based and cloud-based under smart city landscape. |
| 2021 | [18]      | Provided holistic overview and conceptual development of smart city. |
| - | This work | We present a new approach to smart city security based on the ANT-centric security reference architecture, evaluate the specific context of each smart city domain and the context-specific security requirements, and provide context-specific guidance on when, where, and how system designs can implement security strategies. Furthermore, we examine the challenges that current security proposals face in meeting these requirements, as well as our vision for future IoT and IoT security. |

perspective by referring to a security reference architecture, the ANT-centric architecture [9]. This architecture is built on the notion of “security in a zero-trust environment,” identifying and assessing all attack surfaces. Therefore, by referencing to this security reference architecture, security requirements in smart cities can be examined and designed more thoroughly. We choose the ANT architecture also because of its flexibility to suit any IoT system. Furthermore, approaching the security requirements and problems for smart cities from a data-centric standpoint makes it more natural and easier to ensure the privacy of sensitive data throughout its life cycle. From here, we will explain the ANT reference architecture and how to view security issues in smart cities from a data-centric perspective by referring to the architecture.

A. Activity-Centric View

An important concept in the ANT architecture is “critical activities,” which affects the customization of security control countermeasures in the IoT system. Critical activities include but are not limited to sensing and actuating (SA), Preprocessing (PP), Processing (DA), crypto endpoint (CE), network transport (NT), Storage (ST), command and control (CC), and Interfacing with external systems (IO) [9]. More critical activities can be customized based on the features of different IoT systems. The activity-centric view is a new way to look at the generation, collection, transmission, processing, and aggregation of sensitive data in smart cities. The security requirements can be considered during the whole life cycle of the data flow. End-to-end secure data flow and storage are required to ensure data quality and availability in the IoT-enabled smart cities.

B. Network-Centric View

There are many types of networks and protocols in different smart city applications, which makes the network-centric view also important to think about when planning the security requirements. The communication architecture in smart cities can be categorized as public, private, or protected to facilitate risk assessment. The network-centric view makes it easier to identify and assess security policies in the network for critical nodes that are related to critical activities. In the smart environment, there is frequent sensing and wireless communication among different components of various smart city applications, even in the open public space. Therefore, end-to-end secure communication on the network through identity authentication, identity management, and the construction of a secure communication environment is necessary to guarantee the security and privacy of sensitive data.

C. Things-Centric View

IoT-enabled smart cities are fabrics of various devices, systems, and other physical things. The things-centric view in ANT architecture inspire us to consider security problems closely related to the devices itself. New methods for secure software updates to accommodate the features of future smart cities are needed. In addition, security physical things in the IoT systems should have the capability to take proactive detection for intrusion in the early stage of the cyber attacks and should also own the ability to heal quickly after being attacked. Therefore, robust and resilient physical things are essential for smart city applications to secure the generation, collection, transmission, processing, and aggregation processes of sensitive data. In the following sections, we will present an overview of the smart city paradigm and a summary of the shared characteristics among smart city applications and highlight some of the common security and privacy challenges.

III. OVERVIEW OF SMART CITY APPLICATIONS

In this section, we first present an overview of the smart city paradigm and then introduce the major domains of smart cities. In addition, we will present a summary of the shared characteristics among smart city applications and highlight some of the common security and privacy challenges.

To begin, to provide a comprehensive presentation of the smart city landscape, we show an illustration of the major smart city domains in Fig. 2.1 In this scenario, central authority, public community, and service providers are the major players involved in controlling and maintaining the city. Variety of smart devices and applications consists of the key elements of these major players. Smart devices and applications create a bidirectional data network in which any participant can ingest or contribute data. These data exchanges can be done by various wireless communication protocols, and the cloud is likely to be used to handle such massive data traffic. City management becomes smart when it integrates info-comm technologies in every sector of the city management into a bigger system that governs the livelihood of people in the city. For example, a smart home is an intelligent infrastructure where smart environment and living

1This diagram contains illustrations from https://storyset.com.
could be well integrated [19]. Intelligent energy and facility management that is tightly integrated to respond to feedback from the environment constitutes smart utility, which enables intelligent operation of the smart environment. Similar to smart infrastructure, smart transportation, healthcare facilities, traffic infrastructure, and more are all part of interconnected systems that comprise smart healthcare and transportation. In this broad view of the smart city landscape, where every component of the city is interconnected, we take into account the most essential smart city domains that concentrate on improving people’s quality of life: smart healthcare, smart utility, smart transportation, and smart homes. In Table II, we provide a summary table of examples of smart city applications in these sectors as well as the key security or privacy issues they investigate.

### A. Common Characteristics of Applications in Smart City

In the preceding paragraphs, we have introduced the smart city landscape. Here, we summarize what a standard smart city application would look like and its characteristics.

| Major Issues Studied | Confidentiality | Integrity | Availability | Privacy | Interoperability | Efficiency | System Monitoring |
|----------------------|-----------------|-----------|--------------|---------|------------------|------------|-------------------|
| Smart Healthcare     |                 |           |              |         |                  |            |                   |
| TMIS                 | [20]–[27]       | [20]–[27]| [20]         | [20]–[21]| [24]–[27]       | [29]–[30] | (30)              |
| WMSN                 | [28]–[29]       | [28]–[30]| [28]         | [28]    | [29]–[30]        |            |                   |
| Blockchain Healthcare Systems | [32]–[33] | [32]–[33]| [33]         | [33]    | [29]–[30]        |            |                   |
| Smart Utility        |                 |           |              |         |                  |            |                   |
| Smart Gas Management System | -     | -         | -            | -       | [33]–[35]        | [35]–[38] |                   |
| Smart Water Systems  |                 |           |              |         | [39]–[40]        | [40]–[42] |                   |
| Smart Grid           | [43]–[47]       | [43]–[47]| [43]         | [49]    | [44]–[48]        |            |                   |
| Blockchain Metering | [50]–[51]       | [50]–[51]| [50]         | [50]–[51]| [51]–[51]       |            |                   |
| Smart Transport      |                 |           |              |         |                  |            |                   |
| UAV                  | [52]–[52]       | [52]–[54]| [52]–[54]    | [53]–[54]| [54]            |            |                   |
| Smart Charging for EVs | [55]–[57]   | [55]–[57]| [55]–[57]    | [56]    | [55]–[56]        |            |                   |
| IoT Distributed Trust | [58]–[58]    | [58]–[58]| [58]–[58]    | [59]    | [58]            |            |                   |
| Traffic Management Systems | -       | -         | -            | [60]–[61]| [62]–[63]        |            |                   |
| Smart Homes          |                 |           |              |         |                  |            |                   |
| Integration With Smart Grid | -       | -         | -            | [43]–[65]| [43]–[65]        | -          |                   |
| Access Control In Smart Home | [67]–[5] | [67]–[5]  | [5]          | -       | [5]             | -          | -                 |
| Blockchain Home Systems | [68]–[69] | [68]–[69]| [69]–[69]    | [69]    | [68]–[69]       | -          | -                 |
### TABLE III
**SUMMARY OF THE SECURITY FEATURES AND CHALLENGES OF WIRELESS COMMUNICATION PROTOCOLS FOR SMART CITY IoT APPL**

| Protocol | Security Features | Security Challenges |
|----------|-------------------|---------------------|
| Zigbee   | Zigbee Trust Center is responsible for key management and distribution in the network, and it provides cryptographic key establishment and frame protection. (AES 128-bit) | Zigbee is susceptible to jamming, traffic analysis attacks. Since different application layers on the same device trust each other, a compromise on one of the layers can escalate to the other layers. In addition, network keys can be extracted from the hardware, resulting in concerns for the physical capturing attack [71]. |
| Z-wave   | Z-wave network contains master and slave nodes. It provides authentication service, packet encryption, and integrity protection. (AES 128-bit, Message Authentication Code in Cipher Block Chaining mode) | Z-wave is susceptible to traffic analysis, spoofing, MITM attacks. Z-wave devices trust all MAC Protocol Data Unit, making them vulnerable to impersonation attacks [71]. |
| Bluetooth Low Energy (BLE) | BLE provides encryption, authentication, message integrity checks, and 12-byte signature to prevent relay attacks in mode 2. In addition, BLE changes the address of devices frequently to reduce the ability for attackers to track. | BLE uses elliptic curve cryptography, which is not supported in legacy mode pairing. Thus, devices in legacy mode pairing are susceptible to MITM and eavesdropping attacks [71]. |
| IEEE 802.15.4 | The security of IEEE 802.15.4 is implemented at the MAC layer. Security features such as encryption and authentication, access control, confidentiality protection are provided. (AES) | IEEE 802.15.4 is susceptible to active tampering, jamming, eavesdropping attacks. Many attacks aim at different layers of the protocol [72]. |
| 6LoWPAN | 6LoWPAN can operate over other platforms such as Ethernet, Wi-Fi, IEEE 802.15.4, and it has no security features. | 6LoWPAN does not provide any security feature and relies on other protocols or applications to complement its security requirement [72]. |
| Routing RPL | RPL provides message confidentiality and integrity. (AES, CCM, consistency check using challenge-response) | RPL is susceptible to internal attacks [72]. |
| CoAP    | CoAP requires other protocols to provide it with security features. E.g. CoAP can rely on Datagram Transport Layer Security (DTLS) for encryption. | Although DTLS is often implemented to provide security features for CoAP, DTLS is not fully compatible with CoAP (i.e., it does not suit CoAP proxy modes) [72]. |

**User-Centric:** Besides the common objectives, such as optimizing resource utilization and increase system efficiency in conventional systems, improving user experience will be a main objective for standard smart city applications. There will be more focus on providing personalized service and designs that suit the preferences of the users.

**Ubiquitous:** Smart city applications collect a vast volume of user data for insight extraction using ubiquitous sensors and devices located around the city. The data collected from these sensors may be shared between platforms and applications, and can be utilized to perform various data analysis before being transformed into actionable insights at the end devices.

**Data-Centered:** To enhance their operations, most smart city applications will leverage the big data landscape and take a data-driven approach. Better system automation and pattern prediction can be accomplished by employing data intelligence to increase both efficiency and user experience.

**Interoperable:** In smart city applications, we can expect devices with varying capabilities and resource constraints to participate in the same system, and there will be constant data exchange within the system and external parties, imposing high interoperability requirements on the application. For example, most of the applications relies on cloud storage directly or indirectly, for storing the massive data incurred.

**B. Common Challenges of Applications in Smart City**

Standard security requirements for smart city applications include confidentiality, integrity, availability, and accountability, as well as practical security considerations, such as privacy, scalability, mobility, fault tolerance, interoperability, and others. A detailed set of security requirements for smart city applications can be found in [8] and also in [73].

Aside from conventional security challenges, such as maintaining data communication confidentiality, smart city applications will encounter a slew of new ones to meet those security requirements. For example, while security features in wireless communication technologies such as Wi-Fi have been extensively researched, many of the IoT wireless communication protocols have yet to receive adequate security updates. In Table III, we present the security properties of the commonly used wireless communication protocols for smart city IoT applications, as well as the security challenges associated.

By examining the features of smart city applications in the preceding sections, we can derive a set of security and privacy challenges in smart city applications.

1) Securing wireless data communication between systems and between devices of varying capabilities in implementing security mechanisms is a significant challenge. Different parts of the wireless infrastructure in smart cities can be owned and operated by both the government and third-party service providers. Some parts of the wireless network can be vulnerable due to cross-platform interactions and unclear security responsibilities. For example, in many telecare medical information system (TMIS) applications, patient data in health monitoring systems are required to be transported from homes to government-controlled hospitals. The system will be vulnerable if neither party is concerned about the secure interaction between them or makes an invalid assumption about the effort that the other will place on securing the connection. Thus, integrated and end-to-end security solutions that meet the security requirements and wireless constraints, e.g., limited spectrum, are needed.

