Toward a Privacy-Preserving and Secure Smart City: Recent Advances in User-Centric Applications

Mohammad Rasool Momeni, *Graduate Student Member, IEEE*, Abdollah Jabbari, *Member, IEEE*, Carol Fung, *Member, IEEE*, and Raouf Boutaba, *Fellow, IEEE*

***Abstract*—The ever-increasing global population has caused rapid urbanization in recent decades. Many cities around the world are trying to leverage information and communication technologies to resolve the resulting problems, such as traffic congestion and high-energy consumption. This trend is part of the movement toward the development of the so-called smart cities that provide efficient, comfortable, and happy lives to their residents. In this respect, smart cities are indeed promising but have significant underlying complexity due to the number of variety of domains involved, including living, economy, mobility, governance, etc. However, in recent years, numerous cyber attacks and privacy leaks have been major obstacles to the widespread adoption and deployment of smart city applications. In general, smart city domains can be classified into user-centric applications and nonuser-centric applications, such as critical infrastructures. This article examines the key security and privacy challenges associated with recently trending user-centric smart city applications. First, we study the leading technologies along with superior security methods and privacy enhancing technologie in smart cities. We also provide a critical survey of the security and privacy of novel user-centric smart city applications, namely, smart parking, smart charging, and smart home. Our survey provides a detailed review of recent, relevant, and state-of-the-art research works to assist readers in gaining a comprehensive understanding of security and privacy challenges associated with smart cities. Finally, it outlines some research directions worth investigating in the future. The ultimate goal of this survey is to shed light on the pressing security and privacy challenges in smart cities and to provide insights for the development of secure and privacy-preserving smart cities.**

***Index Terms*—Internet of Things (IoT), privacy, security, smart city, survey, user-centric applications.**

I. Introduction

NOWADAYS, 55% of the global population resides in urban regions, and this figure is projected to rise to 68% by 2050 [1]. Forecasts indicate that urbanization could result in an additional 2.5 billion people living in urban areas by 2050 [1]. Rapid urbanization is placing increasing pressure on our climate, environment, and energy resources [2]. Governments attempt to utilize information and communication technologies to manage crowded cities through the creation of smart cities. A smart city is a modern city that connects physical, social, and information technology infrastructures by establishing an intelligent system to improve the performance of existing operations and services [2]. Their purpose is to provide enhanced living conditions and welfare for its inhabitants by leveraging advances in information and communication technologies, with a particular emphasis on the Internet of Things (IoT).

The quality of services in a smart city environment considerably depends on the amount and quality of data collected. The collected data is subsequently processed, analyzed, shared, and stored for various technical, commercial, and societal purposes. The collected data often include personal information, such as identity, visited locations, travel time and duration, and purchased items. They can reveal sensitive private information regarding citizens, such as income level, health status, political interests and affiliations, and lifestyle [3]. In recent years, cyber attacks have also leaked citizens' personal data, such as the leakages of Facebook, Equifax, and Uber users' data [4]. Moreover, they have made important services unavailable at critical times, such as the shutdown of Ireland's national healthcare IT systems in 2021 [5].

Numerous survey papers have explored various aspects of smart cities over the past decade [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18]. To the best of our knowledge, none of them have focused on recently trending user-centric applications in smart cities. There is a lack of thorough surveys that examine the pressing security and privacy challenges associated with novel user-centric smart city applications. We are aware that the literature already contains numerous studies emphasizing the security of critical infrastructures, such as smart grids and smart healthcare systems [19], [20], [21]. However, the security of critical infrastructures in smart cities falls beyond the scope of this survey. This article presents a comprehensive and up-to-date investigation of security and privacy issues in smart parking, smart charging, and smart home domains—applications that have recently attracted a lot of attention. We focus on applications that citizens frequently engage with in their daily lives.

The contributions of this survey can be summarized as follows.

1) We investigate the concept of the smart city, its leading technologies, and renowned security methods and

Received 3 August 2025; accepted 31 August 2025. Date of publication 8 September 2025; date of current version 7 November 2025. This work was supported by the Gina Cody Foundation. *(Corresponding author: Mohammad Rasool Momeni.)*

Mohammad Rasool Momeni, Abdollah Jabbari, and Carol Fung are with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1M8, Canada (e-mail: mohammadrasool.momeni@mail.concordia.ca; abdollah.jabbari@concordia.ca; carol.fung@concordia.ca).

Raouf Boutaba is with the David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: rboutaba@uwaterloo.ca).

Digital Object Identifier 10.1109/JIOT.2025.3607211

TABLE I
LIST OF KEY ACRONYMS

Acronyms	Definitions
ABE	Attribute-Based Encryption
AC	Alternating Current
ACr	Anonymous Credentials
AES	Advanced Encryption Standard
AR	Augmented Reality
BBS GS	Boneh, Boyen, and Shacham Group Signature
BP	Bilinear Pairing
CAGR	Compound Annual Growth Rate
DC	Direct Current
DDoS	Distributed Denial of Service
DP	Differential Privacy
DTN	Delay/Disruption Tolerant Networking
ECC	Elliptic Curve Cryptography
EV	Electric Vehicle
FIPS	Federal Information Processing Standard
FL	Federated Learning
HE	Homomorphic Encryption
HECC	Hyper Elliptic Curve Cryptography
HMAC	Hash-based Message Authentication code
IDS/IPS	Intrusion Detection/Prevention System
IoDT	Internet of Digital Twins
IMD	International Institute for Management Development
KNN	K-Nearest Neighbors
LoRaWAN	Long Range Wide Area Network
LSTM	Long Short-Term Memory
MIMO	Multiple-Input and Multiple-Output
MQTT	Message Queuing Telemetry Transport
NDN	Named Data Networking
NIST	National Institute of Standards and Technology
NoD	NDN-over-DTN
NTRU	N-th degree Truncated polynomial Ring Units
O2O	Online-to-Offline
OAM	Orbital Angular Momentum
OCPP	Open Charge Point Protocol
PIR	Private Information Retrieval
PSI	Private Set Intersection
PUF	Physical Unclonable Function
SDN	Software-Defined Networking
SRS	Short Randomizable Signature
TA	Trusted Authority
V	Volt
VR	Virtual Reality
XR	Extended Reality
ZKP	Zero-Knowledge Proof

privacy enhancing technologies (PETs). We also examine the major security and privacy challenges of each leading technology.

2) We perform an in-depth analysis of novel user-centric categories of the smart city, namely, smart parking, smart charging, and smart home. First, we present an overview of each smart city application. Afterward, a specific classification based on the properties of those smart city applications is provided. Ultimately, we analyze security and privacy issues for the smart city applications mentioned.
3) We propose two taxonomies for each smart city application, based on their inherent properties and known security and privacy protection mechanisms.
4) We present a comprehensive section on future research directions aimed at introducing promising methods to shed light on this path toward resolving existing challenges. It can assist policymakers, scholars, and practitioners in conducting research in these domains.

The remainder of this article is organized as follows. Section II presents a review of relevant survey papers, along with their strengths and weaknesses. Section III is dedicated to the concept of leading technologies, as well as popular security and privacy methods in smart cities. In Section IV, we provide a comprehensive study of security and privacy concerns in new user-centric smart city applications, namely, smart parking, smart charging, and smart home. Section V briefly highlights prosperous case studies and leading practical deployments. Section VI explains the insights and lessons learned from the literature. Section VII provides a discussion highlighting the contributions as well as the limitations of our survey. Section VIII outlines some open challenges and potential research directions. Finally, Section IX concludes this article. Table I presents a list of key acronyms used in this article and their corresponding definitions, arranged alphabetically.

II. RELATED WORK

Here, we present a detailed review of recent and relevant survey papers. We also summarize these works in Table II to provide a clear and concise comparison, highlighting their contributions and limitations.

In [6], Gharaibeh et al. primarily selected a data-driven perspective about the concept of the smart city. They examined the smart city from the perspective of the data life cycle. Indeed, data security and privacy are only a small portion of this review study. In [7], Eckhoff and Wagner mainly focused on privacy and provided taxonomies for threats, challenges, and solutions in the smart city. Although privacy and security are two accompanying phenomena, this survey lacks an investigation of security issues. In another study, Braun et al. defined five main research problems and holistically reviewed the literature according to the designated problems [8]. This survey cannot provide deep understanding of the smart city and corresponding security and privacy challenges.

Cui et al. classified security issues, requirements, and technologies in the context of smart cities [9]. Subsequently, they investigated the literature in each category. Nonetheless, their study does not take into account different applications of the smart city. It is important to study several smart city applications because each application has its own characteristics, requirements, threats, and countermeasures. This gives a deeper and more accurate understanding of smart cities.

Curzon et al. performed a comprehensive survey of PETs in the area of the smart city [10]. Although this is a thorough review regarding privacy issues in the smart city, it does not consider security problems and attacks. Shookhak et al. presented a survey study to investigate security and privacy issues in smart cities [11]. In this study [11], they reviewed the literature based on the IoT and cloud technologies. Nevertheless, similar to Curzon et al.'s study, they did not examine security and privacy issues with respect to some applications of the smart city.

In [12], Andrade et al. performed a systematic literature review considering IoT security issues in the context of the smart city. They also proposed a risk level-based model

TABLE II
SUMMARY OF COMPARING OUR PAPER WITH THE STATE-OF-THE-ART RELATED REVIEW PAPERS

Ref.	Year	Contributions	Limitations
[6]	2017	A thorough review of data management techniques in the smart city considering data life cycle, which includes collection, processing, and dissemination. Networking and computing technologies are also presented.	Limited exploration of security and privacy issues and corresponding solutions, along with a lack of investigating leading technologies.
[7]	2018	A comprehensive study regarding privacy issues in the smart city including strategies, techniques, and building blocks. There is also an accurate taxonomy about different types of privacy, privacy protection methods, and privacy-enhancing technologies.	Failed to cover security approach, comprising security requirements, relevant attacks, and potential countermeasures
[8]	2018	A short survey on five different challenges of the smart city consists of data privacy, network security, trustworthy data sharing, the role of AI, and the reduction of cascading failures.	Lacks an in-depth and detailed review of existing security and privacy challenges together with effective measures
[9]	2018	A review of the security and privacy issues in the context of the smart city, along with security requirements such as confidentiality and integrity. Current security and privacy-enhancing mechanisms are also classified and studied.	Failed to include smart city applications and their related challenges, advances, and solutions
[10]	2019	A thorough study on the smart city and its implemented examples with respect to privacy-related issues, including potential privacy breaches and existing protection technologies.	Lacks coverage of security vulnerabilities, attacks, and countermeasures
[11]	2019	A comprehensive review of security and privacy in the smart city with an emphasis on a classification of security challenges based on IoT and cloud. Privacy challenges, along with detailed security requirements, are explained, and a taxonomy of solutions is also proposed.	Overlooked some leading technologies, such as AI and blockchain, as well as smart city applications
[12]	2020	A systematic literature review with an emphasis on IoT cybersecurity issues based on a top-down approach in the realm of the smart city. A cybersecurity maturity model based on risk levels is also presented and validated.	Failed to investigate other enabling technologies, such as cloud computing, blockchain, and AI, along with their vulnerabilities and mitigation techniques
[13]	2021	An overview of the smart city with a focus on the smart grid, smart building, smart transportation, and smart healthcare areas with respect to cybersecurity and deep learning.	Limited review of security and privacy issues in smart city applications and lacks coverage of enabling technologies, their challenges, and potential solutions
[14]	2022	A systematic study of the security and privacy requirements, challenges, technologies, and solutions for designing a smart and resilient city, along with open research problems and issues.	Lacks a comprehensive exploration of modern smart city applications together with existing security and privacy problems and corresponding measures
[15]	2023	A thorough survey on the security of the smart city from the activity-network-things (ANT) perspective, which consists of smart utility, smart transportation, smart homes, and smart healthcare applications.	Failed to comprise other leading technologies and modern smart city applications, along with their privacy challenges and mitigation techniques
[16]	2023	A comprehensive review of crowdsensing, its applications, and privacy protection mechanisms in the realm of the digital city, along with quantitatively analyzing the current protection technologies for crowdsensing.	Failed to integrate security perspective, including vulnerabilities, attacks, and solutions
[17]	2024	A short survey on the smart city with an emphasis on the role of the IoT, considering its concept, components, and characteristics, along with promising technologies for future smart cities.	Limited investigation of security and privacy challenges and relevant solutions, as well as a lack of study of other leading technologies.
[18]	2025	A thorough review of smart systems that considers smart cities as a specific application, with an emphasis on control, perception, knowledge, communication, and security as the primary components of smart systems.	Lacks providing new insights for readers, particularly regarding recent security and privacy challenges and potential solutions to develop secure smart systems.

to analyze the IoT cybersecurity maturity in a smart city. Although IoT is the most prominent leading technology in smart cities, they have not reviewed other leading technologies, such as cloud computing, artificial intelligence (AI), and blockchain.