2) Allowing heterogeneous devices to interact in a safe and efficient manner is another significant challenge. We expect constant interactions with a variety of public and commercial systems in the smart city environment, and many of these systems are vital for public security. Public infrastructure, such as the intelligent traffic control system and the emergence broadcast system, must be secure. Otherwise, attacks on the IoT systems can...
The security requirements of data generated in smart city systems are time dependent, and providing adequate protection for sensitive information throughout its life cycle is a challenge that smart city applications must overcome. For example, video footage in public surveillance systems exhibits high sensitivity due to privacy concerns, but the degree of sensitivity depends on the recency of the video data. The video footage today can disclose more important information about the status of inhabitants than the video footage taken three months ago, so the more current the data, the more security protection is required here. As a result, providing adequate protection throughout the data life cycle necessitates careful consideration, especially given the massive data scale.

4) Smart city applications have to present a unified representation of the heterogeneous data acquired, which is both crucial and challenging. A unified representation of heterogeneous data types can support effective insight generation across devices and systems. It also allows systems to access the context and the security risk of the data exchange. Thereby, a more appropriate security setting can be established, avoiding unwanted interactions with sensitive data and preventing data loss. For example, with unified representation of data, smart health systems, and smart home systems can communicate efficiently with unified data representations to extend the physical range of their services and notify security breaches to prevent escalation of attacks from one system to another.

5) Another challenge for smart city application is to provide solutions for remote mass updates and system recovery in the event of an attack/intrusion. More malicious attempts by attackers probing for the weakest link in the system are likely to occur due to the large-scale physical deployment of IoT devices in smart cities, which increases the attack surface for attackers to interfere with system operations. At the same time, due to the massive deployment scale, a successful intrusion into these end devices might cause a tidal effect, compromising the security of the system, and even paralyzing it. Consequently, the effect of intrusion will be very significant and impacts many devices. For example, attacks on utility systems can paralyze the public infrastructure in cities within minutes. Thus, it is necessary to have solutions for efficient remote mass updates and attack recovery to increase system resilience.

In the following section, we will evaluate the specific context of each smart city domain and their security requirements from an ANT-centric perspective, presenting existing security proposals, and some of their shortcomings.

IV. CYBERSECURITY IN SMART CITY DOMAINS

In this section, we will provide a systematic study of the security context in each smart city domain, beginning with an overview of developments in each smart domain and the characteristics that applications in each domain will have. Following that, we examine the security requirements of these applications from an ANT-centric perspective and give examples of existing security solutions that may meet such requirements.

A. Smart Healthcare

1) Overview of Developments in Smart Healthcare: Aging will soon be the major issue that many nations must address, especially in developed countries with a high average life expectancy. The need for elder care increases significantly, while the establishment of an affordable, qualified, and responsive healthcare system remains of paramount importance for the quality of life of people. Fortunately, recent technology developments have paved the way for the transformation of the healthcare system into one that is data-driven, cost effective, proactive, personalized, and sensitive.

An illustration of major smart healthcare developments and some of the possible connections between them is shown in Fig. 3. For example, TMIS is a telehealth system [74] that offers remote health monitoring and consultation services for its users. In TMIS, IoT sensors, such as smart wearable body sensors, smart healthcare sensors, and other IoT sensors are
used to provide real-time or periodic updates on patient physiological signals. Information, such as ECG data, physical movements, and air quality are collected and analyzed or monitored on remote servers for medical professionals to analyze medical conditions.

Other developments for smart healthcare include wireless medical sensor network (WMSN) and Blockchain healthcare systems. WMSN is a network formed using wireless sensors deployed on the human body, which is responsible for monitoring vital health signals and transmitting data out of the network periodically [75]. At the same time, blockchain healthcare systems present a distributive solution to protect the data integrity of personal health data in the cloud, utilizing the immutability of blockchain transactions.

2) Characteristics of Applications: Smart healthcare applications often exhibit the following characteristics.

Data-Driven: Many of the proposed smart healthcare systems rely significantly on sensor data to perform functions, such as health monitoring, medication reminders, and tele-healthcare consultations. These systems are highly data-driven in that their logic flow always centers around the use and storage of data. Depending on the nature and variation of the collected data, smart healthcare systems take their respective decision paths to trigger their procedures and alerts. Hence, the security design of smart healthcare systems will then mandate strong protection toward data flow and data interactions concerning sensitive patient data.

Cost Effective: Smart healthcare systems are often built to be cost effective and to achieve affordability to include more people who may not be able to enjoy healthcare services today. The current smart healthcare system mainly revolves around two types of smart healthcare IoT devices: 1) clinical healthcare devices and 2) personal healthcare devices. Examples of clinical healthcare devices include smart continuous monitors for heart rate and glucose level. Personal health devices, on the other hand, act as portable data collectors and aggregators to provide remote monitoring and health measurements for personal healthcare advice or care. They include devices, such as smart wearable and self-monitoring activity trackers. With the use of such devices, many patients could choose home monitoring and recovery as well as remote medical consultation for minor illnesses, saving money on hospitalization and travel. Such developments will impose strict constraints on the accuracy and integrity of sensor readings and the availability of smart systems, requiring a robust, and secure environment for data communication.

Proactive: The conventional healthcare system is often passive and reactive, where patients seek medical advice only when severe symptoms appear. This can lead to the escalation of illnesses where early stage treatments are almost impossible when patients do not pay much attention to their health status. In smart healthcare systems, constant health monitoring is employed to identify critical health signals on a regular basis and to warn users of abnormal health statuses, allowing for early intervention of health conditions. Hence, the design of smart health care systems would extend their considerations to include monitoring preillness factors that can potentially contribute to illness.

Personalized: Smart healthcare systems are highly personalized to cater to different healthcare needs of individuals. Depending on the user’s health history and conditions, smart healthcare systems will have a different monitoring emphasis. Professional medicare will also have a set of features customized in smart healthcare systems to cater to various illnesses and diseases. Nevertheless, such personalization will necessitate a large database architecture in smart healthcare systems that can adjust the content of their services based on individual demands.

Sensitive: Healthcare data are very sensitive and heavily regulated, and applications that interact with it must provide extensive data protection. A successful attack on smart healthcare systems could result in life-threatening situations. Although the size of the deployment for these systems may not be as large as that of smart utility systems and the deployment environment is often in hospitals or residences with limited physical access, the hardware and software security of the components of the smart healthcare system is crucial. Meanwhile, patient anonymity and data confidentiality would impose heavy privacy concerns on such systems.

3) ANT-Centric Security Requirements: In smart healthcare applications, it is vital to protect critical activities that communicate or store sensitive information about the personal health information in their operations, as shown in Fig. 3. From an activity-centric view, we focus on the end-to-end healthcare data flow, from the generation and collection of medical data to its transmission and processing in the data center or cloud. Since cross-platform and cross-device data communication is expected in many smart healthcare applications, a secure communication environment that protects sensitive data flow from end to end is necessary because it is difficult to account for the security of all possible data interactions between devices. In addition, secure storage of sensitive medical data is also crucial for maintaining user privacy and data integrity. From a network perspective, it is crucial to ensure that all critical data communications occur at critical nodes that will involve critical data activities are authenticated to prevent illegal access and data confidentiality violations. For example, it is essential for both the patient and the doctor to authenticate themselves to the systems in order to establish mutual trust. From a things-centric perspective, we consider security issues that are closely tied to healthcare devices and systems. To avoid mishaps in smart healthcare applications that deal with sensitive health data, it is critical to have system resilience against attacks, where systems can detect suspicious activity that risks data integrity and confidentiality, especially when actual medical treatments are involved.

a) (Activity-centric) secure communication environment: While secure communication between system components is necessary, an end-to-end secure communication environment is also a prerequisite for smart healthcare applications. Since the security of a system is determined by how well the weakest link is protected, any parts of the system that are insecure can be the easiest target for attackers. In smart healthcare, our personal health monitoring devices, such as health trackers or smart watches, are constantly transmitting sensitive information about our physical conditions. These devices often
have a limited ability to protect themselves and are transmitting important information, making them the most vulnerable components that deserve the most protection.

For instance, suppose we constructed a complicated cryptographic technique to protect wireless communication between the third-party database that stored our health data and the cloud and we did not establish a secure communication environment between the cloud and the end device. In that case, an attacker could instead attack this connection and capture all the important personal data passed. Thus, we should enhance the security of our smart healthcare applications by extending our security protection right from the start, from where data generation occurs. While there have been many proposals that could provide valuable insights toward fulfilling this requirement, most of them focus on securing parts of the system, such as end-to-end authentication [76] or end-to-end secure key management [77], rather than the complete end-to-end communication security.

In [78], there is a proposal for end-to-end security by enforcing the adoption of the same security protocols throughout the system. The work in [78] is a secure architecture built upon the DTLS protocol for mobility-enabled healthcare IoT. All parties communicating in the system mutually authenticate each other and establish secure sessions via a shared common key. Assuming that smart gateways have sufficient resources to perform security operations, smart gateways ease the computation burden on behalf of medical sensors by performing authentication and authorization of remote end users. However, this application assumes that the application is implemented in smart homes/hospitals where authorized personnel cannot enter the physical premises, eliminating the need for authentication and authorization for remote healthcare centers or caregivers to those sensors. Thus, this design requires an assumption of physical security of the environment, which may fail to protect against malicious insiders and physical intruders. On the other hand, SecureSense [79] combined the DTLS protocol with CoAP to achieve an end-to-end secure communication architecture for the cloud-connected IoT where certificate-based asymmetric cryptography is applied to compliment the cryptographic capability of DTLS. Similarly, the work in [80] attempts to adapt the 6LoWPAN protocol to integrate lightweight end-to-end security to provide a secure communication environment, which they call 6LowPSec.

Although a universal security protocol could improve system security by providing consistency, such protocols will need to specify further their context and the minimum requirement on the hardware and software capabilities for their implementation to improve their feasibility. Alternatively, we could have a centralized agency that defines a set of security protocols for different types of devices or data. Thus, any device wanting to communicate with each other must support the common set of security protocols and pass specific security checks before proceeding with the wireless communication.

b) (Activity-centric) secure storage: The final stage of the data life cycle in a system will be its storage and management. A vulnerability in one of the wireless communication channels can expose a confined set of data exchanges to the attacker. When discovered early, its damage can be constrained within a relatively small range. On the other hand, a database vulnerability puts all information stored in the entire system at risk. As a result, in addition to improving data transmission security, ensuring data security at rest is also crucial, and it is especially so for sensitive healthcare records stored in cloud servers and hospitals.

This article classifies secure storage mechanisms into two types: 1) secure distributed storage and 2) secure cloud storage. Distributed storage refers to the use of storage space on distributed nodes to provide storage services, avoiding a single point of failure. Kher and Kim [81] proposed a set of security services that a secure storage system should support. It includes authentication and authorization, to validate the identity of the party accessing the database; availability, to ensure that the data is readily accessible for authorized parties, where the system would have to perform backup and recovery services; confidentiality and integrity, so that users can trust the system in keeping their data; key sharing and key management, to facilitate efficient sharing and retrieving of data; auditing and intrusion detection, to monitor and detect unauthorized access; usability, manageability, and performance, to provide smooth data storage services to enhance user experience. There has been an exploration on different technologies in achieving secure distributed storage, such as the combination of SHA-3 and Reed–Solomon (RS) erasure code [82], secure erasure codes [83], redundant residue number system (RRNS) [84], and blockchain [85]. Depending on system configurations and application context, some of these mechanisms are more suitable than others. For example, SHA-3 offers more compatibility than blockchain, where many existing systems have been built to support SHA-3.