In another work [13], Ma studied the smart city and cybersecurity issues along with technologies, challenges, and recommendations. In this article [13], Ma focused on a data-driven approach via the deep learning method and its impacts on smart cities. However, they did not consider other enabling technologies and their effects on smart city security.

In [14], Panahi Rizi and Hosseini Seno thoroughly reviewed security and privacy challenges, issues, and gaps in the realm of the smart city. They also studied several solutions and technologies to employ in security and privacy protection frameworks. In addition, they generally investigated some common applications of the smart city, such as smart healthcare and smart transportation. Nevertheless, modern areas, for example, smart charging of electric vehicles have not been considered.

Fan et al. performed a comprehensive security study through a new perspective called activity-network-things (ANTs), with an emphasis on the IoT [15]. Nonetheless, the authors did not review other leading technologies and provided a holistic survey on privacy issues. In another work [16], Cheng et al. primarily focused on crowdsensing and its applications in the digital city. Although it is a thorough study in the selected area, it does not include enabling technologies, their challenges, and relevant security issues.

Houssein et al. reviewed the application of the IoT in smart cities [17]. They also studied three successful case studies of smart cities, namely, Zurich, Amsterdam, and Masdar, in detail. However, the authors did not explore other enabling technologies, such as blockchain and AI, along with their challenges and opportunities. In addition, this study lacks an in-depth security and privacy investigation of smart cities, including emerging applications, for example, smart charging.

Ultimately, Alsadi et al. conducted a comprehensive study on smart systems, covering their theoretical foundations, applications, and recent advancements [18]. They discussed smart cities as a specific application area of smart systems. However, their study fails to provide new insights about rising security and privacy challenges. They provided general information about attacks on smart systems, categorized by physical, network, and application layers. The authors also studied various types of malware, including viruses and worms.

Based on our comprehensive study, several works focus only on specific aspects [12], [13]. Hence, researchers cannot obtain an in-depth view by studying them. Moreover, some papers were published years ago and do not cover the latest advancements, problems, and solutions [6], [7]. Thus, it is necessary to provide an up-to-date reference in the context of the smart city. Several papers fail to thoroughly examine leading technologies along with security and privacy concerns. In Table II, we categorize these shortcomings with descriptors, such as "Limited exploration of security and privacy" and "Overlooked leading technologies" [11], [17]. Thus, we provide a comprehensive and up-to-date survey of critical security and privacy challenges in the area of user-centric smart city applications to address the aforementioned problems.

III. Overview of Smart City

In this section, we provide an overview of the smart city, including a brief review of leading technologies along with superior security methods and PETs. It helps readers gain a better understanding of smart cities before exploring their security vulnerabilities, privacy issues, and potential solutions. For brevity, we provide only a brief introduction here; interested readers are referred to the following references for further details [2], [22], [23].

A. Leading Technologies

The IoT, cloud computing, blockchain, and AI are four underlying technologies that establish and support smart city environments. In this context, IoT is the major leading technology because it accomplishes substantial operations, such as data collection, connectivity, and mobility. There is a growing inclination toward the adoption of IoT across various sectors of the smart city because it has extensive and undeniable abilities to increase efficiency, productivity, monitoring, tracking, and quality [40]. The IoT market size is projected to grow from U.S. $457.29 billion in 2020 to U.S. $11 680.1 billion by 2030, presenting a compound annual growth rate (CAGR) of 38% [41].

Nonetheless, IoT has evolved rapidly without adequate consideration of assessing potential risks, addressing existing vulnerabilities, and implementing appropriate security frameworks. As a result, there has been an increase in threats, intrusions, and vulnerable attack surfaces targeting infrastructures utilizing IoT devices. An IoT botnet, which comprises numerous IoT devices compromised by malware, is a serious threat to the security of IoT systems. Thus, it is not difficult for an attacker controlling an IoT botnet to launch devastating Distributed Denial of Service (DDoS) attacks.

In addition, using cloud computing technology raises different types of security and privacy concerns. In this regard, users are concerned about their data that are stored on cloud servers [42]. Thus, resilient security mechanisms are necessary to protect data privacy and prevent various types of attacks, such as privileged-insider and Denial-of-Service (DoS) attacks. These mechanisms include various encryption algorithms, intrusion detection and prevention systems (IDS/IPS), secure multiparty computation methods, and hashing.

Blockchain is also widely employed to design and implement cryptocurrencies, for example, Bitcoin and Ethereum. There are numerous payment-related studies for smart cities utilizing different types of cryptocurrencies [43], [44]. It is worth noting that Bitcoin and Ethereum are based on pseudo-anonymity. Thus, proposals relying on these methods cannot protect anonymity, which is a prominent feature in most smart city applications. Ultimately, using AI methods imposes the possibility of several security attacks, such as evasion, poisoning, and model inference attacks. In this respect, privacy violation problems, for example, information leakage, are a serious concern that requires close consideration.

B. Security and Privacy

Over the past decade, there has been a significant increase in cyber threats, raising concerns about security and privacy problems in smart cities. Consequently, it has led to a rise in threats, intrusions, and vulnerable attack surfaces targeting different services and applications. Providing a secure and resilient smart city leads to broader acceptance and increased utilization of smart city applications. Nonetheless, security provisioning in smart cities is a complicated procedure because it is a heterogeneous and physically extensive architecture. Privacy preservation on smart city platforms is also an intricate process because these platforms work based on collecting, processing, analyzing, storing, and sharing massive amounts of data. Citizens' private data constitute a large part of the gathered data. In Tables III and IV, we reviewed several renowned security methods and PETs in smart cities.

IV. User-Centric Smart City Applications

In this section, we first explain the methodology used in our research. Subsequently, we examine the critical security and privacy challenges faced by recently trending user-centric smart city applications, namely, smart parking, smart charging, and smart homes. These applications form a major part of citizens' daily interactions. We also review recent advancements and analyze proposed solutions aimed at enhancing security and privacy in these domains. We divide each smart city application according to its inherent characteristics. Afterward, we review recent and relevant research studies in each smart city application based on a security and privacy analysis approach. We also present a comparison of known security and privacy protection mechanisms for the selected smart city applications.

TABLE III
SOME POPULAR SECURITY METHODS

Method	Description	Application
Identity-based encryption	A variant of public-key encryption where the public key can be any arbitrary string, for example, a user name or email address.	Smart grid [24], smart healthcare [25], smart industry [26]
Attribute-based encryption	An extension of public-key encryption in which both private keys and cipher texts rely on user attributes.	Smart healthcare [27], smart transportation [28], smart industry [29]
Homomorphic encryption	A cryptographic technique that enables calculations on encrypted data, ensuring confidentiality throughout data processing.	Smart transportation [30], smart grid [31], smart home [32]
Secret sharing scheme	A scheme in which a secret is split into fragments and distributed to some entities.	Smart grid [33], smart healthcare [34], smart transportation [35]
Proxy Re-encryption	A public-key cryptography method where a proxy can re-encrypt ciphertexts for a different key without accessing the plaintext.	Smart Parking [36], remote sensing [37]
Message authentication code	A short fixed-length cryptographic checksum generated from a message and a secret key to ensure data integrity and authenticity.	Smart transportation [38], telecommunication [39]

TABLE IV
SOME POPULAR PETS

PET	Description	Application
Data anonymization	Using a variety of techniques, including perturbation, masking, generalization, etc., to eliminate the ability to identify attributes.	Smart charging [45], smart home [46], smart healthcare [47]
Differential privacy	A statistical anonymity model to ensure data privacy by using a selected amount of randomized noise via different mathematical algorithms.	Smart grid [48], smart transportation [49], smart building [50]
Zero knowledge proof	A method that allows a prover to demonstrate a statement to a verifier without disclosing the statement or any additional information about it.	Smart grid [51], smart healthcare [52], smart home [53]
Multi-party computation	It allows multiple parties to jointly perform a computation without disclosing each other's private inputs. There is no reliance on a trusted third party.	Smart grid [54], smart home [55]
Anonymous credentials	A mechanism that enables users to verify their identity, group membership, or any other attribute without compromising their privacy.	Smart transportation [56], smart charging [57], smart industry [58]
Blind Signature	It allows a signer to sign a message without learning what the message contains.	Smart grid [59], crowdsensing [60]

A. Research Methodology

We carried out a series of steps based on the PRISMA method [61], as described in the following.

1) *Defining the Scope of Research:* Initially, we determined the scope of our survey to explore security and privacy problems, corresponding solutions, and recent advances in novel user-centric smart city applications, namely, smart parking, smart charging, and smart homes. In our study, we considered research works that are mainly based on cryptographic schemes. We decided to focus on studies published in 2020 and beyond to include recent developments.
2) *Defining Search Strategy:* We determined several key words, such as "smart city," "IoT," "security," and "privacy" to search for papers. Subsequently, we performed an extensive search in prestigious databases, for example, IEEE Xplore, ACM Digital Library, Science Direct, and Springer. We collected +300 papers in this step.
3) *Screening:* In this step, we meticulously studied +200 recent studies on the security and privacy of smart cities. Initially, we carried out a review of the "title," "abstract," "introduction," and "conclusion" for each paper. Afterward, we excluded irrelevant and duplicate studies. We also refined the search strategy based on the outcomes of our screening.
4) *Complete Review:* In this step, we first thoroughly reviewed the remaining +130 papers using a security and privacy analysis approach. Subsequently, we categorized them based on two criteria, the properties of each smart city application, along with security and privacy protection mechanisms.

B. Smart Parking

In this section, we review the concept of smart parking and related security and privacy issues. We also classify this application into public parking, private parking, and autonomous valet parking based on the existing research works for better investigation.

1) Overview: A significant growth in the number of vehicles and the world population has led to intolerable traffic volume in most cities across the world. Nowadays, finding an appropriate parking spot is a difficult process in congested cities throughout the globe. Drivers should cruise around the desired location and visit multiple places to find a suitable parking lot. It results in wasting time, extra fuel consumption, air pollution, traffic congestion, and noise [62]. Therefore, finding parking lots is a major reason for traffic congestion, which influences the world economy.

Smart parking intends to manage the situation and mitigate the problems by adopting cutting-edge technologies, such as IoT and cloud computing. It results in reducing stress and anger in drivers, enhancing traffic flow, and less fuel consumption [63]. In this regard, the city council of Girona, Spain, intends to implement a new LoRaWAN-based smart parking system as part of its policy for developing and deploying a smart city [64]. Security and privacy are two important issues when developing smart parking management systems. Preventing unauthorized access to parking spots and preserving citizens' private information are two fundamental measures in this context.

2) Smart Parking Methodologies: Here, we accurately investigate the security and privacy issues related to each smart parking methodology, i.e., public parking, private parking, and autonomous valet parking.

a) Public parking: City managers and governments are often expanding public parking lots to create new spaces and reduce traffic volume. Public parking lots play a significant role because they have a large capacity to accommodate vehicles. In the following, we review some recent and relevant research works with an emphasis on security and privacy.

Badr et al. [65] proposed a secure and privacy-preserving smart parking system. They applied short randomizable signature and private information retrieval methods to perform anonymous authentication and protect drivers' location privacy. They also used the commitment technique to guarantee fair parking rates. This technique can retain the integrity of parking rates against the attacks of competitors. This proposal includes a blockchain-based reputation management system in which drivers can anonymously rate the parking service.