On the other hand, Yang et al. [86] and Ghani et al. [87] have surveyed the security issues for cloud storage. Issues, such as data confidentiality, atomicity, data access, and data breaches have been presented in these surveys, coupled with different security mechanisms to resolve those issues, such as identity-based encryption, attribute-based encryption, homomorphic encryption, and searchable encryption. In smart healthcare applications, the location of data storage as well as the level of complexity in secure storage protections differ from one another. Nonetheless, system designers will need to determine the optimal tradeoff between computational complexity and storage and access security, ensuring that data of varying sensitivity is adequately protected.

c) (Network-centric) authentication: In smart healthcare applications, authentication is the first line of defense for a secure communication channel. It validates the identity of the patient/user who is exchanging information with the medical systems. When paired with an authorization system, the authentication protocol could ensure that only authorized users/devices have access to or upload sensitive medical records, hence protecting confidential medical information from exploitation.

Hardware-based authentication protocols for smart healthcare systems have been proposed in [29] and [31]. Alladi et al. [29] proposed a lightweight authentication protocol, to mitigate the risk of physical node tampering and
node replacement attacks on smart healthcare IoT devices. Their two-way two-stage authentication scheme implements the physical unclonable functions (PUFs). The use of PUFs allows computationally expensive cryptographic operations to be performed in the PUF chips, saving precious resources on the smart device. While both logical and physical security during data exchange has been enhanced via the adoption of PUFs, the scheme requires the challenge and response pairs of every PUF to be stored in the cloud database, prior to the deployment of these devices and be retrieved for each round of authentication. This will limit the scalability of the scheme because when the number of smart devices in the network increases, there would be increasingly significant storage demand and time delay due to cloud access.

Similarly, xTSeH [31] aims to build a trust chain from the hardware level to establish a network of trust for the smart healthcare IoT devices. The scheme extends the security functions of the trusted platform module (TPM) to smart embedded devices (SEDs) (also refers to smart healthcare IoT devices here) that were not equipped with TPM, using TPM-chipped SEDs as the root of trust. Application-level proxies were designed as a communication bridge between the root of trust and non-TPM-chipped SEDs that requires authentication, verification, or trusted booting services. This scheme protects system integrity and ensures the authenticity of smart devices. However, these security services impose a significant delay on system performance, especially the validation of the non-TPM-chipped SEDs. This is a challenging bottleneck because TPM chips process in serial, hence, further optimization will be needed.

There are many proposals for software-based authentication as well. An overview of the different biometric-based authentication methods for smart healthcare can be found in [88]. Awasthi and Srivastava [21] proposed a three-factor authentication scheme for TMIS to enable secure data transfer between smart healthcare IoT devices and remote servers, as well as to provide medical personnel authorized access to patient data. This scheme is found to be vulnerable to offline password-guessing attacks, reflection attacks, and fails to provide patient anonymity [22], [23]. To overcome the drawback in Awasthi and Srivastava’s approach, both [22], [24] suggested their version of three-factor authentication protocols using the smart card. Later, these schemes were found to be susceptible to offline password-guessing attacks and lack patient anonymity as well [23]. From that point, Mishra et al. [23] proposed another three-factor authentication protocol using a personalized smart card, which [25], [26] conclude to fail in protecting against server impersonation attacks, stolen smart card attacks, and being irresistible to MITM attack and replay attacks. Deebak and Al-Turjman [27] reviewed authentication protocols on the secure smart healthcare system adopting smart healthcare IoT devices. Furthermore, they proposed a mutual authentication scheme for the cloud-assisted medical information system, allowing the secure exchange of electronic medical records (EMRs) and patient data without data duplication. However, they did not address the issue of secure communication during remote registration of medical devices and patients with the healthcare center, nor the secure storage of medical records in the system. A summary of the different authentication techniques that have been used under the various smart domains is presented in Table IV.

d) (Things-centric) system resilience on attacks: Keeping resilience to deal with insider and outsider risks and attacks is crucial for smart healthcare applications. In health monitoring systems and WSNs, we have sensors and actuators that are always monitoring important health signals and transmitting this data to the cloud or hospital for health risk evaluations. If wrong information regarding a person’s health is transmitted, incorrect medical assessments and threats can be made, perhaps leading to life-threatening consequences. As a result, it is critical for smart healthcare applications dealing with sensitive health data to detect suspicious activity that threatens data integrity and confidentiality, especially when actual medical treatments are involved.

As described in [89], resilience mainly focuses on the integration of runtime situational awareness and prior risk analysis, which means that a resilient system should have the ability to take proactive defense and mitigate countermeasures against attacks to maintain system security and robustness. As one of the most important security posture monitoring tools, intrusion detection systems (IDSs) can identify suspicious activities and detect possible attacks to make the network run in more security and normal operating state. There exist many mature intrusion detection techniques for the traditional network system. However, these IDS techniques can not be applied to IoT systems directly because of the many different characteristics between healthcare IoT and traditional network systems. Complex and high computational techniques are not suitable for healthcare IoT system as it is constrained, and there are many lightweight health trackers/sensors in smart healthcare applications, which we should consider their memory capacity, battery life, and network bandwidth when designing security detection approaches [90].

New machine learning and deep learning methods for detecting abnormalities in smart healthcare applications have emerged as a result of recent breakthroughs in artificial intelligence. Such methods place a little computational burden on the user device and can detect anomalies with astounding accuracy. Iwendi et al. [91] developed an IDS for network traffic in smart healthcare systems by combining a genetic algorithm and the Random Forest algorithm on network traffic data. Their proposed algorithm achieved a detection rate of 98.81% and a false alarm rate of 0.8% on the NSL-KDD data set. However, this approach can be further improved by considering the patient’s biometric data as well. For example, Hady et al. [92] built

| Authentication Techniques | References |
|--------------------------|-----------|
| Hardware-based authentication (TPM & SED) | [29] [31] |
| Software-based authentication (ECC & RSA) | [44]–[46] [55] [59] [67] |
| Biometric-based authentication (Facial & Iris & Fingerprint) | [88] |
| Multi-factor-based authentication | [21]–[26] |
their IDS utilizing both the network traffic data and patients' biometric data. It has been discovered that by training with both biometric and network traffic data, the detection accuracy of IDS will be similar to, if not greater than, that of the best performing using either traffic or network data.

B. Smart Utility

1) Overview of Developments in Smart Utility: Smart utility generally refers to public gas, electricity, and water systems that use smart infrastructure to provide safe, more efficient, and reliable utility services. Such a system is often data-driven and proactive, with real-time detection capabilities and system intelligence, as well as one that allows for constant user interaction.

An illustration of major smart utility developments and some of the possible connections between them is shown in Fig. 4. There are three common types of smart utility systems: 1) smart gas management systems; 2) smart water systems; and 3) smart grids. Smart gas management systems incorporate smart sensors on our gas systems, mainly designed for system monitoring (load monitoring) and detection (gas or fire detection). Smart water systems enable cities to manage better and administer their water systems. Its main issue is the lack of consistent methodology and a unified data interpretation to develop a comprehensive water management infrastructure that encompasses all parts of a city’s water network, resulting in partial solutions that address specific problems in a given context. On the other hand, a smart grid transforms the electric power grid to allow interactive real-time connectivity between users and devices, allowing two-way high-speed communication across applications for smart system monitoring and control. A successful attack on the electrical grid has the strongest instant negative ramification among all attacks on public infrastructure.

2) Characteristics of Applications: Smart utility applications often exhibit the following characteristics.

Data-Driven: IoT sensors are placed around critical infrastructures to constantly monitor the physical condition of the system and its components, providing important system measurements and feedback for performance analysis. For example, pressure sensors and temperature sensors are common IoT sensors deployed to monitor the physical state of a system component in smart utility systems. With such data collected, smart utility systems can generate useful insights on consumption patterns, system maintenance needs and make optimal operational decisions. Hence, smart utility system designs are often centered around data collection, processing, and storage.

Proactive: In traditional utility systems, we regularly perform periodic maintenance services to monitor system condition and prevent unanticipated system breakdowns. This is time consuming and inefficient since we are unable to fully utilize our resources; yet it is needed to avoid unanticipated service disruptions. In the event of a breakdown, we undertake reactive repairs to save the faulty system components. With smart utility systems, we are able to constantly monitor our system components and even predict the optimal maintenance timing from the data generated. By taking a proactive approach, the smart utility system can optimize resource utilization and deliver better service quality. To achieve proactiveness, smart utility systems often rely on strong machine learning models and data analysis techniques to predict patterns and provide actionable insight, which further exaggerates the importance of data integrity.

Real-Time Detection: Sensors for utility systems have a higher requirement for battery life than in other applications. Many of these sensors will be placed in physically inaccessible locations, such as in the underground tunnel or bottomless water tanks constructed miles deep in the ground. Replenishing the batteries inside these sensors in such scenarios would be a challenging task, and hence it is often left unmonitored. Thus, real-time detection is a special feature that smart utility systems can afford with the help of low-energy-consumption IoT devices and wireless communication protocols.

User Participation: A key functionality of smart utility systems is the interactivity between parties. By leveraging on the insight generated from system data, better market decisions can be made by utility companies, energy traders, and even consumers to balance the demand and supply of utilities with market force. Since more data communication
between different parties is expected, strong authentication is a prerequisite for reliable user participation.

3) ANT-Centric Security Requirements: From an activity-centric view, securing essential activities that may affect the availability and accuracy of data over the full data life cycle is critical to the security of the system in smart utility applications. Integrating data collected from numerous smart utility sensors, applications, and processes is a critical and complicated task, as illustrated in Fig. 4. As a result, in order to preserve the overall security of the ecosystem and data flow, we must address the potential security concerns associated with such integration. Furthermore, smart utility applications will necessitate efforts to maintain Quality-of-Security-Service (QoSS) in order to protect the data flow’s health throughout its life cycle. From a network-centric perspective, authentication is an essential security requirement against network attacks, ensuring that all critical data communications occur at critical nodes are appropriately protected so that data integrity and system availability can be maintained. From a things-centric perspective, we consider security issues that have a direct impact on smart utility devices and systems. Due to the extensive attack surface of smart utility applications and the strong instant negative ramification on public infrastructure, there is a requirement for system resilience on attack in the form of a strong healing ability after attacks occur to limit the damage caused by attacks.

a) (Activity-centric) secure integration: Integration for data collected from various sensors, applications, and processes is challenging. It is difficult to group multiple technologies into one for smooth data collection. The context and environment from which the data value is collected vary significantly. The smart grid may employ blockchain for autonomous user transactions on electricity, where electricity is priced in terms of system currencies, whereas smart water management systems price based on the cost of water treatment per household and real consumption. This contributes to barriers in providing consistent data interpretation, and additional contextual data need to be present to generate useful insights for end users.

More importantly, we must consider the potential security risks associated with such integration. Since mandating a uniform set of protocols to be implemented by different utility system is currently challenging, the systems will try to connect resource-constrained devices securely using the methods that those devices support [93]. Some devices can support a basic mechanism, while others do not attempt to protect user information. For example, a sophisticated smart utility management server may protect consumption data by encrypting it with strong cryptographic mechanisms; however, these data are decrypted by smart gateways and distributed to end point devices such as smart meters installed in homes, where the data is not protected. Thus, these devices became the weakest link in the system, where attackers could easily breach in, and attacks can rapidly escalate to the rest of the system. Hence, efforts for secure integration would be necessary to enhance system security.

These criteria can be fulfilled in a variety of ways. Although there are no proposals for secure integration of smart grid, smart water, and smart gas management systems, we can learn valuable insights from system integration proposals. For example, Khalid and Ameen [93] have provided a discussion on the recent effort toward secure integration. Similarly, a narrower integration perspective between IoT and cloud computing [94], blockchain [95] has also been studied.

b) (Activity-centric) maintenance of quality of security service: Similar to Quality of Service (QoS), Quality of Security Service (QoSS) is the concept that quantifies the level of security in a system, where a variable level of security services and requirements exist. The level of security in a system would then refer to the degree of security factors considered. This is a critical metric for ensuring the safe deployment of large-scale IoT applications in smart cities. Similarly, QoSS can enhance system performance and achieve higher user satisfaction to provide users or network tasks with a range of appropriate security choices [96].

Smart utility systems are often large-scale networks with a wide range of target users. It is anticipated that more interactions between systems and users will happen to optimize resource utilization, such as energy trading in smart grid systems and consumption monitoring in smart metering infrastructures. While users are becoming more aware of the importance of their privacy and data, common users cannot judge the level of security in a smart utility system due to a lack of measurable security metrics. Even when a manufacturer gives assurances about the level of security that users can anticipate from their system, there is no way for users to verify that these promises are kept. As a result, there is minimal transparency for consumer checks and balances, making it difficult to build trust with the users in such situations.

The development of QoSS parameters not only can build trust between users and manufacturers, but it could also gain user involvement in monitoring the system status to provide more responsive feedback on possible attacks. This is especially important for large-scale systems like smart utility systems, where it may take a long time before they can filter out any faults in the systems. As a starting point, the authors in [97] have provided a quantitative expert opinion survey (EOS) on the choice of quality criteria for the security metric, evaluating possible factors to consider for QoSS. Factors, such as accuracy and time dependability of the system, are possible candidates for the security metric.

On the other hand, the method used in [98] can be adopted for a data-centric approach for the development of QoSS. In this article, the appropriate level of security that the data deserves is determined by the path that the data has traversed in the system. To determine the final security level of the data, one has to refer to the security level given to all the physical components that it has visited, the various source data used in formulating it, the context where the source data is generated. By considering the sensitivity of all nodes and operations related to the data, we could determine the importance of the data and thus define a suitable level of security to enforce in our system to protect it. This approach can be used as a starting gear for system designers to evaluate the level of security their systems need. In summary, maintaining QoSS through
systems can help develop confidence between parties while also allowing for a thorough security evaluation for system designers to identify security risks early. This will encourage user interactions and better system monitoring via user feedback.

c) (Network-centric) authentication: Most of the existing literature on authentication of smart utility systems focuses on the smart grid, hence we will use the smart grid as an example to introduce how authentication can be done in smart utility systems. Due to the intrinsic scale of modern cities’ electrical grids, which are continuously connected to a huge number of devices and systems, there is a large “attack surface” for the attackers to exploit on [39]. This attack surface includes smart IoT devices, central servers, user end-point systems, and all other possible entry points for the attacker to intrude the system. Furthermore, the smart grid’s significant reliance on communication and networking infrastructure exacerbates this problem, posing system security, and privacy risks via the communication channel.

A successful attack on the electrical grid has the strongest instant negative ramification among all attacks on public infrastructure, as the majority of the city’s public systems will be paralyzed instantly. As a result, it is critical to incorporate security and privacy considerations into smart grid architecture, to protect the IoT devices and the system components. Xia and Wang [44] have proposed a simple and highly efficient secure key management system, with computation costs of 5 and 4 ms for a single authentication instance at the smart electricity meter and utility service provider, respectively. However, [45] points out that the scheme fails to provide security features, such as strong credential privacy and security for the session key. Likewise, Srinivas et al. [46] presented the AAS-IoTSG, a novel authentication scheme for the smart grid using ECC-based Schnorr’s signature mechanism. Although it also comes with a considerable computation overhead, elliptic curve cryptographic (ECC) is much stronger than the conventional AES and RSA keys with the same key sizes in the current context. It is thus a more efficient candidate if we choose to employ cryptographic algorithms. For example, we choose a nonsingular elliptic curve $E_q(u,v)$ of the form $y^2 = x^3 + u^3 + v(mod q)$ over a prime (finite) field $Z_q = 0, 1, \ldots, q - 1$ with a base point $P$. A 256-bit ECC key over this ECC curve is as strong as a 3072-bit RSA key. Hence, ECC can be a more suitable candidate to keep up with the growing cryptographic capabilities of the attacker.

d) (Things-centric) system resilience on attacks: System resilience against attack from insiders and outsiders is crucial for smart utility. As described in [89], resilience mainly focuses on the integration of runtime situational awareness and prior risk analysis, and once it is attacked, it can also return to a normal and healthy operating state as soon as possible. This is especially important for smart utility applications where a slight disruption of utility services will result in an extensive impact on the operations of smart cities.

Due to the limited memory capacity of the lightweight devices/sensors, IoT system such as the smart utility system is much easier to attack by the Distributed Denial of Service (DDoS) attack. Besides, the basic components of an IoT system that generate data and make wireless communications are small and simple devices/sensors instead of human or complex machines. It becomes more difficult to secure data privacy in different smart city applications than traditional Internet applications. For example, DDoS attacks on smart grid systems may cause power interruption, which will affect the normal life of individual users and hinder the production work of enterprises. Since most of the smart utility operations are time critical and safety critical, security mitigation countermeasures should consider meeting the critical conditions while devices/sensors or applications are under attack. For some applications that need to keep working in real time, multiple security responses and recovery methods should be arranged to enhance the system’s resilience. Due to the complexity of the smart utility ecosystem, where a large amount of data traffic is exchanged constantly between heterogeneous devices, designing for system resilience to attacks can be a very challenging security requirement but a necessary future direction before the adoption of smart utility systems.

C. Smart Transportation

1) Overview of Developments in Smart Transportation: Intelligence transport systems (ITSs) aim to improve the transport systems’ road safety, efficiency, reliability, and user experience for all road users, including pedestrians, train riders, motorcyclists, and everyone else who participates in the transportation network of the society. As a result, a variety of smart transportation applications have evolved to transform our safety-critical transportation system into one that is data-driven, interoperable, and capable of providing real-time intelligence. An illustration of major smart transportation developments and some of the possible connections between them is shown in Fig. 5.

Besides unmanned aerial vehicles (UAVs) and smart charging for electric vehicles (EVs). Some of the main developments toward smart transportation include Internet of Vehicle (IoV) distributed trust and intelligent traffic management systems. IoV distributed trust is an alternative trust management methodology compared to conventional centralized trust management where a single trust authority is responsible for generating authentication materials. Due to the extensive connectivity, changing topology, and requirement for privacy protection while guaranteeing proper traceability, authenticating IoV wireless communications is problematic. As a result, distributed trust management will aid in alleviating the present limits on IoV authentication tasks.

On the other hand, intelligent traffic management systems include smart traffic monitoring systems, smart road side units, and many more, they provide functionalities, such as in-transit attestation, authentication, and support many other operations, such as smart RSU, smart traffic control systems, smart traffic monitoring systems using UAVs to regulate and ensure safe driving practices, video-based traffic control for routing optimization using ant colony optimization, and vehicle-to-vehicle wireless communication.
2) Characteristics of Applications: Smart transportation applications often exhibit the following characteristics.

Data-Driven: Real-time traffic data collection is critical for strategic transportation planning. With more information, we can make better-informed decisions regarding our transportation plans and optimize our resource use. Sensors and cameras on vehicles and roadside infrastructure, provide vital traffic data, such as vehicle density, travel speed, and location. This data is transformed into useful information for tasks, such as traffic forecasting, route planning, surveillance, and more, where we utilize it for generating transport intelligence. Given the criticality of transportation systems in public security, there is a strong need to ensure data integrity and availability for data-driven smart transportation applications.

Real-Time Intelligence: In traditional transportation systems, traffic authorities typically invest significant resources monitoring current traffic conditions and attempting to resolve ongoing traffic accidents as quickly as possible to avoid traffic congestion. However, because of the massive scale of transportation networks, there is often a lack of manpower and technical capabilities to examine every single detail generated in the system. In smart transportation systems, real-time processing and insight generation can be done with the substantial computing power in the system and provide immediate feedback on the traffic condition, with a strong emphasis on resilience toward attacks on the availability of data and systems.

Interoperability: Higher interoperability is expected in smart transportation systems where cross-platform interactions can be integrated to improve the resource utilization in smart cities further. For example, smart transportation systems are typically paired with the smart grid system to enable routing and charging optimization for EVs. Similarly, end-user entertainment products, such as the smart phone and smart watch can interface with smart vehicles to provide user-friendly transitions between activities. Thus, secure communication for smart transportation applications needs to also consider interactions across platforms and devices.

Safety-Critical: Both traditional and smart transportation systems prioritize safety, yet the latter can reach higher levels of safety than the former. In fact, one of the main reasons for implementing smart transportation systems is to improve traffic safety and decrease the occurrence of accidents caused by human error. With improved sensing and computing capabilities, autonomous driving could provide a safe and efficient alternative mode of transportation for metropolitan commuters. Nonetheless, the security and privacy of the data collected are the top concerns for implementing reliable and safety-critical smart transportation applications due to their implication for public security.

3) ANT-Centric Security Requirements: From an activity-centric perspective, securing critical activities that may affect the availability, integrity, and confidentiality of data communication over the full data life cycle is critical to the security of smart transportation applications. With reference to Fig. 5, there are various types of smart vehicles that exhibit high computation power and are where much of the crucial data processing and storing occurs. Thus, securing these edge devices is important for protecting critical information flow and data activities in smart transportation applications. From a network-centric perspective, vehicle, and device authentication is a critical security requirement for establishing a trusted traffic network, guaranteeing that devices are who they claim to be. Furthermore, authentication can be integrated with identity management and access control to ensure that all important traffic communications are legal and adhere to the transportation authority’s access restrictions. From a things-centric perspective, we consider security issues of components and vehicles in smart transportation infrastructures. Secure updates are especially crucial for smart transportation applications because of the vast network of public transportation infrastructure, where on-site maintenance is impossible.

   a) (Activity-centric) security at the edge: Edge computing provides computation and storage offloading for many smart city applications. It uses edge devices to operate as microservers, collecting data from end nodes, aggregating, and filtering it, providing real-time feedback and completing any user requests it can, and only sending intensive processing and permanent storage to the central server. Securing wireless communication at the edge is an essential task for reliable
smart transportation applications. For example, UAVs can aid in edge network connectivity [99], caching, and computation. However, UAV-based applications have not been able to widely apply for real time and scalable tasks, due to their limited flight time, the requirement of periodic charging, and the lack of secure wireless communication protocols. Similarly, smart charging for EVs requires secure wireless communication between charging stations, service providers, and EVs, where they are seamlessly connected to make charging-related decisions.

Xiao et al. [100] believed that the introduction of edge computing has increased the attack surface due to the following.

1) Weaker computation power of the edge devices, which are vulnerable to existing attacks which are ineffective on most advanced systems now, such as small-scale DDoS.
2) Attack unawareness of the users, since users are generally unaware of the system states of sensors and panels if no user interface is provided.
3) OS and protocol heterogeneity, since there is little standardization across different edge devices.
4) Coarse-grained access control, besides conventionally access permissions, such as read and write, edge devices provide more capabilities that need to be regulated.