In [66], Singh et al. proposed a blockchain-based privacy-preserving smart parking system. An elliptic curve cryptography (ECC)-based ring signature technique is used to protect users' data security. To provide location privacy, they applied an improved private information retrieval approach. The Redis cache and the B+ tree algorithm are employed to construct the private information retrieval solution. The Redis cache is a high-performance key-value memory system primarily utilized to address data processing timeliness issues during high concurrency situations in relational databases. The B+ tree is combined with the Redis cache to mitigate computational overhead because the computational complexity of private information retrieval using the Redis cache can grow with an increase in the number of users and their transactions. In addition, it secretly retrieves parking offers from a multitransaction mode consortium blockchain. Various parking space owners cooperate to build the multitransaction mode consortium blockchain.

Lai et al. proposed a reliable and secure smart parking system that provides dual privacy protection [67]. Differential privacy and mix zone methods are employed to conceal drivers' mobility patterns. To provide anonymous authentication among vehicles, the parking server, and the fog node, they used a novel group signature scheme. The authors also designed a trust model to compute the reliability of the vehicles. The trust model applies both direct trust and recommendation trust to evaluate the reliability. In this scheme, the fog node detects and removes duplicate reports using the message-lock encryption technique. Thus, it can significantly decrease the computation overhead of the server. The authors also proposed an incentive mechanism to reward participating vehicles. It can effectively prevent the same vehicle from obtaining multiple rewards.

In another study [68], Li et al. designed a privacy-aware and decentralized parking recommendation system. They utilized several cryptographic techniques, such as zero-knowledge proof, private set intersection, and an anonymous credential system. In this paper [68], existing parking spots are recommended obliviously. The scheme provides a real-time solution for parking reservation, navigation, and payment. The authors also used a private blockchain and smart contract in their proposal. Ultimately, the proposed scheme comprises an anonymous payment method for the cost of the parking space.

Khaliq et al. [69] proposed a parking recommender system using ECC and local differential privacy. To ensure anonymity and integrity, they applied anonymous credentials and a hash-based message authentication code (HMAC), respectively. They also leveraged the Laplace mechanism, a differential privacy method, to add random noise and remove the necessity for a trusted third party to perturb data. Moreover, the IOTA distributed ledger technology is used to provide immutability and scalability.

In another scheme [70], Singh et al. designed a secure and privacy-preserving smart parking framework for a sustainable city environment. They applied blockchain, AI, and virtualization as three enabling technologies in their scheme. They also divided their framework into six layers as follows: physical, parking, transaction, security, storage and analysis, and driver. The authors implemented the ECC algorithm to provide security by encrypting and decrypting the data, which corresponds to parking zones. They analyze the data using deep learning (deep LSTM networks) to recommend the best parking lot to drivers.

In [71], Hakeem et al. proposed a distributed mobile system to handle parking assignments. The scheme employs users' smartphones to perform computations on parking requests. This offloading technique, along with a distributed dispatcher, maintains the scalability of the system. An entropy-based cloaking method is used to protect the drivers' privacy. Furthermore, the phones of parked drivers are organized into a K-D tree to manage parking requests in a distributed manner. Sun et al. designed a decentralized parking assistance scheme [72]. The consortium blockchain, smart contract, and a double auction pricing algorithm are employed in this proposal. Parking spots are allocated based on user preferences to increase the quality of the user experience. Various analyzes demonstrate that transaction confirmation time and allocation ratio are improved compared to some recent and analogous studies.

In another paper [73], Dujić Rodić et al. investigated how LoRaWAN can result in privacy leakage in smart parking systems. LoRaWAN is a media access control (MAC) layer protocol developed on top of LoRa modulation. LoRaWAN is extensively employed as a communication protocol in smart parking projects because IoT is the primary technology for designing and implementing smart parking systems. It achieves two main advantages, according to the following: First, it is compatible with power-constrained devices; second, it supports coverage over several kilometers [74]. The variation in signal strength of LoRaWAN-enabled parking systems can disclose information about parking lot occupancy. It allows for passive side-channel attacks from long distances. Adversaries can use supervised machine learning techniques to perceive the status of parking spots.

b) Private parking: Despite the development of public parking lots, they alone cannot significantly address the existing issues. High investment, maintenance costs, rapid growth in the number of vehicles, and limited availability of spaces are serious challenges for building new public parking lots [79]. Academic researchers and industry professionals

have presented different proposals, utilizing the concept of private parking.

Zhu et al. proposed an anonymous smart parking and payment system in vehicular networks (ASAP) [75]. They leveraged the short randomizable signature to achieve anonymity and conditional privacy. Moreover, their proposal supports quick result matching and anonymous payment using the hashmap and E-cash, respectively. ASAP is robust against several attacks, such as replay, impersonation, and modification attacks. However, it cannot provide unlinkability in the payment phase and is not immune against man-in-the-middle attacks [71], [79]. In [44], Zhang et al. proposed a decentralized and privacy-aware smart parking system that achieves fairness and reliability. They utilized the BBS group signature, a form of short group signatures, along with the bloom filter, pseudo-random function, and vector-based encryption to guarantee users' privacy. In this scheme [44], reliability is achieved by using a decentralization approach. Additionally, the blockchain smart contract provides fairness. Location, time, and parking price are three factors for allocating parking lots. Nevertheless, the proposed method excludes a parking reservation solution.

Wang et al. proposed a privacy-aware private parking-sharing system based on blockchain technology [76]. The authors employed the market design concept for sharing vacant parking spaces. The protocol provides both anonymous authentication and anonymous payment at the same time. Their scheme relies on multiple cryptographic techniques, for example, bilinear pairing, signatures of knowledge (a variant of noninteractive zero-knowledge proof), distributed anonymous credentials, and a one-way accumulator. Nonetheless, the protocol cannot prevent attackers from gaining unauthorized access to parking spots [88]. In addition, the payment phase cannot provide unlinkability since each coin has a unique serial number and each payment transaction holds a unique transaction ID. It is of utmost importance to preserve the payer's anonymity and untraceability, as well as the unlinkability between various transactions made by the same payer [89].

In another scheme [77], Ibrahim et al. proposed a blockchain-based parking sharing system using the online-to-offline (O2O) model. The principal goal of the O2O model is to raise the awareness of online services. Subsequently, potential users can review various offers and visit local physical locations to make purchases. The proposed scheme provides reliable parking finding and reservation services. The authors applied hash-based data verification and role-based access control to achieve security. In this proposal [77], an off-chain model is also designed to support scalability. However, the protocol lacks a specific and clear payment solution.

Baza et al. designed a decentralized smart parking system using blockchain technology [78]. In this article, both drivers and parking owners send their requests and offers in an encrypted format to achieve privacy. The blockchain can perform matching operations without decrypting the submitted information. The authors also implemented an overlapping and partitioning method to improve the accuracy of the matching results. Therefore, it results in maximizing the benefit for private parking owners. However, the proposed protocol does not consider a privacy-aware payment phase.

In [79], Limbasiya et al. designed a lightweight and secure communication protocol (SAMPARK) for private parking systems. It provides information about available parking lots and parking reservations. The proposed scheme mainly relies on lightweight cryptographic methods, such as hash functions and XOR operations. It is robust against several attacks, including replay, sybil, and password-guessing attacks. Nonetheless, storing some sensitive information and using preshared keys leads to stolen verifier attacks. It also facilitates background knowledge for adversaries, which causes inference attacks. In addition, it can provide background knowledge for privileged insiders, which makes the protocol vulnerable to insider attacks. It will allow privileged insiders to trace vehicle users and link their activities.

In another scheme [80], An et al. proposed an incentive-based parking spot sharing platform. This proposal protects the privacy of users' destinations. In this regard, the Laplace mechanism is used as a differential privacy method to achieve location privacy. The authors defined online parking sharing as a social welfare maximization problem within a two-sided market. They also designed novel threshold value-based rules to identify winners, payments, and reimbursements. The scheme determines winners by solving a mixed-integer nonlinear programming problem. The problem intends to minimize the distance between the user's destination and the assigned parking lot.

In [81], Brenner et al. present a decentralized private parking system based on blockchain technology. They implemented their scheme on two different blockchain platforms: Ethereum and Hyperledger Fabric. They designed several experiments at a variety of transaction send rates to evaluate latency and throughput. Nonetheless, their proposal does not include any particular security or privacy solutions.

c) Autonomous valet parking: The considerable development in sensor networks, communication protocols, and control systems has revolutionized the automotive industry. It has accelerated the leap toward autonomous driving. Following the current trend, autonomous valet parking is a novel context that intends to mitigate parking problems in smart cities. In this area, the parking process initiates when a driver leaves their own vehicle. The vehicle can discover a vacant spot and accomplish the process. The driver can monitor the process via their smartphone. In the following, we investigate the state-of-the-art research works, considering security and privacy issues in this area.

Huang et al. designed a secure and privacy-aware reservation protocol in the context of autonomous valet parking [82]. The authors utilized different methods, such as zero-knowledge proof, proxy resignature, anonymous credential, and bloom filter, in their scheme. The proposed protocol achieves identity privacy, location privacy, and unlinkability simultaneously. In addition, it can withstand double-reservation attacks by using the tokenization mechanism. However, using location obfuscation affects optimal parking scheduling in the presented protocol.

In [83], Ni et al. proposed a robust and privacy-preserving automated valet parking scheme for self-driving vehicles. The scheme consists of a two-factor authentication protocol relying on a one-time password and smart devices to prevent unauthorized access to autonomous vehicles. In this article [83], the BBS+ signature, an improved variant of BBS signature, and Cuckoo filter, a probabilistic data structure, are applied to protect location privacy against malicious parking spot owners. The scheme also allows a trusted authority to trace anonymous drivers for localizing a stolen vehicle.

In another paper [84], Pokhrel et al. proposed a secure and privacy-aware parking reservation framework for autonomous vehicles. They used the zero-knowledge proof to provide identity privacy and the Laplace mechanism to guarantee location privacy. They also adopted reinforcement learning for inference and actions within the system to maximize rewards, leveraging an experience-based approach. The scheme successfully prevents multiple-reservation and collusion attacks. Xu et al. proposed a lattice-based ring signature protocol to ensure security and privacy for autonomous valet parking approaches [85]. The correctness, unforgeability, authenticity, and integrity of messages are accomplished in this scheme. Moreover, it is robust against potential quantum computer attacks. The authors also employed the Cuckoo filter for adding and removing parking service entries.

In [86], Hua et al. proposed a cross-domain self-authentication protocol for autonomous valet parking systems based on consortium blockchain. They exploited the pseudonymous mechanism and edge computing to resolve privacy leakage problems. The authors classified users into two groups to enhance the performance of the authentication operation. Furthermore, they used smart contracts for registration, management, and cross-domain authentication. Additionally, the proposed scheme attempts to solve information-isolated islands and redundant registration challenges in this area. Wang et al. designed a secure reservation service in the realm of long-range autonomous valet parking [87]. The proposed scheme consists of a three-factor authentication and key agreement protocol based on smart cards, passwords, and biometrics. The authors employed bilinear pairing, ECC, and fuzzy extractor methods to construct their protocol. It can successfully thwart data forgery, eavesdropping, and hijacking the control of vehicles. The scheme is also robust against replay, multiple-reservation, and offline dictionary-guessing attacks.

3) Security and Privacy Analysis: In this section, we compare the reviewed papers in terms of security and privacy protection methods in Table V. Subsequently, we examine serious security and privacy challenges in this area.

Identity privacy protection is an important issue because most privacy-preserving schemes depend on pseudonymous mechanisms. It is possible to de-anonymize users in these schemes and provide traceability through graph analysis and address clustering methods [90], [91]. Furthermore, providing anonymity and accountability at the same time is a big challenge in the proposed schemes. Group signatures are a suitable candidate to achieve anonymity-yet-accountability. The ability to de-anonymize misbehaving users is a great advantage of group signature schemes [92]. It is worth noting that relying on a trusted third party can reduce the efficiency and reliability of the scheme, such as [44], [75]. Unauthorized access to parking lots is also a critical security vulnerability that future research should address.

C. Smart Charging

We review the smart charging context along with multiple research studies, focusing on security and privacy issues. We also divide this smart city application into charging stations, wired charging, and wireless charging to provide a more accurate study and deeper understanding.