Besides the difficulties mentioned above, we have yet to establish a boundary for edge devices’ responsibility. For example, in cases where devices are incapable of applying any security measures, we need to decide if the edge server should be responsible for encrypting the data. If the data is worth protecting, another challenge is how we, or the edge server, determine the security level that should be applied to it or treat all data equally. From the standpoint of data gathering, we must decide whether the edge server should listen to any device or only a restricted group of devices in the physical environment.

Different combinations of technologies can be used to satisfy this requirement. System designers have to consider the different interactions with edge devices and employ appropriate security mechanisms. For example, multifactor authentication can prevent unauthorized access to edge devices, while complex cryptographic algorithms can secure communication between the cloud and the edge servers [101].

b) (Network-centric) authentication: IoV is a complex IoT device capable of sensing and controlling other subcomponents for autonomous navigation, making driving safer, and more enjoyable. By connecting wirelessly to roadside units and analytical cloud, its cognitive abilities are supported by an extensive smart transportation infrastructure that constantly provides traffic and environmental data. These smart vehicles are also expected to broadcast messages to the transportation infrastructure and vehicles in their immediate vicinity on a continuous basis to facilitate traffic information exchanges. While efficient data exchange is necessary for a pleasant driving experience, there is a primary requirement to guarantee the data authenticity; any malicious information could have disastrous effects on road safety. However, due to the extensive connectivity and rapidly changing topology caused by high mobility, authentication in the IoV has become very challenging. Furthermore, in order to protect users’ privacy, it is undesirable to authenticate IoV communications directly based on vehicle identities, because an attacker can simply infer the location of the vehicle by collecting broadcasted IoV messages. In order to protect user privacy, assigning pseudonyms to IoV that are frequently updated to ensure anonymity is a common way to establish conditional anonymous authentication. Such a method necessitates frequent changes to pseudonyms and is vulnerable to Sybil attacks, in which a single vehicle is capable of impersonating several vehicles using multiple pseudonyms.

As a result, to reduce the risk of Sybil attacks, it is necessary to be able to determine whether several signatures on the same message belong to the same vehicle, which leads to the concept of message-linkable group signatures. However, there is a key security flaw in this scheme: it assumes that the group manager can be trusted. For strict adherence to the “zero trust principle” where no party should be trusted, the author in [59] proposed a novel message linkable group signature scheme with decentralization tracing (MLGSDT) for conditional anonymous authentication with abuse-resistant tracing in IoV. By combining the MLGSDT scheme and the decentralized group model, the proposed mechanism could achieve a distributed trust for IoV in smart transportation.

c) (Network-centric) identity management and access control: Identity management and access control refer to the technology that makes a set of rules to define who meets the requirements for accessing, using, or modifying certain resources or data in specific devices of a system. Identity management and access control can also be called identity and access management (IAM). IAM ensures the security and productivity of the system by allocating the right resources to the right objects. It is a key technology to protect information security and avoid unauthorized data access by authorizing and revoking authorization based on delegation policies [102]. In smart transportation systems, traffic data is both safety critical and time critical. Traffic authorities require an effective and highly secure IAM in order to deliver important traffic information, claim liabilities for traffic accidents, and track violations of traffic rules.

Unlike traditional Internet systems, IAM in smart transportation focus more on the digital management of devices that hardly require direct manual operation and involve the management and authentication of users and services. For example, Khodaei and Papadimitratos [103] believed that designing a security infrastructure, such as a vehicular public key infrastructure (VPKI), will enable secure conditionally anonymous vehicular communication. However, there are several challenges for implementing such IAM in smart transportation systems, including but not limited to revocation, credential abuse, default password risk, virtual eavesdropping, and some extreme environments for on-site access control management. More recently, there have been attempts to build IAM for smart transportation via the blockchain. By utilizing decentralization and immutability of the blockchain technology, blockchain-based decentralized identity management system can provide strong security and transparency for all parties in smart transportation.
systems [104]. However, there have always been computation and compatibility concerns for the adoption of blockchain technologies.

d) (Things-centric) secure updates: Due to the enormous number of smart transportation infrastructures deployed, on-site maintenance is no longer feasible, especially for urgent mass updates for security patching. This has directed our interest toward remote updating mechanisms, performing updates, and integrity attestation over the air. However, due to the wireless nature of such mechanisms, security concerns have become growingly prominent.

A combination of different security approaches can be adopted to satisfy this requirement. For example, in [105], secure code update by attestation (SCUBA) is presented for resource-constrained IoT sensor networks to perform detection and automatic recovery of compromised nodes via secure code updates. SCUBA identifies compromised regions using authentication and software-based attestation and transmits the code update to repair the infected region. Similarly, Perito and Tsudik [106] proposed a Proof of Secure Erasure (PoSE) scheme for the secure remote update. In PoSE, the prover first performs secure erasure of all writable memory contents to remove possible malicious code before retrieving and installing code updates. However, it is pointed out by [107] that SCUBA and PoSE have significant drawbacks that make them unrealistic for deployment. The assumption of strict local wireless communication, or the lack of support for version roll-back if the current version fails, contributes to their unsuitability.

D. Smart Homes

1) Overview of Developments in Smart Homes: A smart home, also known as an automated home, is a home that is filled with the physical embodiment of an integrated and automated context-aware support system that improves our quality of life [108]. The intelligence of our interactive home system arises from its ability to be context-aware. It gains its perception via sensor readings obtained from IoT devices, which quantifies the physical phenomenon emerging from human activities, to convey the context around the inhabitant [109]. In summary, a smart home is one that is data-driven, context-aware, personalized, and interoperable. An illustration of major smart home developments and some of the possible connections between them is shown in Fig. 6. One of the most significant advancement in smart home systems is their integration with the smart grid, enabling improved automation in smart homes by allowing various smart home applications to interact with the smart grid to obtain data, such as utility consumption and market price. However, implementing this integration will necessitate cross-platform data communication and impose severe data security challenges.

2) Characteristics of Applications: Smart home applications often exhibit the following characteristics.

Data-Driven: A smart home system is always data-driven and requires constant SA to improve the user experience. The smart home typically consists of smart IoT devices equipped with a wireless communication interface, which forms a wireless sensor network. A central hub device is present to perform local processing, storage, data aggregation, and forward/receive information over the Internet. The cloud is expected to manage insight generation from the continuous, heterogeneous pool of data given by smart homes. Thus, the entire system flow of smart home systems is centered around the collection, processing, and storage of data.

Context-Aware: Context awareness, or the ability to gather information about the surrounding environment and adapt system behavior, is a fundamental feature of many smart home systems. Smart home systems can recognize events in the environment and forecast future patterns of interactions using sensor data, delivering relevant knowledge that allows systems to adapt to the lifestyle of the occupants. The capacity to deliver context-aware insights about the user raises serious privacy and security concerns concerning the use and storage of sensitive personal data.

Personalized: From the contextual data, our smart home systems could deduce the current status and provide adaptive services as defined by the user or its default algorithm. A smart temperature sensor, for example, can detect the presence of human activity by comparing records in its database with
a sudden spike in temperature, which can activate the user’s default lighting. As a result, consumers can experience a personalized set of services in smart homes that adapt to their own behaviors and preferences. Nevertheless, such personalization will require model training over a large amount of sensitive user data and exhibit a strong need for data integrity and confidentiality.

Interoperability: A smart home must be highly interoperable with cloud services, third-party applications, and consumer devices. In a typical smart home, the cloud maintains data security and secrecy and provides reliable services to enable the operation of third-party applications. These third-party applications are designed to provide interactive home automation services to users who could enjoy personalized smart home control via their mobile gadgets. For instance, many of such applications would leverage the system’s contextual feedback to provide users with sensing and proactive recommendations. However, many IoT service providers built their IoT solutions using noninteroperable hardware, context-specific features, and unique architectures that produce fragmented deployments rather than collaborative ones [110]. While safeguarding data communication across devices and platforms is critical to overall system security, noninteroperable devices do not allow for secure and efficient data communication.

3) ANT-Centric Security Requirements: In smart home applications, it is vital to protect critical activities that communicate or store sensitive user information in their operations. As shown in Fig. 6, a typical smart home relies on a variety of smart systems and devices to provide context-aware and intelligent services to its residents. Hence, secure integration of these devices and systems is an important requirement for protecting critical data activities in smart home applications from an activity-centric view. From a network-centric perspective, system and device authentication, identity management, and access control are critical to prevent unauthorized access to smart home devices and, to protect sensitive user information. These security requirements are crucial for safety, especially in smart home applications where unauthorized users can do harm to the owners by engaging in undesirable activities. From a things-centric perspective, we consider security issues that have a direct impact on smart home devices. Among all other things-centric requirements, secure updates are especially crucial for smart home applications because on-site servicing of every smart home in town will be highly inefficient and inconvenient for the inhabitants.

a) (Activity-centric) secure integration: A typical smart home relies on a variety of smart systems and devices to provide context-aware and intelligent services to its residents. For example, smart homes will rely on smart utility systems components to offer continuous feedback on utility service consumption and system status. Such data is transformed into insights on energy trading, user consumption analytics, and even reports on leak detection. Integration of data collected from various sensors, applications, and processes is challenging, especially when smart homes have to deal with heterogeneous third-party smart household devices. It is challenging to combine different technologies for efficient data collection. The context and environment in which the data value is acquired varies considerably. This adds to the challenges of delivering consistent data interpretation, and extra contextual data is required to create relevant insights. More importantly, we must address the potential security threats that such integration may bring.

Unfortunately, no examples of smart automation systems achieving system-wide security have been provided due to the high complexity involved. Nonetheless, Saleem et al. [43] have provided a good starting point where they consider the integration of the smart grid with home automation systems via a layered network structure. In this structure, a home area network (HAN) is deployed in homes, connects electrical appliances with the smart meter, and is responsible for managing the power demand of residents. On top of the HAN layer, the field area network (FAN) collects service and metering information from multiple HANs and transmits data to a data collector. The data collector will then exchange information with the wide area network (WAN) for system-wide communication to support optimization schemes and analysis. Different application domains of these network layers have also been presented here. In addition, applications of HAN include remote home monitoring and control systems, advanced metering infrastructure (AMI) providing a two-way flow of power consumption data, integration of distributed energy resources (DERs) for better predictability and reliability of nonrenewable power supply, and power demand management for consumers to reduce their utility bills.

b) (Network-centric) authentication: The majority of the literature on smart home system security is centered on user authentication and identification, to prevent unauthorized access to smart IoT devices and to protect sensitive user information. Various remote user authentication scheme has been reviewed in [67], and most of the proposed scheme either fails against stolen smart card attacks or privileged insider attacks or cannot support mutual authentication. Hence, the authors proposed a secure remote user authentication scheme using symmetric encryption/decryption, XOR operations, and one-way hash functions. Although the system has been confirmed to be resistant to attacks, such as device/smartphone capture attacks and user/device/gateway impersonation attacks, the use of a biometric key and a 1024-bit secret key puts severe memory constrain on the smart IoT devices. In addition, all smart IoT devices, users, and gateway nodes must complete secure offline registration with a trusted registration authority (RA), this hinders the scheme’s usability. Nonetheless, authentication in smart homes would require careful consideration of what to protect and how robust the security system should be. Following these decisions, system designers may acquire insights about feasible authentication schemes from other smart city domains.

c) (Network-centric) identity management and access control: Identity management and access control refer to the technology that makes a set of rules to define who meets the requirements for accessing, using, or modifying certain resources or data in specific devices of a system. This security requirement is safety-critical in smart home applications where unauthorized users can bring damage to the owners by
performing undesirable activities. For example, to avoid accidents, a visiting acquaintance should not be given access to the coffer, and children should not be given access to adult medicine.