1) Overview: Policymakers in most countries are diligently endeavoring to motivate individuals to transition from combustion engines to electric vehicles. Air pollution and the constraints of fossil fuels are the most outstanding criteria for replacing combustion engines. In line with the current trend, electric vehicles have gained significant attention in recent years [93]. According to a study published by the International Energy Agency (IEA), the global fleet of electric vehicles (excluding two- and three-wheelers) is projected to reach 230 million by 2030, representing 12% of the global vehicle market [94]. Nevertheless, the proliferation of electric vehicles poses some challenges in terms of electricity supply and the development of charging stations.

Providing a convenient charging process through the development of charging stations on streets and roads is a momentous component of the widespread embrace of electric vehicles. In this regard, another study demonstrates that the electric vehicle charging station market is estimated to grow from U.S. $11.9 billion in 2022 to U.S. $76.9 billion by 2027, registering a CAGR of 45.0% [95]. The positive trend of the electric vehicle charging station market is driven by various factors, including the global surge in electric vehicle sales, governmental support, and policies encouraging mass electric vehicle adoption.

2) Smart Charging Methodologies: In this part, we present a detailed review of relevant security and privacy issues in the context of smart charging. We divide the current area into the following three domains: charging stations, wired charging, and wireless charging.

a) Charging stations: The main function of a charging station is to feed electricity to EV batteries. In recent years, the IoT has modernized the operation of charging stations by providing several capabilities, such as remote monitoring, management, scheduling, and driver billing [96]. Charging stations can be categorized either based on location (e.g., public and private) or the maximum amount of electricity they transfer to EV batteries (e.g., Level-1, Level-2, and Level-3). Level-1, Level-2, and Level-3 charging stations primarily supply power at 120V, 240V, and 480V, respectively [96]. It is worth mentioning that Level-3 can also provide up to 800V energy for several plug-in vehicles. This category is also known as direct current (DC) fast charging. In addition, the Level-1 charging stations are limited to North America because other countries support a 220V power supply for plug-in EVs [97].

TABLE V
COMPARISON OF KNOWN SECURITY AND PRIVACY PROTECTION MECHANISMS IN THE CONTEXT OF SMART PARKING SYSTEMS

Classification	Ref.	Security and Privacy Protection Mechanisms														
		BP	SRS	ZKP	Ring Signature	ECC	PIR	DP	ACr	HMAC	BBS GS	Bloom Filter	Pseudonyms	Pr. Re-signature	BBS+ Signature	Cuckoo Filter
Public Parking	[65]	✓	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–
	[66]	–	–	–	✓	✓	✓	–	–	–	–	–	–	–	–	–
	[67]	✓	–	–	–	–	–	✓	–	–	–	–	–	–	–	–
	[68]	–	–	✓	–	–	–	–	✓	–	–	–	✓	–	–	–
	[69]	–	–	–	–	✓	–	✓	✓	✓	–	–	–	–	–	–
	[70]	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–
	[71]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[72]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[73]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Private Parking	[75]	✓	✓	–	–	–	–	–	–	–	–	–	–	–	–	–
	[44]	–	–	–	–	–	–	–	–	–	✓	✓	✓	–	–	–
	[76]	✓	–	✓	–	–	–	–	✓	–	–	–	–	–	–	–
	[77]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[78]	✓	–	–	–	–	–	–	–	–	–	–	✓	–	–	–
	[79]	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–
	[80]	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	–
	[81]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Autonomous Valet Parking	[82]	–	–	✓	–	–	–	–	✓	–	–	✓	✓	✓	–	–
	[83]	✓	–	✓	–	–	–	–	–	–	–	–	–	–	✓	✓
	[84]	✓	–	✓	–	–	–	✓	✓	–	–	–	–	–	–	–
	[85]	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	✓
	[86]	–	–	–	–	✓	–	–	–	✓	–	–	✓	–	–	–
	[87]	✓	–	–	–	✓	–	–	–	–	–	–	–	–	–	–

Open charge point protocol (OCPP) is a widely implemented de facto standard protocol to provide sustainable communication in the smart charging process. It is an integral part of reservation and management of charging operations for achieving the quality of service. Hence, communication security is an important approach for preserving the security of smart charging. In this regard, Garofalaki et al. investigated the EV charging operation, considering the security problems and challenges of OCPP [98]. They presented a comprehensive review of physical attacks on OCPP-based charging platforms and their countermeasures. Initially, they studied the participants in an OCPP-based charging system. Afterward, they explained the security issues and pertinent measures. Eventually, their survey concluded with open security problems and future research proposals.

In another study, the authors conducted a survey to analyze OCPP-v2.0.1, the most recent version, and its new functionalities, threats, and security countermeasures in the realm of industry 4.0 [99]. They utilized STRIDE, which is a popular threat analysis methodology, to recognize and grade threats based on control and energy criteria. Subsequently, they combined STRIDE with DREAD, a risk evaluation model, to assess the impacts of each attack on control and energy. Finally, the authors identified a set of mitigation solutions according to the results of the risk assessment.

Finding a nearby charging station is an indispensable requisite for EV drivers. It brings some advantages, from reducing EV drivers' anxiety to increasing the acceptance of EVs in societies. Nonetheless, it is imperative to use PETs to preserve EV drivers' sensitive information, such as home and work addresses, mileage, and political affiliations. A privacy breach in this context will reveal the users' lifestyle. In this regard, Danish et al. proposed an efficient charging selection scheme for EV drivers using blockchain technology [100]. They designed a decentralized-based framework to provide secure charging services and trusted reservations by using

smart contracts. In this scheme, the selection of charging stations is performed locally without disclosing sensitive personal information. The protocol is robust against some attacks, for instance, repudiation, tampering, and false reservation attacks.

In another study, Teimoori et al. proposed a blockchain-based intelligent recommendation system to find a suitable charging station for EV drivers [101]. They applied a distributed vertical federated learning (FL) method to protect data privacy among data holders, while a shared model is training. In addition, they used a decentralized cloudlet framework to decrease the communication overhead. In this scheme, cloudlet-based aggregators are responsible for summarizing and sending training parameters in an encrypted format using homomorphic encryption (HE).

In another scheme, Islam et al. proposed a data-oriented security management solution [102]. They adopted differential privacy and FL techniques to design a collaborative network intrusion detection system (NIDS) for EV charging stations. The authors also employed the reinforcement learning method to design an intelligent privacy allocation mechanism at charging stations. The proposed model can dynamically optimize the privacy budget and utility, which eliminates the need for human interventions, for example, inputs from domain knowledge experts. It can also withstand inference attacks on model parameters by leveraging utility-optimized local differential privacy.

An abundant increase in the number of electric vehicles in recent years has led to a burden for EV drivers to charge their EVs. The number of daily charging requests has increased exponentially, while the charging stations have not expanded sufficiently. To confront the problem mentioned, designing optimal charging reservation mechanisms is an effective solution. Hou et al. proposed a secure and privacy-aware authentication protocol for charging reservations of EVs [103]. To provide a reasonable performance, the authors moved computation overhead from EVs to the smart grid center. They utilized the MASK function to conceal private data and the reverse fuzzy extractor to ensure the reliability of the physical unclonable function (PUF) responses. The results of the analyzes demonstrate that the scheme can accommodate a flexible number of users while ensuring the confidentiality and privacy of sensitive reservation data.

Authentication is a drastic defense mechanism against adversaries by providing services for legitimate users. In the realm of smart charging, it is essential to design a fast authentication protocol to achieve users' satisfaction. Wang et al. proposed an ultrafast and lightweight authentication protocol based on extended chaotic maps [104]. Their protocol provides mutual authentication and mitigates internal attacks. Nevertheless, it is vulnerable to single point of failure problems since it is designed based on a centralized server approach. Later, Chen et al. [105] proved that Wang et al.'s scheme is also susceptible to session key leakage. Furthermore, it is indicated that there are inaccuracies in both the EV-owner registration and authentication phases. In [106], Liang et al. proposed an authentication framework for the charging process that ensures both privacy protection and physical security. The framework consists of two schemes: the first is a fully anonymous authentication protocol based on random signatures, and the second is a privacy-preserving data aggregation scheme for the overall electricity consumption of charging stations.

b) Wired charging: Currently, wired charging is the most prevalent method for charging EVs. Stationary charging stations, along with their belongings, are distributed in various areas of cities all over the world. Wired charging can be divided into alternating current (AC) and DC charging modes. There are three levels for both AC and DC chargers according to the maximum voltage, current, and power. Though common power grids are based on AC power, researchers have demonstrated that DC chargers considerably increase the performance of the charging process [107]. In this regard, DC chargers provide time savings for EV drivers by decreasing the charging time. As a result, existing charging stations are primarily DC-type and operate based on a three-phase, four-wire system [108]. It is worth noting that DC fast-charging stations require larger charging cables because they convey a higher value of current than AC charging stations [109].

Zhang et al. proposed a power exchange system based on blockchain to enable EV drivers to securely trade their surplus electricity [110]. They proposed a Proof-of-Benefit consensus to handle massive amounts of trading transactions. It successfully provides high scalability and low variance. Plain transactions can lead to widespread information leakage and analysis of EV drivers' behavior since they encompass sensitive information. Payment details, mileage, and visited locations are some examples of personal and private information. Thus, the authors also designed an authentication protocol using ECC and a data encryption method through a symmetric encryption algorithm.

In another paper [111], Li et al. designed a robust and decentralized charging scheme based on blockchain and fog computing for EVs. A consortium blockchain based on Hyperledger Fabric is designed to provide a secure storage platform and preserve privacy. In this study [111], fog computing is used to reduce communication overhead by enabling local processing. It can effectively decrease the heavy load on cloud servers. The authors also developed a mutual authentication protocol to guarantee the security of communication between EV drivers and fog nodes. They employed the ECC and bilinear pairing as two underlying cryptographic methods.

In [112], Zhang et al. proposed a lightweight and privacy-aware scheme for charging and discharging of electric vehicles. They employed a consortium blockchain to maintain data integrity and prevent single point of failure problems. To preserve the identity privacy of EV drivers, a pseudo-identity algorithm is designed. The authors also used a certificateless signcryption algorithm to protect the confidentiality of real-time power information. This algorithm performs both information signature and encryption in one operation. The proposed algorithm consists of batch aggregation and verification to achieve operational efficiency.

Preserving identity privacy is a critical approach while charging electric vehicles at charging stations. In this regard, Parameswarath et al. proposed a decentralized and privacy-preserving authentication protocol [57]. They applied several

methods, including a decentralized identifier, verifiable credentials, and zero-knowledge proof, to construct the scheme. In this study [57], EV drivers will remain anonymous throughout the charging process at any charging station. However, other participants can verify the EV drivers and investigate their authenticity by using verifiable credentials.

Finally, Li et al. proposed a secure and blockchain-based model to improve the security of EV smart charging [113]. In this scheme, they utilized Hyperledger Fabric to perform key management and trust evaluation. It provides nonrepudiation, authenticity, and tamper-proofness of keys and events. The authors adopted the idea of "never trust, always verify" using the zero-trust architecture (ZTA) to secure data and other worthwhile assets throughout their life cycle. It provides dynamic authorization by implementing dynamic trust assessments of entities. They also used ShangMi cryptographic algorithms and compared them with popular encryption algorithms, such as AES, DES, and RSA.

c) Wireless charging: Although wired charging is the most common method to charge EVs, several difficulties, such as vandalism and safety issues, arise from open contacts and dangling charging cables in cities [123]. Therefore, wireless charging is a suitable supplement and even a conceivable alternative to wired charging. The global market size of wireless charging for electric vehicles is estimated to grow from U.S. $80 million in 2023 to U.S. $1279 million by 2030, presenting a CAGR of 48.4% [124]. The strategy of wireless charging for electric vehicles can be classified into the following three categories: static, quasi-dynamic, and dynamic [125]. Although there are several technical barriers, economic issues, and security concerns, dynamic wireless charging of electric vehicles is a promising technology. It fulfills numerous advantages, for example, mobility and extending driving range, which alleviate range anxiety. Furthermore, it significantly decreases long charging times, which results in time savings for EV drivers. In addition, the battery will be smaller and lighter, which will reduce the cost of producing EVs [126].