A low-cost and user-friendly smart home environment with access control is proposed in [111], where they employ off-the-shelf sensors and technologies for building their smart environment. Similarly, the work in [112] presents a practical solution for context-sensitive access control in smart home systems. Their approach relies on constant monitoring of network data and detecting behavioral anomalies, and they build access control and use cases based on the knowledge graph they build. Despite the simplicity of these approaches, the presence of access control rules in both proposals will be a significant burden when a more complex smart home environment is presented.

d) (Things-centric) secure updates: Remote updates are necessary for smart home applications because on-site servicing of every smart home in town will be highly inefficient and inconvenient for the inhabitants. Furthermore, in order to protect our users’ safety and privacy, we must address the security problems raised by remote updates due to their wireless nature.

A combination of different security approaches can be adopted to satisfy these requirements. Besides those secure updates proposals mentioned in smart transportation, another recent direction for secure updates is the application of blockchain technology. Since the update package must maintain its integrity without compromising the code’s privacy, blockchain may be a viable option for implementing secure updates. Due to the unmodifiability and transparency of blockchain, the concern for unauthorized modification will no longer exist. Any node in the distributed network can verify the validity of the update package it receives. Due to the distributed nature of blockchain, no central agency will be needed to facilitate mass updates, and it would be possible to rely on peer nodes in relaying update packages. An example of blockchain-based secure update for IoT can be found in [113].

In the next section, we will investigate the challenges and gaps that current security solutions have to overcome to meet the set of security requirements from an ANT-centric perspective.

V. SECURITY CHALLENGES FOR SMART CITY APPLICATIONS FROM ANT-CENTRIC VIEW

The interconnectedness between smart devices has a significant impact on how we live in cities, enabling a smarter, cheaper, and more convenient alternative lifestyle. These IoT-enabled smart devices could perform tasks ranging from simple lighting control to complex traffic management in metropolitan cities. Due to the vast capabilities of these smart systems and the magnitude of their impact on our lives, they require an unprecedented level of trust from their users. This trust stems from the technology’s reliability and security and the system’s commitment to protecting users’ private assets, such as private data and accounts. McKnight et al. [114] mentioned in one of their studies that “one is more likely to explore and use more features of a technology if one trusts it.”

With the unique set of security requirements for building a smart city from the ANT-centric view, many current security proposals in Section IV may fail to meet them due to emerging challenges like the assumption of trusted cloud server. While numerous proposals have been made for secure smart city applications, most schemes that use contemporary innovations, such as blockchain, cloud, and edge servers, need to focus more on one or more security requirements. Furthermore, with growing connectivity between heterogeneous devices and systems in smart city applications, developers have to address a new set of security challenges in addition to the traditional security challenges. In this section, we present the set of challenges that current security solutions for smart city applications will encounter in meeting this set of requirements and provide a new research perspective toward the evaluation of security frameworks and design. These could also serve as future research directions where research can be aimed at fulfilling these challenges in existing frameworks or giving insights into future research directions.

To better illustrate these security challenges, we categorize them according to the ANT architecture. In this view, the activity-centric perspective facilitates understanding of system components’ context and identifies security challenges relating to the sensitive operations performed in the system. In comparison, the network-centric perspective focused on security challenges for wireless communication between network components and the flow of sensitive data. The things-centric perspective aids in understanding the relationship between the security challenges of heterogeneous data acquisition via heterogeneous IoT devices.

A. Activity-Centric Security Challenges

The activity-centric perspective facilitates understanding of the context of system components and identifies security challenges relating to the sensitive operations performed in the system. We have identified a few security challenges related to the usage of edge/cloud systems and challenges originating from big data and the use of big data in our operations, which are more relevant to IoT systems in smart cities in this section.

1) Assumption of Trusted Cloud/Edge: The adoption of cloud infrastructure to improve the efficiency and performance of our systems is a key feature of the 5G network [115], [116]. In many smart city applications, the edge cloud is essential for bridging the central cloud and the local user to facilitate efficient data exchanges. Similarly, the adoption of edge servers for storage or computation offloading has become popular due to its relatively low latency and high computation capabilities. However, a significant challenge for such applications is the assumption that the cloud/edge can always be trusted. Coppolino et al. [117] have identified the main security challenges in the cloud, including shared technologies vulnerability, data breach, account or service traffic hijacking, DDoS, and malicious insiders. To guard against data theft, system designers have to consider major players, such as external attackers, malicious internal users, and even hostile employees from cloud providers. Furthermore, solutions employing hybrid cloud and edge cloud also have to
consider intercloud interactions’ security to ensure consistent data protection throughout the backend process.

2) Accommodating Enormous Data Volume and Dynamic Traffic: With the deployment of smart IoT sensors in cities, large amounts of data are continuously generated, and this data forms the backbone of urban intelligence. This data load poses a significant challenge to the current technological infrastructure in processing, storing, and providing real-time insights. As a result, resource allocation and system performance optimization are critical for systems to meet their expectations in the face of large data volume. In this context, any system attempting to address smart city issues needs to be prepared to handle a nonperiodic, sudden burst of data gracefully. Depending on the application, this could entail efforts to maintain timely service delivery in a time-sensitive application or handle an unanticipated burst in data volume without compromising service quality. Similarly, the security mechanism must accommodate an instantaneous surge in traffic without compromising security or performance, guaranteeing that the QoS promised to the user is delivered.

3) New Types of Interactions: Different smart city systems could potentially interact due to the growing connectivity between them, leading to the frequent occurrence of cross-system or cross-platform interactions. Thus, a proliferation of new interaction types and styles can be expected. We will need to specify rules for handling such nontraditional interactions and incorporate resilience into our systems to protect against them. In addition, system designers have to consider the system’s openness and account for the security risk for possible interactions with external platforms or users.

Consider the case of D2D wireless communication resource allocation in IoT applications, where there is a high density of smart devices per unit area that constantly demands communication resources. According to Hussain et al. [118], this leads to congestion, network overload, and degradation of the Signal Noise Ratio in the wireless communication channel. While the traditional centralized approach deals with large but infrequent data transmission from traditional communication devices, IoT devices require a new approach for small and frequent data exchanges. Additionally, while frequent packet transmission might be a sign of flooding in many traditional systems, many IoT device interactions are characterized by small and frequent data transmission; therefore, accessing such metrics the same way as conventional systems would be inappropriate. For example, the diverse IoT platforms and support for heterogeneous end devices have made device management a highly complex task where conventional ML models that train on HTTP and TCP flows are not suitable for IoT-enabled end devices that operate on lightweight communication protocols. To account for both spatial and temporal features, the authors in [119] and [120] have proposed ML and deep learning pipelines to model the behavior of IoT devices.

Similarly, the temporal, once-only interaction with unknown smart devices can disturb system security in smart city scenarios. In the case of IoV, a user might travel to a neighboring country and share data with other IoV or smart transportation infrastructures there. The two transportation systems may not use a single platform and protocol due to different government regulations. However, to fully utilize the capabilities of IoV, the car must interface with other devices to gather traffic intelligence. While most of these interactions will be once-off, it is necessary to provide security protection to ensure the security of the device itself, i.e., not to be hijacked by others or attacked.

4) Lack of Unified Representation: A unified representation of heterogeneous data types can support effective insight generation across devices and systems. It also allows systems to access the context and the security risk of the data exchange. Thereby, a more appropriate security setting can be established, avoiding unwanted interactions with sensitive data and preventing data loss. The problem of defining a unified representation of heterogeneous data sources for cooperative tasks has been intensified by the introduction of big data. Prior to the emergence of big data, researchers have been focusing on knowledge discovery for structured data, attempting to unify representation among structured databases. For instance, Castano and De Antonellis [121] have studied the problem of data integration for the structured data source. The types of semantic heterogeneity for structure data studied in this article include name and structural heterogeneity, which can be further subdivided into type conflict, key conflicts, and domain conflicts.

Besides the heterogeneity mentioned above in structured data, Wang [122] has studied the heterogeneity in big data, which is likely to be a major characteristic for smart city applications. The heterogeneity in big data includes syntactic heterogeneity, conceptual heterogeneity, terminological heterogeneity, and pragmatic heterogeneity. Although advanced processing and analysis techniques can achieve data integration between structured and machine data to a reasonable extent, providing a high-level data fusion between unstructured analog sensor data will remain a challenging task. However, due to the complexity of such tasks, it is tough to achieve a context-independent approach to present a unified representation of the heterogeneous data. As a result, appropriately handling heterogeneous data types may be a significant security challenge for smart city system designers.

5) Data Sensitivity: Different data types have different sensitivity levels, and even the input data in an application can have different levels of sensitivity. Pulse data, mobility tracker data, and a live video of the patient may all be fed into an in-home health monitoring system simultaneously. From a privacy-preserving perspective, the patient’s live video data deserves the most stringent security mechanism it could provide. From a healthcare product perspective, pulse data should remain top-secret to meet customers’ expectations on the security of their health data. After defining the sensitivity of input data, how different data types should be protected comes the question. While we are familiar with how structured data could be stored and protected, the balance between protection for unstructured data and the ease in extracting knowledge from it for integrated information queries remains difficult. Thus, designing system security architecture with data of different sensitivity will be a challenging task.

B. Network-Centric Security Challenges

Secure communication is the foundation of a secure system. It safeguards the confidentiality, integrity, and availability of...
TABLE V DIFFERENT NETWORK TOPOLOGY

| Topology | Explanation |
|----------|-------------|
| Star     | Nodes are in the radio range of the central node and communicate directly with the central node. All network traffic in this network will pass through the central node. This is the most simple topology and works best for typical master-and-slave relationships between devices. |
| Tree     | Each node is within the radio range of its parent branch and children branch. In this topology, network communication can be multi-hopped, with nodes relying on their neighbors to relay messages to nodes outside of their radio range. |
| Mesh     | Each node can establish a wireless communication link with one or more neighbors, allowing for more traffic routing options in the network communication. However, as the number of possible routing paths grows, the complexity of the routing decision increases as well. |
| Cellular | Each node communicates directly with the cluster head of their cell. These cluster heads are placed so that they can offer sufficient coverage for all nodes while avoiding radio range overlaps with other cluster heads. For inter-cluster communication, these cluster heads communicate with other cluster heads directly. |

information exchanged in the network. Common attacks on wireless communications channels include blackhole, wormhole, and pharming attacks that disrupt the delivery of data; Jamming channel, DDoS, and Syn Flooding attacks that disable the availability of services; eavesdropping and traffic analysis that leaks confidential data to unauthorized third parties. Thus, prevention and detection of attacks on wireless communication channels are critical for all systems relying on wireless networks to perform data transmission to provide reliable and timely service delivery. In addition, the survey in [123] and [124] has presented a few communication security challenges prevalent in IoT systems that deserve more attention. For example, the size of cryptographic keys and certificates for trust management must be kept short due to resource constraints in IoT devices, and the performance overhead for secure storage or code attestation must be within reasonable parameters to extend the battery life of devices that are not powered directly. Furthermore, while the standardization of network protocols is extremely challenging due to different performance requirements between different system components, secure and efficient routing is vital to the overall security of the system. If more than one routing protocol is adopted throughout the system, the compatibility between protocols should also be investigated.

1) Wireless Communication Protocols: A set of devices communicating with neighbors within its radio range can form a network, which can be arranged in different topologies. Simple network topology can achieve low latency in relaying messages, while complex network topology can offer better routing decisions and flexibility [123]. There are four main network topologies that are commonly implemented and are shown in Table V.