Wu et al. proposed a secure and privacy-aware management protocol for energy harvesting dynamic wireless systems [114]. In this article, the authors considered three different system states as follows: high-power state, medium-power state, and low-power state. In all working states, the system executes effective, secure, and reliable operations. In the medium-power state, the system uses a bargaining game theory based on reputation to disseminate power. However, when the system works in the low-power state, it operates according to an incentive model to attract the desire of EVs to sell electric energy. Moreover, the protocol employs a blockchain smart contract to implement the payment phase. Ultimately, the security and integrity of the proposed scheme depend on the ECC and an RSA-based signature, respectively.

In [115], Roman and Gondim designed a secure authentication and key distribution protocol for dynamic wireless charging of EVs. They utilized cloud computing to achieve reliability, scalability, and flexibility. Furthermore, they applied fog computing to provide low latency and pervasive mobility. In this scheme, EV drivers purchase a ticket before sending a charging request. The proposed protocol adopts a prepaid approach for the payment of charging costs based on blind signatures. It ensures the anonymity of EV drivers throughout the charging process. The authors claimed that the protocol is robust against some attacks, for example, impersonation, privileged insiders, and known key attacks.

In another scheme [116], Babu et al. proposed a secure authentication protocol in the context of dynamic wireless charging of EVs. They used lightweight cryptographic techniques, such as ECC, hash functions, and hash chains. This proposal achieves mutual authentication between EVs and the fog server, and between EVs and roadside units. Thus, it can withstand man-in-the-middle and impersonation attacks.

Wang et al. proposed a secure and decentralized scheme for EVs, adopting the concept of charge-while-on-the-road [117]. They designed a fine-grained access control method based on blockchain, which supports traceability and auditability. In this study, EV drivers have full control over their data during trust management because they can store data and issue access tokens to decentralized ledgers. They also designed a scheduling algorithm based on game theory. It optimizes the strategies of three defined energy parties (i.e., the energy nodes, charging EVs, and discharging EVs). Ultimately, they designed a distributed trust model to detect dishonest energy nodes.

In [118], Abouyoussef and Ismail designed a privacy-preserving and scalable networking strategy for dynamic wireless charging of EVs. The proposed networking strategy consists of the following three parts: power coordination, fast authentication, and billing. The scheme relies on a private blockchain where a charging service provider takes decisions. It applies both back-channel and blockchain transactions to achieve the efficiency of communications. The authors also used a group signature method to ensure EV drivers' anonymity and data unlinkability. Additionally, the charging service provider can identify the identity of a malicious EV driver. Finally, a unique distributed random number generator is designed to guarantee the zero-collision probability among all EV drivers over time using HMAC.

In another scheme [119], Babu et al. proposed a secure and lightweight authentication protocol suitable for dynamic wireless charging environments. The proposed scheme includes a prominent feature called seamless handover. It enables EV drivers to conveniently move among numerous roadside units with quick validation. In addition, the authors employed a pseudonymous mechanism to provide identity privacy. The proposed protocol also achieves untraceability and forward secrecy. In terms of performance, the proposed scheme is lightweight since it is mainly designed based on hash functions and XOR operations. Nevertheless, Nguyen et al. [127] claimed that Babu et al.'s protocol is vulnerable to eavesdropping and interception when authentication messages transform into bits at the physical layer.

In another paper [120], Babu et al. proposed a PUF-based and lightweight security protocol for dynamic charging of EVs. The authors used the PUF mechanism to resist machine learning-based attacks. The proposed protocol can also withstand impersonation, privileged insider, and man-in-the-middle attacks. However, in [128], the authors claimed

that Babu et al.'s scheme cannot guarantee unlinkability and perfect forward secrecy. Similar to the preceding research work, this protocol is also lightweight because it is built upon hash functions and XOR operations. This proposal provides pervasive handover for EV drivers both within and among region charging servers.

To withstand potential quantum computer attacks, the authors designed a secure and privacy-preserving authentication protocol based on post-quantum cryptosystems [121]. They applied identity-based encryption with NTRU lattices, a public-key cryptosystem, in the ring learning with error framework. They proved their proposed scheme is also robust against known attacks in the area of EVs. The proposed protocol successfully prevents adversaries from identity spoofing and location tracking.

Eventually, Razmjouei et al. proposed a secure and lightweight charging framework for dynamic wireless charging of EVs [122]. In this regard, they designed a directed acyclic graph (DAG)-based smart contract leveraging cloud computing and edge computing technologies. Moreover, they proposed a collaborative computing resource allocation scheme that assists each access system in choosing a customized service strategy. The authors considered a key distribution center to establish a shared secret key among entities. A certificate authority is also included, which encompasses a registration server and an authentication server.

3) Security and Privacy Analysis: Here, we investigate substantial security and privacy challenges in this context. In addition to identity and location privacy, protecting financial information remains a significant challenge in the smart charging domain. If adversaries are able to correlate citizens' financial details with their locations during each payment, they could infer their entire lifestyle patterns. Developing anonymous payment protocols specifically tailored for the charging process is an important gap that needs further research. Moreover, the broad development of electric vehicles and charging stations has extended the attack surface of smart grids because a charging station acts as an intermediary between the smart grid (as a critical infrastructure) and electric vehicles. Cyber attacks in this domain have caused widespread power outages and blackouts, posing serious threats to national security and public safety [129], [130]. In this section, we also performed a comparison of the studied papers in terms of security and privacy protection methods in Table VI.

D. Smart Home

In this section, we aim to study the concept of smart homes and investigate the top security and privacy challenges. We classified this section into authentication, access control, and digital forensics from the perspective of major security services because the smart home is a complex area. In addition, smart homes cover a wide range of applications, each deserving focused and dedicated study.

1) Overview: The smart home is one of the most important domains of the smart city, in which numerous IoT and non-IoT devices are connected to the Internet. Since Lutolf introduced the concept of the smart home in 1992, there have been a lot of advancements until today [131]. In the last decade, smart home systems have gained tremendous attention, both from academia and industry. It is anticipated that the smart home market will reach U.S. $237.07 billion in 2032 from U.S. $101.79 billion in 2024 at a CAGR of 11.1% [132]. In line with the current trend, several tech giants, such as Amazon, Google, Apple, and Samsung, have developed their own smart home platforms. Nowadays, citizens can easily monitor and control various devices at home, which has notably raised life satisfaction. Nevertheless, serious security and privacy concerns have emerged from a technology-oriented life. Smart home environments require robust and resilient defense mechanisms because any security vulnerability or privacy breach will directly result in the private information disclosure of inhabitants.

2) Smart Home Methodologies: Here, we extensively investigate major defense solutions implemented in various smart home systems, with an emphasis on authentication, access control, and digital forensics.

a) Authentication: Authentication is an inevitable mechanism to protect users, devices, and services in the realm of smart homes. The design of authentication protocols in this area is vastly different from that in other domains. Smart home systems predominantly consist of resource-constrained IoT devices, which cannot execute resource-intensive cryptographic operations. In the following, we review some cutting-edge authentication schemes developed for smart home systems.

In [133], Lin et al. proposed a decentralized mutual authentication protocol between users and a home gateway in the context of smart homes. They used blockchain technology to provide immutability and transparency. In addition, they designed a short group signature to be able to trace a misbehaving user. In this scheme [133], access control is provided through a revocation list rather than a policy table.

Poh et al. proposed an efficient scheme for security and privacy provisioning in smart homes [134]. The scheme is divided into the following two protocols: a lightweight authentication and key establishment protocol, and an interactive searchable encryption protocol. The presented authentication protocol achieves entity and data authentication together with data confidentiality. Furthermore, the searchable encryption protocol guarantees security and privacy for queries in smart homes. Therefore, no one, including service providers and gateway nodes, can infer anything from the data. It is important to note that the authors of this research considered both data-in-transit and data-at-rest security and privacy.

In [135], Yu et al. proposed a three-factor and lightweight authentication protocol for IoT-enabled smart homes. Initially, they proved that Kaur and Kumar's authentication scheme is vulnerable to impersonation and session key disclosure attacks [136]. Subsequently, they presented their privacy-aware authentication protocol, followed by a comprehensive security analysis. In the security analysis section, they investigated the robustness against several known attacks, such as impersonation, session key disclosure, and offline password-guessing attacks. The proposed scheme primarily relies on a fuzzy extractor method and a hash function. Thus, it is lightweight and suitable for resource-limited smart home devices.

TABLE VI
COMPARISON OF KNOWN SECURITY AND PRIVACY PROTECTION MECHANISMS IN THE CONTEXT OF SMART CHARGING SYSTEMS

Classification	Ref.	Security and Privacy Protection Mechanisms														
		BP	Hash Chain	ZKP	FL	ECC	Chaotic Maps	AES	HE	MAC	ID-based Enc.	NTRU	Pseudonyms	PUF	ZTA	RSA
Charging Stations	[100]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[101]	–	–	–	✓	–	–	–	✓	–	–	–	–	–	–	–
	[102]	–	–	–	✓	–	–	–	–	–	–	–	–	–	–	–
	[103]	–	–	–	–	–	–	–	–	–	–	–	✓	✓	–	–
	[104]	–	–	–	–	–	✓	–	–	–	–	–	–	–	–	–
	[106]	✓	–	–	–	–	–	–	–	–	–	–	–	✓	–	–
Wired Charging	[110]	–	–	–	–	✓	–	–	–	–	–	–	–	–	–	–
	[111]	✓	–	–	–	✓	–	–	–	✓	–	–	–	–	–	–
	[112]	–	–	–	–	–	–	–	–	–	–	–	✓	–	–	–
	[57]	–	–	✓	–	–	–	–	–	–	–	–	–	–	–	✓
	[113]	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–
Wireless Charging	[114]	–	–	–	–	✓	–	–	–	✓	–	–	–	–	–	✓
	[115]	✓	✓	–	–	–	–	–	–	✓	–	–	✓	–	–	–
	[116]	–	✓	–	–	✓	–	–	–	–	–	–	✓	–	–	–
	[117]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[118]	–	–	–	–	–	–	✓	–	✓	–	–	–	–	–	✓
	[119]	–	–	–	–	–	–	–	–	✓	–	–	✓	–	–	–
	[120]	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	✓
	[121]	–	–	–	–	–	–	✓	–	–	✓	✓	✓	–	–	–
	[122]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

Using passwords or smart cards for authentication imposes an extra encumbrance regarding memorizing or carrying them, respectively. Hence, Nimmy et al. [137] proposed a lightweight and privacy-preserving remote user authentication protocol based on geometric secret sharing for smart home systems. Geometric secret sharing is a suitable method that provides security against fake gateway and device impersonation attacks. The proposed scheme also utilizes photo response nonuniformity (PRNU), a mechanism to identify an individual camera [138], to uniquely identify the user's smartphone. Using PRNU and biometrics prevents spoofing, smartphone capture, and phishing attacks. In addition, the proposed protocol relies on both public-key and symmetric-key cryptography.

In [139], Iqbal et al. designed a secure and SDN-enabled architecture for smart home systems, considering two different scenarios. In this architecture, a controller is responsible for processing complex operations throughout the network rather than resource-restricted smart home devices. The proposed scheme encompasses a lightweight and privacy-preserving authentication protocol. It supports both secure interactions with smart devices and changing the user's smart mobile. In the second scenario of this proposal [139], the authentication must be repeated because it is assumed that the user holds a new smart mobile device.

Demir et al. proposed a zero-knowledge mutual verification and authentication model for smart home systems [140]. The proposed scheme consists of the following four participants: IoT devices, home gateway, vendor, and home management system. In this proposal, entities authenticate each other by generating proofs utilizing their credentials. To protect privacy, the authors applied fake proofs in a communication model to conceal the identity of IoT devices. They also used AES to secretly share keys and the Camenisch-Shoup encryption method to generate public and private key pairs. The home management system obfuscates MQTT communications to achieve untraceability and prevent any intrusion. Finally, the proposed scheme is mainly based on Idemix verifiable encryption, which is an anonymous credential system developed by IBM [141].

In another scheme [142], Pirayesh et al. designed a secure device authentication and key agreement protocol for smart home networks. They combined physical layer security with hyperelliptic curve cryptography (HECC) to provide stronger security. In other words, they used the inherent randomness of wireless channels to resist eavesdropping attacks. Additionally,

in this protocol [142], both entities participate in the session key generation using dynamic parameters of the wireless channel. Ultimately, they employed a fuzzy extractor to minimize the impact of noise on wireless channels during the extraction of channel-based nonces.

In another paper [143], Iqbal et al. present a secure and privacy-preserving communication protocol for SDN-based smart homes. This proposal intends to achieve smart device authentication, data privacy (both data-at-rest and data-in-transit), and user queries. The proposed protocol includes the following two sections: authentication and key establishment, and user-encrypted searchable queries. The authentication and key establishment scheme aims to provide the authenticity of entities and security for in-transit data. Furthermore, the searchable encryption protocol ensures the privacy of user queries on smart home devices.

In [144], Kane et al. designed a secure network architecture and authentication scheme for LoRa 2.4 GHz-based home area networks. It encompasses appropriate mechanisms for secure data transmission, initial key distribution, and evolving key management. It is worth mentioning that the proposed scheme follows a practical implementation instead of simulation. To provide security, integrity, and authenticity, it applies ChaCha20-Poly1305, an authenticated cipher with associated data (AEAD), which is suitable for resource-constrained smart home devices.

In another study [55], Uppuluri and Lakshmeeswari intend to provide secure multiparty access to different services in smart homes while blocking intrusions caused by attackers. Thus, the authors designed a secure multiparty access and authentication protocol using a fuzzy extractor method. In this scheme [55], a fixed number of biometrics is required to authenticate a user. In other words, a minimum number of participants must authenticate a user. Afterward, a secret string will be generated based on the personal strings of participating users. Hence, an adversary cannot successfully perform a penetration if they obtain the secret credential of only one user. In this proposal [55], KNN is employed to accurately calculate the distance between the registered biometric and the data presented during the authentication.

In another scheme [145], Xu et al. proposed a secure authentication protocol for smart home environments based on blockchain and fog computing. The presented protocol includes TA (trusted authority), end-user, smart contract, smart device, and fog node as participants. The authors adopted a private blockchain because it provides an authorization mechanism and restricts admissions. To address privacy concerns, they applied a fuzzy extractor in the proposed method. It is worth highlighting that authentication is carried out collaboratively by smart contracts on the blockchain and off-chain operations.

Ultimately, Yang et al. proposed a secure authentication protocol in the context of smart homes using blockchain technology [146]. They adopted fog computing to mitigate the latency problem of cloud computing and provide cross-domain authentication. Fog computing is also the main component of the designed federated blockchain, in which fog nodes process the computing tasks of resource-constrained smart home devices. In this scheme [146], users' and smart home data are stored on the blockchain to preserve data integrity. The proposed decentralized authentication protocol can address the single point of failure problem, which is common in centralized approaches. The proposed scheme achieves anonymity and untraceability, and is robust against impersonation, desynchronization, and offline password-guessing attacks.

b) Access control: Access control is a prominent defense method for security and privacy provisioning. It is often combined with authentication to create a robust defense mechanism. In other words, access control and authentication are two accompanying approaches that provide safety against both internal malicious users and external adversaries. Access control intends to protect various resources (e.g., devices, data, and information flow) against unauthorized access. Qiu et al. considered access control as the backbone method to achieve information security [147].

In [148], Stolojescu-Crisan et al. presented two IoT-based systems for smart home environments. qToggle for home automation scenarios and MotionEyeOS, which is a video surveillance operating system for single-board computers. In this scheme [148], qToggle is applied to provide security and access control. It is a simple and flexible solution that can be used to control devices in homes or buildings. Moreover, qToggle simplifies firmware updates in a standardized manner for different types and models of devices. It manages programmable systems with a TCP/IP stack via HTTP requests.

Li et al. proposed a decentralized and fine-grained data access control protocol for IoT-enabled smart home systems [149]. They designed four different smart contracts and a consortium blockchain network to construct and implement their protocol. They also presented a policy customization method to easily add access policies to the blockchain through smart contracts. The proposed scheme can successfully remove the coding strain. This proposal also builds trust and achieves security and privacy through the adoption of bilinear pairing, ECC, and pseudonym methods.

Zhang et al. presented a dual-auditing protocol for fine-grained access control in smart home systems [150]. The authors employed an attribute-based encryption (ABE) method to preserve the security of data sharing. Moreover, they outsourced encryption computing by leveraging edge servers, which can reduce the heavy burden imposed by ABE on resource-constrained smart home devices. Data integrity in an edge server is investigated by designing a zero-knowledge proof mechanism. In addition, the correctness of data in cloud servers is checked by using the aggregation of data blocks and signatures. In this protocol [150], Zhang et al. employed the following two measures to withstand collusion attacks. First, they proposed a hybrid encryption using both AES, a symmetric encryption algorithm, and ABE, an asymmetric encryption algorithm. Second, they leveraged a smart contract with the counting bloom filter.

Ameer et al. proposed two different access control models for smart home IoT, $HyBAC_{RC}$ and $HyBAC_{AC}$ [151]. First, they explained why it is essential to develop a hybrid approach, combining both attribute-based access control and

role-based access control. $HyBAC_{RC}$ is a role-oriented hybrid model, while $HyBAC_{AC}$ is an attribute-oriented hybrid model. $HyBAC_{RC}$ includes relatively static attributes that correspond to access decisions within user and device roles. It leverages the dynamic attributes of users and devices to capture rapidly changing characteristics. Subsequently, it restricts the permissions accessible to each user. In $HyBAC_{AC}$, the user role is one of the multiple user attributes they possess.

In [152], Qashlan et al. designed a three-layer and privacy-preserving architecture in the realm of smart homes. The primary goal of the proposed architecture is to restrict what can be deduced about individual training data from the model. To do so, the authors proposed an access control smart contract on the private Ethereum blockchain to guarantee security among clients, IoT devices, and the cloud. It authenticates various access requests to smart home devices. To preserve privacy, they also utilized TensorFlow machine learning and Renyi differential privacy. Ultimately, Sun et al. proposed an efficient hierarchical delegable signature scheme that ensures forward security [153]. It offers fine-grained, privacy-preserving authorization for citizens in smart home environments and guarantees the integrity of communication content. The authors used bilinear pairing to construct their scheme.

c) Digital forensics: Due to the vast number of cyber attacks in recent years, digital forensics has become a substantial category of data and information security. It intends to provide high-quality and reliable forensic data from attack scenarios and determine the amount of damage [154]. Digital forensics has the following standard procedures to achieve evidence: identification, collection, examination, analysis, and reporting. The results of this process play a crucial role in increasing the robustness of smart home systems against various attacks [155]. In fact, the outputs will be applied as a variety of commands and configurations to defense mechanisms, for example, IDSs/IPSs and firewalls. It is worth mentioning that traditional digital forensics methods cannot provide worthwhile results in modern areas, such as IoT-enabled smart homes [156]. Smart city applications, in particular smart homes, rely on several technologies simultaneously, which leads to the creation of ground-breaking and broad attack scenarios.

Iqbal et al. investigated the feasibility of performing a forensic analysis on a variety of smart plugs [157]. The authors leveraged five IoT devices, along with their related Android apps. They carried out their experiments with various network setups to obtain forensic data. They also determined the existing challenges in the current experiments for forensic analysis. In addition, this article encompasses a review of numerous research studies in the corresponding context. In [158], Barral et al. explained different steps to reverse engineer a Google Home device to extract its firmware and data. Subsequently, they described the data analysis process, which results from the dump. In this regard, they proposed a novel technique to repair corrupted SquashFS file systems based on the assumption of a single or double bit-flip per fragment. They also presented another new technique to manage several potential repairs utilizing a three-valued logic.

Nowadays, IoT cameras are a low-cost and prevalent method to provide physical security. Hence, security provisioning in this domain is imperative since the attack surface has expanded significantly [159]. Following the current trend, firmware security is an important branch of device security. Bhardwaj et al. proposed a firmware security analysis model for IoT-based camera devices [160]. Their comprehensive model consists of twelve steps to carry out firmware analysis and security evaluation. In this regard, the authors quantified the entropy of different types of camera firmware. To do so, they measured the complexity and randomness of data-in-transit, the complication of the firmware code, and the amount of randomness in firmware inputs. They also extracted the compressed file systems and performed a search for some keywords within them.

In another scheme [161], Tok and Chattopadhyay provided a threat model template that can be employed by enthusiasts to discover potential threats in their own research studies. First, they used the STRIDE threat modeling methodology and the Microsoft threat modeling tool to detect threats. Subsequently, they designed a threat model that consists of four layers. Eventually, they converted the identified threats into potential offenses and relevant evidence sources and types.

In another paper [162], Liu et al. proposed a Forensics-as-a-Service (FaaS) model for smart home systems. The proposed model independently operates and makes no change to IoT devices, apps, or platforms because it utilizes a nonintrusive solution. It employs network side-channel analysis for monitoring IoT devices and collecting data. Afterward, it generates provenance graphs by segmenting and clustering the gathered data for smart home modeling. Because nonintrusive solutions cannot efficiently collect data and model a smart home, the authors utilized ML techniques. Finally, they developed a policy-based forensic analysis method using graph-based smart home modeling.

3) Security and Privacy Analysis: Here, we examine key security and privacy challenges in this domain. Any security vulnerability or privacy breach in smart home systems can be life-threatening because it directly impacts citizens' safety. In general, protecting citizens' privacy in the smart home ecosystem is a challenging issue since various smart appliances continuously collect data from inhabitants. A significant portion of this collected data consists of sensitive personal information, which requires robust protection mechanisms. Dragos, an industrial cybersecurity company, reported a cyber attack that resulted in the disruption of central heating to more than 600 apartment buildings in Lviv, Ukraine, during cold weather [163]. The adversaries issued Modbus protocol commands to ENCO controllers used for process control in district heating, hot water, and ventilation systems. Subsequently, it led to incorrect measurements and system failures. Here, we also compared the studied papers in terms of security and privacy protection mechanisms in Table VII. In this table, we excluded digital forensics studies because they employ distinct methods.

TABLE VII
COMPARISON OF KNOWN SECURITY AND PRIVACY PROTECTION MECHANISMS IN THE CONTEXT OF SMART HOME SYSTEMS

Classification	Ref.	Security and Privacy Protection Mechanisms														
		BP	Bloom Filter	ZKP	ABE	ECC	ACr	AES	Group Signature	Camenisch-shoup	Fuzzy Extractor	DP	Pseudonyms	Symmetric Enc.	ChaCha20	MAC
Authentication	[133]	✓	–	–	–	–	–	✓	✓	–	–	–	–	–	–	✓
	[134]	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	✓
	[135]	–	–	–	–	–	–	–	–	–	✓	–	–	✓	–	–
	[137]	–	–	–	–	✓	–	✓	–	–	–	–	–	–	–	–
	[139]	–	–	–	–	–	–	–	–	–	–	–	–	✓	–	–
	[140]	–	–	✓	–	–	✓	✓	–	✓	–	–	–	–	–	✓
	[142]	–	–	–	–	✓	–	✓	–	–	✓	–	–	–	–	–
	[143]	–	–	–	–	–	–	✓	–	–	–	–	–	–	–	✓
	[144]	–	–	–	–	–	–	–	–	–	–	–	–	–	✓	–
	[55]	–	–	–	–	–	–	–	–	–	✓	–	–	–	–	–
	[145]	–	–	–	–	✓	–	–	–	–	✓	–	✓	–	–	–
	[146]	–	–	–	–	–	–	–	–	–	✓	–	✓	–	–	–
Access Control	[148]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[149]	✓	–	–	–	✓	–	✓	–	–	–	–	✓	–	–	–
	[150]	✓	✓	✓	✓	–	–	✓	–	–	–	–	–	–	–	–
	[151]	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	[152]	–	–	–	–	–	–	–	–	–	–	✓	–	–	–	–
	[153]	✓	–	–	–	–	–	–	–	–	–	–	–	–	–	–

V. CASE STUDIES

In this section, we explore the practical advancements and prosperous deployments of smart cities around the world. Most cities around the world have started to design, develop, and implement their smart city projects in the last decade. There are a multitude of worldwide case studies that assist city managers in moving toward smart city implementations. In line with the current trend, the International Institute for Management Development (IMD) published a thorough report and examined the smart city index [164]. They investigated 146 cities all over the world and ranked them based on structures and technologies under five primary areas, namely, health and safety, mobility, activities, opportunities (work and school), and governance. According to the report, the cities of Zurich, Oslo, and Geneva ranked first to third, respectively. The cities of Al-Khobar, Bucharest, Chengdu, and Zagreb also experienced the most substantial improvements in this ranking, as reflected by the analyzed indicators.