Communication protocols are rules that define how data is exchanged within the network. Many wireless IoT communication protocols have been developed for various uses due to the various device capabilities and requirements. Table III provides a description of the security features of the most commonly used wireless communication protocols for smart city applications, as well as their corresponding security challenges. While there is no standardization for the protocols, data formats, and systems adopted by vendors, it is common to see smart devices of different types and brands being deployed in the same system. Hence, interoperability between devices becomes a major challenge in providing secure communication between heterogeneous devices.

2) Security Protocols: Various standard security protocols and solutions have been developed to ensure communication security, such as DTLS, CETIC-6LBR (6LoWPAN border router), IPsec, IKEv2, and host identity protocol (HIP). Burg et al. [123] presented a summary of wireless communication principles about the connectivity requirements of IoT. Communication standards and the gap between their security features and actual IoT system vulnerabilities are also highlighted.

For example, traditional security protocols are built on OSI stacks, which may or may not be fully implemented in many IoT systems. Traditional security mechanisms are often employed in the medium access control (MAC) or higher layers, assuming that the underlying physical link and data link layers will provide a reliable system link. However, the physical-layer security follows the information-theoretic principle. The strength of the security mechanism depends on the assumption of varied channel conditions between the user and attacker. As a result, security guarantees are rarely 100%. Furthermore, the system architecture of many IoT systems differs significantly from the traditional system architecture, where they introduce their layers, such as perception and actuation layers. These new layers often require new adaptations of current security protocols to ensure system security. Hence, it is wise to investigate the security requirements for every layer of the system and their context to evaluate the choice of security protocols used for system security.

3) Distributed Communication: The majority of current wireless IoT communication solutions use a centralized approach, in which a central authority or server manages data sharing between devices. As the number of devices in the network grows, communication to and from the center server will quickly become a bottleneck, resulting in substantial network latency. While others argue that edge servers should be used to offload centralized computing activities, a decentralization approach can best deal with the issue of scalability. One of the ways to establish a decentralized IoT network is via P2P networking technologies. Like any other widely adopted technology, when the P2P technology is commonly deployed, we expect many adversarial attacks.

Okada et al. [125] highlighted that besides adversarial attacks, there are other challenges in the architecture of a P2P network. One such issue is the selfish behavior of users. While many P2P applications are designed to serve a large number of users over a network, a “hotspot” issue may nevertheless arise, in which some nodes with popular content must service more peers than others. Some selfish users might want to reserve more resources for themselves, such as disk space, bandwidth, and power, by altering their system configurations to act in their interest. Although these users are not explicit attackers, their action degrades the overall system performance if no
checks and balance are in place. Another significant challenge in a peer-to-peer network is the concept of trust. Since there is no root of trust, the system must devise a way to assess the trustworthiness of external data transfers and respond appropriately to defend itself. Thus, providing a secure approach for distribution communication is a challenging task.

C. Things-Centric Security Challenges

Due to the growing connectivity between systems and applications’ dependence on big data, many smart city applications will be directly or indirectly dependent on a large scale of IoT devices for data collection. Unfortunately, while these IoT devices are important data sources that support system operations, many of them have limited resources and capacity to implement comprehensive security measures, leaving them vulnerable to attack. More malicious attempts by attackers probing for the weakest link in the system are likely to occur due to the large-scale physical deployment, which increases the attack surface for attackers to interfere with the systems.

At the same time, due to the massive deployment scale, a successful intrusion into these end devices might cause a tidal effect, compromising the security of the system and even paralyzing it. Consequently, the effect of intrusion will be very significant and impacts many devices. In addition, dealing with the aftermath of an attack can be equally concerning. Traditionally, technicians could upgrade the sensor network on-site, either to install patches for updates or to address a loophole in these devices. Such a management approach is no longer feasible, especially for mass upgrades, due to a large number of devices deployed. Furthermore, many of these devices may be physically inaccessible to technicians or almost impossible to access. Hence, we shall direct our interest toward remote updating mechanisms, performing updates, and integrity attestation over the air. However, due to the wireless nature of such mechanisms, security concerns have become growingly prominent. Thus, smart city systems that have a large-scale physical deployment of devices in open environments will therefore contribute to a proliferation of security challenges, such as ensuring secure mass updates and performing large-scale system recovery.

D. Potential Solutions or Directions

With the above discussion, we can foresee some of the emerging security challenges that are important to be addressed in smart city applications. Fortunately, promising solutions or research directions have been proposed to mitigate some of these potential fallbacks. For example, [126] comprehensively studied security issues in IoT-based cloud computing and concluded that deep learning-based security solutions can be effective in attack prevention and detection in the cloud. Similarly, machine learning has been a growing trend for implementing security monitoring systems.

To address the data security for dynamic and sensitive data flow, the authors in [127] proposed an adaptive neuro-fuzzy inference system for storing medical IoT data in the cloud securely to assess the level of security protection for the flow of medical data. Similarly, Zulkifl et al. [128] have applied fuzzy logic and blockchain technology to achieve adaptive security for healthcare IoTs without a centralized management agent. In both cases, privacy and security are top concerns to protect sensitive medical data. Also, differentiated security and context-aware security solutions are emerging topics that researchers may consider. The notion of QoSS can be an ample design consideration that drives the direction of security solutions. Given the diversity of the IoT ecosystem, different types of infotainment data can have different security and efficiency requirements. Systems can be more efficient by reducing the complexity of the security framework and ensuring that important communications are adequately protected by tailoring security protections according to the type and nature of data exchanged [129].

VI. Future IoT and Future IoT Security

As our vision of a smart city becomes a reality, it is essential that our security techniques grow in tandem with the changing landscape. Future IoT in smart cities is expected to be fully intelligent, with seamless cross-functional and cross-platform interactions. An important characteristic of the data communication in future smart city application is wireless. While a small portion of current applications can maintain their usability using wired data communication, that is not feasible for city-wide deployment of intelligent systems. Furthermore, wireless communication protocols can promote effective communication between various systems, where each wireless component of the systems might possibly operate as a point of interaction between systems.

As IoT progresses from “perceptive” to “cognitive,” we expect these devices to learn from our actions and help pave the way for deeper integration of people, things, and infrastructure. Cognitive IoT devices can sense their surrounding environment, gathering information about other participants nearby. The intelligence agent is fed with relevant data from users and the environment and a corresponding set of execution options and system/environmental feedback from the execution. The more information the cognitive IoT device can collect, the better it could formulate its decision path. By iteratively updating the best strategy under user-defined policies to achieve the best reward, the agent gains the ability to make intelligent decisions. Since the core model’s cognitive ability is based on the collection of behavioral insights from our actions and feedback, which serve as the model’s knowledge base, the quality of data can heavily impact the model’s performance.

As IoT applications become more intelligent, new security vulnerabilities emerge. To begin with, such a model’s training necessitates a large database, and the model could allow for online training, where new samples generated in real time can be processed and fed into the model for training. The high volume and ever-expanding data set put enormous strain on the system’s ability to store and analyze data securely. Sharing and analyzing of cyber threat intelligence files between different security organizations in smart cities to maintain awareness of emerging vulnerabilities is also necessary [130]. In addition, since more cross-functional interactions are anticipated, we can expect more frequent and
massive data flows between systems, exposing more attack surfaces to external attackers. Future IoT security would require extensive protection toward sensitive data flow among system components and across systems. Furthermore, as the number of IoT devices grows exponentially, more systems will be encountering large traffic flow from these devices due to the increasing connectivity between systems. The large growth in IoT devices further exacerbates the demand for wireless bandwidth. To achieve better efficiency with large data traffic, a popular approach is the adoption of cognitive radio, which provides appealing strategies, such as spectrum sensing, self-learning, circumstantial perceiving, and spectrum access. However, they can also add to security and privacy risks [131].

VII. CONCLUSION

In this article, we have introduced a new perspective on security issues in smart cities from a data-centric viewpoint by referring to ANT-centric architecture. We studied the concept of a smart city holistically, starting with end applications to abstract shared characteristics and highlighted some privacy and security challenges these smart city applications will face. Following that, we evaluated the specific context of each smart city domain and the context-specific security requirements. By doing so, we want to provide directions for smart city system designers on when, where, and how they should implement security strategies and the possible security challenges they need to consider. Furthermore, we investigated the challenges and gaps that current cryptographic solutions have to overcome. Finally, we give our view of the future IoT and IoT security.

Overall, while emerging technologies have enormous potential for addressing difficulties in IoT-enabled smart cities, security must be considered throughout the data life cycle and any possible interactions with the outside world. Only then will the system withstand attacks on every component of the large network. Aside from the usual security considerations, proposals for IoT-enabled smart city applications must carefully evaluate the application’s context and social expectations to ensure its feasibility. Other security issues, such as secure updates for massive IoT networks, interoperability between different protocols, and maintenance of QoSs deserve more research attention. As our IoT systems gradually evolve from “perceptive” toward “cognitive,” autonomous or semi-autonomous complex systems capable of cognitive decision making will become commonplace. How best to implement security in such a sophisticated and intelligent system will be of great value toward the development of our smart city landscape.

ACKNOWLEDGMENT

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of National Research Foundation, Singapore.

REFERENCES

[1] S. McLeod, “Maslow’s hierarchy of needs,” Simply Psychol., vol. 1, pp. 1–18, Mar. 2007.
[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.
[3] L. S. Vaishlery, “Global IoT and Non-IoT Connections 2010–2025,” Mar. 2021. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/
[4] A. A. Tole et al., “Big data challenges,” Database Syst. J., vol. 4, no. 3, pp. 31–40, 2013.
[5] M. Wazid, A. K. Das, V. Oddeh, N. Kumar, and W. Susilo, “Secure remote user authenticated key establishment protocol for smart home environment,” IEEE Trans. Depend. Secure Comput., vol. 17, no. 2, pp. 391–406, Mar./Apr. 2020.
[6] K. Y. Lam, Securing the Internet of Thing: Cybersecurity from IT to OT, Chapter in Navigating the Digital Age, 35–44, Forbes Media, Jersey City, NJ, USA, 2016.
[7] H. HaddadiPajouh, A. Dehghantanhava, R. M. Parizi, M. Aledhari, and H. Karimipour, “A survey on Internet of Things security: Requirements, challenges, and solutions,” Internet Things, vol. 14, Jun. 2021, Art. no. 100129.
[8] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, “Security requirements for the Internet of Things: A systematic approach,” Sensors, vol. 20, no. 20, p. 5897, 2020.
[9] K.-Y. Lam, S. Mitra, F. Gonderman, and X. Yi, “ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities,” IEEE Internet Things J., vol. 9, no. 8, pp. 5895–5908, Apr. 2022.
[10] M. Binti, M. Noor, and W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” Comput. Netw., vol. 148, pp. 283–294, Jan. 2019.
[11] N. Neschenko, E. Bou-Harh, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations,” IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.
[12] P. R. A. Jurcut, T. Niculcea, and N.-A. Le-Khac, “Security considerations for Internet of Things: A survey,” SN Comput. Sci., vol. 1, p. 193, Jun. 2020.
[13] F. Al-Turjman, H. Zahnmatkesh, and R. Shahrroze, “An overview of security and privacy in smart cities’ IoT communications,” Trans. Emerg. Telecommun. Technol., vol. 33, no. 3, 2022, Art. no. e3677.
[14] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved,” IEEE Internet Things J., vol. 6, no. 2, pp. 1606–1616, Apr. 2019.
[15] J. Hou, L. Qu, and W. Shi, “A survey on Internet of Things security from data perspectives,” Comput. Netw., vol. 148, pp. 295–306, Jan. 2019.
[16] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, “Security and privacy in smart cities: Challenges and opportunities,” IEEE Access, vol. 6, pp. 46134–46145, 2018.
[17] M. Sookhak, H. Tang, Y. He, and F. R. Yu, “Security and privacy in smart cities’ IoT communications,” Telecommun. Technol., vol. 33, no. 3, 2022, Art. no. e3677.
[18] A. B. Haque, B. Bhushan, and G. Dhiman, “Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends,” Exp. Syst., vol. 39, no. 5, 2022, Art. no. e12753.
[19] R. Sánchez-Corcua et al., “Smart cities survey: Technologies, application domains and challenges for the cities of the future,” Int. J. Distr. Sensor Netw., vol. 15, no. 6, pp. 1–19, 2019.
[20] N. Y. Philip, J. J. P. C. Rodrigues, H. Wang, S. J. Fong, and J. Chen, “Internet of Things for in-home health monitoring systems: Current advances, challenges and future directions,” IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 300–310, Feb. 2021.
[21] A. Awasthi and K. Srivastava, “A biometric authentication scheme for telecare medicine information systems with nonce,” J. Med. Syst., vol. 37, no. 5, pp. 1–4, 2013.
[22] Z. Tan, “A user anonymity preserving three-factor authentication scheme for telecare medicine information systems,” J. Med. Syst., vol. 38, no. 3, pp. 1–9, 2014.
[23] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, and M. K. Khan, “Cryptanalysis and improvement of Yan et al.’s biometric-based authentication scheme for telecare medicine information systems,” J. Med. Syst., vol. 38, no. 6, pp. 1–12, 2014.
[24] X. Yan, W. Li, P. Li, J. Wang, X. Hao, and P. Gong, “A secure biometrics-based authentication scheme for telecare medicine information systems,” J. Med. Syst., vol. 37, no. 5, pp. 1–6, 2013.

[25] R. Amin and G. Biswas, “A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity,” J. Med. Syst., vol. 39, no. 8, pp. 1–19, 2015.

[26] L. Zhang, S. Zhu, and S. Tang, “Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme,” IEEE J. Biomed. Health Informat., vol. 21, no. 2, pp. 465–475, Mar. 2017.

[27] B. D. Deebak and F. Al-Turjman, “Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of Medical Things,” IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 361–369, Apr. 2021.

[28] P. Kumar and H.-J. Lee, “Security issues in healthcare applications using wireless medical sensor networks: A survey,” Sensors, vol. 12, no. 1, pp. 55–91, 2012.

[29] T. Alladi, V. Chamola, and Naren, “HARCI: A two-way authentication protocol for three entity healthcare IoT networks,” IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 361–369, Feb. 2021.

[30] W. Yuanbing, L. Wanrong, and L. Bin, “An improved authentication and attestation scheme for in-transit vehicles in IoV scenario,” IEEE Access, vol. 9, pp. 105101–105117, 2021.

[31] D. Lu, R. Han, Y. Shen, X. Dong, J. Ma, X. Du, and M. Guizani, “TSEh: A trusted platform module sharing scheme towards smart IoT-Health devices,” IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 370–383, Feb. 2021.

[32] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and H. Hossain, “A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes,” IEEE Access, vol. 8, pp. 118433–118471, 2020.

[33] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and H. Hossain, “A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes,” IEEE Access, vol. 8, pp. 118433–118471, 2020.

[34] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and H. Hossain, “A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes,” IEEE Access, vol. 8, pp. 118433–118471, 2020.

[35] K. Keshamoni and S. Hemanth, “Smart gas level monitoring, booking and gas availability verification for smart grid environment,” IEEE J. Biomed. Health Inf., vol. 19, no. 22, p. 4862, 2019.

[36] Y. Kabalci, E. Kabalci, S. Padmanaban, J. B. Holm-Nielsen, and T. K. Rosing, “Secure and lightweight authentication scheme for smart grid,” IEEE Trans. Ind. Informat., vol. 17, no. 7, pp. 4962–4969, Jul. 2021.

[37] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, “Secure and lightweight authentication scheme for smart metering infrastructure in smart grid,” IEEE Trans. Ind. Informat., vol. 16, no. 5, pp. 3548–3557, May 2020.

[38] N. H. Mollah, M. Mohammadrezaee, J. Hunt, and B. Zakeri, “Internet of Things (IoT) and the energy sector,” Energies, vol. 13, no. 2, p. 494, 2020.

[39] Y. Kabalci, E. Kabalci, S. Padmanaban, J. B. Holm-Nielsen, and F. Blaabjerg, “Internet of Things applications as energy Internet in smart grids and smart environments,” Electronics, vol. 8, no. 9, p. 972, 2019.

[40] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, “Blockchain in smart grids: A review on different use cases,” Sensors, vol. 19, no. 22, pp. 4862, 2019.

[41] M. B. Mollah et al., “Blockchain for future smart grid: A comprehensive survey,” IEEE Internet Things J., vol. 8, no. 1, pp. 18–43, Jan. 2021.

[42] V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani, “A distributed framework for energy trading between uav and charging stations for critical applications,” IEEE Trans. Veh. Technol., vol. 69, no. 5, pp. 5391–5402, May 2020.

[43] N. Cheng, W. Xu, W. Shi, Y. Zhou, N. Lu, H. Zhou, and X. Shen, “Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities,” IEEE Commun. Mag., vol. 56, no. 8, pp. 26–32, Aug. 2018.

[44] J. Liu, Y. Shi, Z. M. Faddlallah, and N. Kato, “Space-air-ground integrated network: A survey,” IEEE Commun. Survys Tuts., vol. 20, no. 4, pp. 2714–2741, 4th Quart., 2018.

[45] G. Kumar et al., “A privacy-preserving secure framework for electric vehicles in iot using matching market and signcryption,” IEEE Trans. Veh. Technol., vol. 69, no. 7, pp. 7707–7722, Jul. 2020.

[46] R. Gottumukkala, R. Merchant, A. Tanzin, K. Leon, A. Roche, and P. Darby, “Cyber-physical system security of vehicle charging stations,” in Proc. IEEE Green Technol. Conf. (GreenTech), 2019, pp. 1–5.

[47] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, “A detailed security assessment of the EV charging ecosystem,” IEEE Mater. Soc., vol. 34, no. 3, pp. 200–207, May/Jun. 2020.

[48] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, “A lightweight authentication and attestation scheme for in-transit vehicles in IoV scenario,” IEEE Trans. Veh. Technol., vol. 69, no. 12, pp. 14188–14197, Dec. 2020.

[49] J. Li, Y. Li, C. Cao, and K.-Y. Lam, “Conditional anonymous authentication with abuse-resistant tracing and distributed trust for Internet of Vehicles,” IEEE Internet Things J., vol. 9, no. 11, pp. 8749–8762, Jun. 2022.

[50] M. Passafiume, M. Lucarelli, G. Collodi, and A. Cidronali, “A road-side unit architecture suitable for concurrent multi-lane vehicular communications,” in Proc. IEEE MIT-S Int. Conf. Micro. Intell. Mobility (ICMIM), 2020, pp. 1–4.

[51] Y. Liang, N. Ma, X. Li, and J. Hu, “Stochastic road side unit location optimization for information propagation in the Internet of Vehicles,” IEEE Internet Things J., vol. 8, no. 17, pp. 13316–13327, Sep. 2021.

[52] W.-H. Lee and C.-Y. Chiu, “Design and implementation of a smart traffic signal control system for smart city applications,” Sensors, vol. 20, no. 2, p. 508, 2020.

[53] K. Ragavan, K. Venkatalakshmi, and V. Kandasamy, “Traffic video-based intelligent traffic control system for smart cities using modified ant colony optimizer,” Comput. Intell., vol. 37, pp. 1–21, Nov. 2020.

[54] N. A. Khan, N. Janhjali, S. N. Brohi, R. S. A. Usmani, and A. Nayyar, “Smart traffic monitoring system using unmanned aerial vehicles (UAV’s),” Comput. Commun., vol. 157, pp. 434–443, May 2020.

[55] F. Samie, L. Bauer, and J. Henkel, “Edge computing for smart grid: An overview on architectures and solutions,” in IoT Smart Grids, Cham, Switzerland: Springer, 2019, pp. 21–42.

[56] U. Zafar, S. Bayhan, and A. Sanfilippo, “Home energy management system concepts, configurations, and technologies for the smart grid,” IEEE Access, vol. 8, pp. 119271–119286, 2020.

[57] M. Wiazid, A. K. Das, V. Odeku, N. Kumar, and W. Susilo, “Secure remote user authenticated key establishment protocol for smart home environment,” IEEE Trans. Depend. Secure Comput., vol. 17, no. 2, pp. 391–406, Mar/Apr. 2020.

[58] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. R. Choo, “HomChain: A blockchain-based secure mutual authentication scheme for smart homes,” IEEE Internet Things J., vol. 7, no. 2, pp. 818–829, Feb. 2020.
Jiani Fan received the bachelor’s degree in information systems from Singapore Management University, Singapore, in 2020. She is currently pursuing the Ph.D. degree in computer science with Nanyang Technological University, Singapore.

Her research interests include IoT Security, cybersecurity, and Internet of Vehicles.

Wenzhuo Yang received the bachelor’s degree in measuring and controlling technologies and instruments from Beijing University of Posts and Telecommunications, Beijing, China, in 2016, and the Ph.D. degree from the School of Computer Science and Engineering, Nanyang Technological University, Singapore, in 2022.

She is currently a Research Fellow with the Strategic Centre for Research in Privacy-Preserving Technologies and Systems, Nanyang Technological University. Her research interests include privacy-preserving machine learning, IoT security, and intrusion detection.

Ziyao Liu received the B.E. degree from the School of Electronics Information Engineering, Zhengzhou University, Zhengzhou, China, in 2015, and the M.S. degree from Beijing Institute of Technology, Beijing, China, in 2018. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, Nanyang Technological University, Singapore.

His research interests include privacy-preserving machine learning, multi-party computation, and applied cryptography.

Jiwen Kang received the Ph.D. degree from Guangdong University of Technology, Guangzhou, China, in 2018.

He was a Postdoctoral Fellow with Nanyang Technological University, Singapore, from 2018 to 2021. He is currently a Professor with Guangdong University of Technology. His research interests mainly focus on blockchain, security, and privacy protection in wireless communications and networking.

Dusit Niyato (Fellow, IEEE) received the B.Eng. degree from the King Mongkut’s Institute of Technology Ladkrabang, Bangkok, Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Winnipeg, MB, Canada, in 2008.

He is currently a Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests are in the areas of the Internet of Things, machine learning, and incentive mechanism design.

Kwok-Yan Lam (Senior Member, IEEE) received the B.Sc. degree (First Class Hons.) from the University of London, London, U.K., in 1987, and the Ph.D. degree from the University of Cambridge, Cambridge, U.K., in 1990.

He is the Associate Vice President (Strategy and Partnerships) and the Professor with the School of Computer Science and Engineering, Nanyang Technological University (NTU), Singapore. He is currently also the Director of the Strategic Centre for Research in Privacy-Preserving Technologies and Systems. Since August 2020, he is on part-time secondment to the INTERPOL as a Consultant of Cyber and New Technology Innovation. Prior to joining NTU, he was a Professor with Tsinghua University, Beijing, China, from 2002 to 2010, and a Faculty Member of the National University of Singapore, Singapore, and the University of London since 1990. He was a Visiting Scientist with the Isaac Newton Institute, Cambridge University, and a Visiting Professor with the European Institute for Systems Security. His research interests include distributed systems, intelligent systems, IoT security, distributed protocols for blockchain, homeland security, and cybersecurity.

Dr. Lam received the Singapore Foundation Award from the Japanese Chamber of Commerce and Industry in recognition of his research and development achievement in information security in Singapore, in 1998.