VI. INSIGHTS AND LESSONS LEARNED

In this section, we discuss the insights and lessons learned from the literature reviewed. As mentioned earlier, the smart city is a multidisciplinary research domain covering technological and nontechnological themes. However, nontechnological subjects, such as social, cultural, and environmental issues, are beyond the scope of this research.

It is worth mentioning that user-centric smart city applications (i.e., smart parking, smart charging, and smart home) have some common security and privacy challenges. For instance, preserving the privacy of identity, location, and financial information are critical concerns in both smart parking and smart home environments, indicating that privacy preservation remains a primary issue in these domains. While these privacy challenges also exist in smart charging, an additional and significant concern is the security of EV charging stations. Any vulnerability in this area can impact smart grids, which are critical infrastructures. It may threaten national security and public safety. Consequently, the nature of threats and the corresponding protection mechanisms in smart charging differ from those in smart parking and smart home ecosystems.

Our survey demonstrates that security and privacy are integral portions of smart cities. In accordance with the current trajectory, new smart city projects must implement the following strategies: 1) smart cities integrate a plethora of interconnected devices. Hence, security and privacy measures must prioritize a unified defense strategy rather than a series of isolated solutions; 2) the exchange and analysis of cyber

threat intelligence files across security organizations in smart cities is essential for staying aware of ground-breaking vulnerabilities [165]; 3) it is compulsory to utilize the concepts of security and privacy by design; 4) using novel advancements, in particular post-quantum cryptosystems, is indispensable; 5) security protocols in this context should be lightweight to achieve shorter execution times. It will result in improving citizens' experience, convenience, and contentment; and 6) some user-centric smart city applications, such as smart charging, link citizens to critical infrastructures. This can be a point where most forthcoming attacks and damages can occur. Thus, implementing resilient defense measures, such as ZTA, is necessary. We will comprehensively examine the last three strategies mentioned above in Section VIII.

Although we focused on technological issues, nontechnological themes are important to strengthen smart city deployments. In this regard, increasing citizens' security awareness about the risks of cyber attacks and privacy disclosure, as well as methods for augmenting cybersecurity in daily activities, is an undeniable necessity [166].

VII. Discussions on This Survey

In this section, we provide a brief review of the contributions and limitations of this study. Our survey is a detailed and up-to-date study that investigates key security and privacy challenges in recently trending smart city applications from a new perspective. This survey emphasizes user-centric applications, reflecting the core mission of smart cities to enhance citizens' quality of life. We examine applications that are frequently used by citizens in their daily lives, such as smart parking, smart charging, and smart homes. Contrary to current studies, our survey initially attempts to accurately define the concept of a smart city. It assists in providing a better and deeper understanding for readers to conduct future research works in this area. It is carried out by presenting the definition and leading technologies of the smart city, along with superior methods to protect security and privacy. Our survey also provides a comprehensive discussion of open challenges and future research directions to support the development of secure and privacy-preserving smart cities. Ultimately, this article distinguishes itself by focusing on research that employs cryptographic schemes.

Nonetheless, further research should be performed both in academia and industry. This will result in enhanced security and privacy preservation for citizens, which in turn paves the way for the development and deployment of smart cities. In future work, we will thoroughly investigate how AI-based methods can strengthen the security of smart city services and protect citizens' privacy.

VIII. Open Challenges and Future Research Directions

Although remarkable studies have been conducted in academia and industry, there is a need to develop several solutions to address existing security vulnerabilities and privacy violations, as well as to provide higher efficiency. Here, we clarify the research gaps in this context to motivate researchers in academia and industry to conduct future research studies.

A. Post-Quantum Cryptography

The security of smart cities, including their critical infrastructures, services, and applications, depends heavily on public-key cryptosystems, such as ECC. Moreover, public-key cryptosystems constitute a significant component of privacy-preserving protocols within smart city environments. Nonetheless, quantum computers will soon pose a significant threat to public-key cryptosystems. A powerful quantum computer, equipped with a sufficient number of qubits and high-quality quantum gates, can not only break numerous asymmetric encryption algorithms but also weaken the security of symmetric encryption algorithms [167]. Therefore, designing post-quantum cryptosystems is a crucial step toward achieving privacy-preserving and secure smart cities.

Lohachab et al. [168] and Fernández-Caramés et al. [169] conducted a comprehensive survey to secure IoT networks. They investigated IoT characteristics, various types of post-quantum cryptosystems, and challenges for applying these cryptosystems in an IoT network. In [170], Sharma et al. proposed a post-quantum secure ant colony optimization protocol for 5G smart cities. It uses ring learning with error-based key exchange, which provides robustness against quantum computer attacks. The proposed protocol can manage Internet of Vehicles (IoV) environments with dynamic changes in network topology based on controllers, destination, vehicle mobility, and road structure. Although post-quantum cryptosystems can provide essential security in the era of quantum computers, there are two important challenges, as described below.

1) Meeting the Requirements of Users: The major goal of researchers in the area of cryptography is to present the highest security achievable under different restrictions in real-world scenarios. As an example, a novel implementation of McEliece's code-based system takes less computation time than ECC [171]. Nonetheless, the large key size is the main barrier to its wide development. Future works of post-quantum cryptography (PQC) in the context of the smart city should consider compatibility with resource-constrained IoT devices [168], [169]. Computation time, communication overhead, and energy consumption are three paramount properties that should be considered to meet the limitations of IoT devices.

2) Standardization: Standardization is a prerequisite for the broad deployment and acceptance of post-quantum cryptosystems. Although de facto standards sometimes emerge without studies in standard organizations, official standardization is more accepted. It also significantly decreases relevant risks. In this regard, Kumar [172] and Kan et al. [173] performed an in-depth study on the research, development, and standardization of post-quantum cryptosystems. Following the current trend, the NIST opened a call and is standardizing the selected post-quantum cryptosystems. The NIST selected three candidates in the section of digital signature algorithms

and one candidate for the section of public-key encryption and key-establishment algorithms in 2022 [174].

Eventually, the NIST released the first three finalized standards for PQC, titled federal information processing standards (FIPSs) 203, FIPS 204, and FIPS 205 [175]. FIPS 203 is a cryptographic scheme, while FIPS 204 and FIPS 205 belong to digital signature schemes. This significant milestone marks the beginning of a new era of security. Nonetheless, it is essential to develop standardized post-quantum cryptosystems tailored to various domains, such as IoT, to address their specific requirements.

B. Zero-Trust Architecture

Though there are some flaws in the existing conventional security mechanisms, they provide a reasonable level of protection. It is worth highlighting that, in most cases, technology itself does not inherently cause security problems. Instead, human errors in technology implementation create opportunities for attackers. However, traditional mechanisms cannot achieve strong protection for security-sensitive applications. Several smart city applications connect citizens with critical infrastructure systems. As explained earlier, smart charging is an example in this context.

ZTA is a novel paradigm that can provide drastic defense and resilient safety. The first systematic model of this concept dates back to 2010 by Kindervag et al. [176]. He explained that ZTA aims to optimize current security architectures and technologies to achieve future flexibility. Based on the report of the NIST, ZTA is not a straightforward concept that can be realized by only one technology [177]. It will be built based on different elements, including continuous and context-aware authentication, risk-aware access control, micro-segmentation, encryption, and threat intelligence, as described in [178].

In [179], Xagoraris et al. performed a study about the role of a zero-trust security framework for sustainable and resilient smart cities. Initially, they investigated the threats and vulnerabilities in an IoT and cloud-based smart city. They also reviewed potential cyber attacks in the area of smart grids. Ultimately, they studied the importance of a zero-trust security framework based on blockchain to mitigate the existing vulnerabilities and risks. Wang et al. proposed an accurate and privacy-preserving traffic flow prediction scheme based on zero trust in the smart city [180]. They leveraged the locality-sensitive hashing technique to convert multiparty sensor data to related indices in offline mode. In another scheme [181], Zhao et al. designed a zero trust-based security architecture for charging stations. The proposed scheme comprises an ECC-based authentication protocol and zero trust-based access control. It preserves the confidentiality of messages transmitted between vehicles and charging stations.

Although zero-trust models can provide resilient security protection, preserving users' privacy while designing zero-trust schemes is challenging. Aligning with the current issue, most authentication and access control protocols in this context use behavior events during the access process [113]. It can result in citizens' privacy leakages by creating users' profiles. Hence, future works in this context should propose privacy-preserving schemes based on the zero-trust concept.

C. Wireless Technology (6G)

Connectivity is one of the indispensable elements of establishing smart cities since it realizes ubiquitous computing [14]. Thus, the quality of various services in the smart city predominantly depends on communication technologies. Smart city applications require broad coverage, low latency, high-data rate, and reliable communication technologies. Nowadays, 5G provides suitable performance and responds appropriately to existing requirements. Nonetheless, it is necessary to take steps toward 6G because, in the not-too-distant future, 5G cannot provide satisfactory services in smart cities. The continuous increase in the number of connected devices and, as a result, the explosive growth of data are the paramount causes for migrating to 6G. The 6G market is projected to grow from U.S. $5.9 billion in 2023 to about U.S. $100 billion by 2033, with a CAGR of 35.2% from 2023 to 2032 [182].

Nidhi et al. [183] explained that 6G technology is estimated to reach almost complete geographical coverage, geo-location update rates in milliseconds, and subcentimeter geo-location accuracy. They also defined the following 6G use cases: human digital twin, high-speed Internet access in the air, modern smart cities, autonomous systems, and holographic communication-based extended reality (XR).

In another study [184], Singh et al. described AI as one of the enabling technologies of the 6G. Hence, 6G is expected to train itself and learn through real-time feedback from the environment. Nevertheless, AI algorithms impose heavy computational overhead, which results in high power consumption. Therefore, there is a great need to develop optimal AI methods, new signal processing models, and efficient power supply mechanisms. They also determined blockchain-based spectrum, quantum communications, spatial modulation-MIMO, and orbital angular momentum (OAM) multiplexing as other enabling technologies of the 6G. Finally, they introduced the following applications that are dependent on the development of the 6G: tactile Internet, holographic communication, industrial Internet, fully automated driving, and the Internet of Bio-Nano-Things.

Quantum computing is a substantial driver for shaping the future of the 6G. As an example, quantum key distribution is a leading-edge topic in this area, which can augment the security of communication networks. Quantum machine learning is another modern paradigm to increase the efficiency of optimization algorithms. Akbar et al. [185] present a thorough survey about the role of quantum computing in 6G technology. Initially, they conducted a literature review and recognized fifteen important applications of quantum computing in 6G. Afterward, they carried out interviews with industry experts to identify the best practices for the main applications of quantum computing in the 6G. Eventually, the authors presented 49 best practices to effectively implement the identified important quantum applications in the 6G.

In [186], the authors proposed an autonomous irrigation system based on IoT, AI, and 6G. In this scheme, providers

or operators can develop auto-learning models to optimize network parameters, resources, and architectures. Furthermore, the 6G network provides consistent availability and supports various QoS requirements for a vast number of devices. The development and deployment of the 6G create new challenges related to standardization, security, and privacy. The significant increase in pervasive connectivity provided by 6G will expose smart cities to a new generation and groundbreaking threats. Extended attack surface, data privacy and integrity, AI-powered cyber attacks, and physical layer-based attacks (e.g., jamming of terahertz signals [187]) are potential threats in this context. Hence, 6G cellular networks require further research, particularly in terms of security and privacy.

D. Lightweight Security Protocols

Researchers in the field of cryptography have always faced the great challenge of balancing security and performance. On the one hand, the consistency of service availability in smart cities is an undeniable necessity. On the other hand, to counter ever-increasing cyber attacks, it is vital to improve the security and privacy of citizens. Thus, the development and employment of lightweight security protocols is an indispensable solution because most citizens own resource-constrained smartphones when using smart city applications. Furthermore, various types of IoT equipment are also resource-restricted devices that cannot tolerate heavy processing, which causes the battery to deplete quickly. Over the past decade, researchers have leveraged various cryptographic primitives, such as PUFs, fuzzy extractors, and hash functions, to develop lightweight security protocols [134], [135].

In [188], Thakor et al. performed a comprehensive review of lightweight cryptography algorithms. Initially, they studied the performance of the selected algorithms. Afterward, they performed an accurate cryptanalysis. Eventually, the authors investigated several real-time use cases. In another study [189], Thabit et al. studied lightweight block, stream, and hybrid ciphers. Subsequently, they focused on the symmetric lightweight block ciphers. In this regard, they presented a thorough security assessment, performance comparison, and computational complexity analysis.

In 2018, the NIST opened a call to standardize lightweight cryptography algorithms [190]. Ultimately, they announced the selection of the Ascon family in February 2023. Therefore, the NIST and the Ascon team have decided to start standardizing it, which is in progress. Despite all the efforts [191], it is necessary to enhance the security of the existing algorithms and propose other novel algorithms to provide robustness against growing threats. The newly presented algorithms should be able to withstand potential quantum computer attacks. Noura et al.'s research work is an example of how to bridge this gap [192]. They proposed a new lightweight and dynamic key-dependent stream cipher algorithm for emerging systems. It consists of two functions: a typical round function based on cryptographic primitives, and another function for updating these primitives. The results demonstrate that it is compatible with resource-restricted devices and real-time applications.

Robustness against quantum computer attacks and emerging attack vectors, such as machine learning-based attacks or modern side-channel techniques, along with efficiency improvements, are prime issues in future works of lightweight cryptography. Minimizing key sizes, utilizing more frequent dynamic keys, reducing block sizes, simplifying rounds, and creating straightforward key schedules are other open challenges that require attention from researchers [193].

E. Metaverse

The concept of Metaverse has reached significant interest in recent years, particularly after Facebook rebranded as Meta in 2021. Metaverse can be considered an immersive 3-D virtual world where people can interact using avatars to perform their daily activities [194]. In addition, there is a potential for communications, transactions, and new experiences globally [195]. Metaverse consists of several advanced technologies, for example, augmented reality (AR), virtual reality (VR), AI, blockchain, digital twins, IoT, and 3-D modeling.

An economic report indicates that the capital spent on the Metaverse was more than U.S. $120 billion in 2022, which is projected to create a maximum value of U.S. $5 trillion by 2030 [196]. Another economic study by the European Parliament estimates that the worldwide market size of the Metaverse will reach €597.3 billion by 2030 [197]. In [198], Yaqoob et al. investigated the application of Metaverse in the context of smart cities, along with its enabling technologies. Initially, they defined notable advantages of the Metaverse for smart cities. Afterward, they studied several Metaverse-based solutions for various smart city applications, such as smart homes and smart transportation. This study also consists of some evolving projects and use cases, for example, Microsoft Mesh, Amazon AR view, Decenteraland, and Nikeland.

In another study [199], Sarwatt et al. presented a thorough review of the Metaverse application in smart transportation. It includes real case studies and ongoing research projects throughout the world. They also studied the economic, technological, and societal impacts of Metaverse incorporation in smart transportation, along with corresponding challenges. Furthermore, they explained, for example, how Metaverse can improve safety in smart transportation by accident prevention, road hazard warning, and intersection collision warning. The development of Metaverse will cause security and privacy challenges because it leverages novel technologies. As an example, AR and VR are two cutting-edge technologies propelling the Metaverse. They pose new security risks and vulnerabilities as clarified in [200] and [201]. Concerning the same issue, social engineering, DoS attacks, and identity theft are common threats in this area [202].

F. Digital Twins

The digital twin is a promising technology for developing and deploying future smart cities. It can be defined as a virtual replica of a physical object, system, process, or concept,

created through a software model or computer program that interacts with and remains aligned with its physical counterpart [203]. It allows us to perform simulations, testing, monitoring, and analysis [204]. In addition, by generating a digital twin of a physical entity, organizations can obtain useful insights, leverage data-driven decisions, and optimize overall performance. It has gained significant attention in the last decade in academia and industry. Following the current trend, some technology pioneers, for example, Nvidia and Meta, have announced that they are investing in digital twins. The global market of digital twins is estimated to reach U.S. $110.1 billion by 2028 from U.S. $10.1 billion in 2023, growing at a CAGR of 61.3% between 2023 and 2028 [205].

In [206], Wang et al. presented a thorough review of digital twins with an emphasis on architecture, enabling technologies, as well as security and privacy challenges. They proposed an accurate classification of security and privacy threats in the Internet of Digital Twins (IoDT), which include but are not limited to relevant threats to data, communication, and privacy. Subsequently, they studied security and privacy countermeasures in IoDT, such as data security, authentication, access control, and trust management. Here, IoDT denotes a network of linked virtual twins and their corresponding physical entities, along with their properties and values. Although digital twin technology provides a lot of advantages in smart cities, some barriers hinder its leverage. In the following, we explore open security and privacy challenges.

1) *Data Security:* Data plays a crucial role in the IoDT because there is a great need to exchange data between virtual twins and their relevant physical objects to maintain synchronization. There is also another data flow among virtual twins. Therefore, data tampering [207], data poisoning [208], and model inconsistency attacks [209], along with the desynchronization of digital twins [210], are serious threats to data in this part.
2) *Privacy Protection:* The collected data in the IoDT often consist of citizens' personal data. Subsequently, they will be shared among different entities within the IoDT. Hence, this continuous and ubiquitous data collection and sharing exposes citizens' private information to various information disclosure risks. Privacy leakage in model aggregations [211] and model deployments [212], membership inference attacks [213], and model inversion attacks [214] are potential threats in this area. It is worth mentioning that data owners should be able to determine data components for selective disclosure [215]. Aligning with the current issue, blockchain is a promising technology to safeguard data privacy in this domain [216].
3) *Communication Security:* Intertwin (data exchange among virtual twins) and intratwin (data exchange between virtual twins and their related real-world entity) communications require strong security mechanisms to ensure confidentiality and integrity. Otherwise, it will result in attacks, such as eavesdropping, message flooding, interest flooding, DoS, and DDoS attacks. In this regard, data encryption, access privilege, penetration testing, and automated code scanning are key protection methods [217].

IX. Conclusion

In this article, we reviewed the pressing security and privacy challenges in smart cities from a new lens. Initially, we conducted a detailed overview of the smart city, comprising leading technologies, along with renowned security and privacy schemes. Afterward, we investigated the security and privacy issues of recently trending user-centric applications of the smart city, namely, smart parking, smart charging, and smart home. We classified each smart city application according to its inherent attributes. Thereafter, we reviewed the state-of-the-art research works in each smart city application based on a security and privacy analysis approach. We also provided a comparison of known security and privacy protection mechanisms for the selected smart city applications. Hence, we presented two different taxonomies for all smart city applications to provide profound insights for readers. Moreover, we investigated successful case studies and highlighted key insights and lessons learned from the literature. Ultimately, we provided a thorough section on future research directions, encompassing the most recent topics to illuminate and pave the way toward secure and privacy-preserving smart cities.

References

[1] United Nations Department of Economic and S. Affairs. "World urbanization prospects: The 2018 revision." 2019. [Online]. Available: https://www.un-ilibrary.org/content/books/9789210043144
[2] K. Fan et al., "SC-chain: An efficient blockchain framework for smart city," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 7863–7877, Mar. 2024.
[3] R. Auer, R. Böhme, J. Clark, and D. Demirag, "Mapping the privacy landscape for central bank digital currencies: Now is the time to shape what future payment flows will reveal about you," *Queue*, vol. 20, no. 4, pp. 16–38, Sep. 2022.
[4] Y. B. Choi, "Organizational cyber data breach analysis of facebook, equifax, and uber cases," *Int. J. Cyber Res. Educ.*, vol. 3, no. 1, pp. 58–64, 2021.
[5] *Conti Cyber Attack on the HSE*, Health Service Executive, Dublin, Ireland, 2021. [Online]. Available: http://hdl.handle.net/10147/631006
[6] A. Gharaibeh et al., "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.
[7] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, 1st Quart., 2018.
[8] T. Braun, B. C. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustain. Cities Soc.*, vol. 39, pp. 499–507, May 2018.
[9] 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.
[10] J. Curzon, A. Almehmadi, and K. El-Khatib, "A survey of privacy enhancing technologies for smart cities," *Pervasive Mobile Comput.*, vol. 55, pp. 76–95, Apr. 2019.
[11] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: A survey, research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1718–1743, 2nd Quart., 2019.
[12] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "A comprehensive study of the IoT cybersecurity in smart cities," *IEEE Access*, vol. 8, pp. 228922–228941, 2020.
[13] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Rep.*, vol. 7, pp. 7999–8012, Nov. 2021.

[14] M. H. Panahi Rizi and S. A. Hosseini Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet Things*, vol. 20, Nov. 2022, Art. no. 100584.

[15] J. Fan et al., "Understanding security in smart city domains from the ANT-centric perspective," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11199–11223, Jul. 2023.

[16] X. Cheng, B. He, G. Li, and B. Cheng, "A survey of Crowdsensing and privacy protection in digital city," *IEEE Trans. Comput. Social Syst.*, vol. 10, no. 6, pp. 3471–3487, Dec. 2023.

[17] E. H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, "Internet of Things in smart cities: Comprehensive review, open issues, and challenges," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34941–34952, Nov. 2024.

[18] N. Alsadi, W. Hilal, A. McCafferty-Leroux, S. Gadsden, and J. Yawney, "Smart systems: A review of theory, applications, and recent advances," *Internet Things*, vol. 33, Sep. 2025, Art. no. 101667.

[19] S. M. A. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: Applications and challenges," *IEEE Access*, vol. 9, pp. 50961–50981, 2021.

[20] M. Adil et al., "Healthcare Internet of Things: Security threats, challenges, and future research directions," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19046–19069, Jun. 2024.

[21] M. Adil, A. Farouk, H. Abulkasim, A. Ali, H. Song, and Z. Jin, "NG-ICPS: Next generation industrial-CPS, security threats in the era of artificial intelligence, and open challenges with future research directions," *IEEE Internet Things J.*, vol. 12, no. 2, pp. 1343–1367, Jan. 2025.

[22] M. Shen et al., "Blockchains for artificial intelligence of things: A comprehensive survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14483–14506, Aug. 2023.

[23] S. Solera-Cotanilla, M. Álvarez Campana, C. Sánchez-Zas, and M. Vega-Barbas, "Proposal for a security and privacy enhancement system for private smart environments," *Internet Things*, vol. 31, May 2025, Art. no. 101585.

[24] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood, and N. Kumar, "An identity based authentication protocol for smart grid environment using physical Uncloneable function," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4426–4434, Sep. 2021.

[25] Z. Liu, L. Hu, Z. Cai, X. Liu, and Y. Liu, "SeCoSe: Toward searchable and communicable Healthcare service seeking in flexible and secure EHR sharing," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4999–5014, 2024.

[26] T.-F. Lee and Y.-C. Huang, "Efficient extended chaotic map-based IBE for industrial environment," *IEEE Access*, vol. 10, pp. 71278–71283, 2022.

[27] J. Su, L. Zhang, and Y. Mu, "BA-RMKABSE: Blockchain-aided ranked multi-keyword attribute-based searchable encryption with hiding policy for smart health system," *Future Gener. Comput. Syst.*, vol. 132, pp. 299–309, Jul. 2022.

[28] H. Tian, X. Li, H. Quan, C.-C. Chang, and T. Baker, "A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15793–15806, Jul. 2021.

[29] Shruti, S. Rani, and G. Srivastava, "Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme," *Exp. Syst. Appl.*, vol. 235, Jan. 2024, Art. no. 121180.

[30] H. Malik, S. Tahir, H. Tahir, M. Ihtasham, and F. Khan, "A homomorphic approach for security and privacy preservation of smart airports," *Future Gener. Comput. Syst.*, vol. 141, pp. 500–513, Apr. 2023.

[31] Z.-P. Yuan, P. Li, Z.-L. Li, and J. Xia, "A fully distributed privacy-preserving energy management system for networked Microgrid cluster based on homomorphic encryption," *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 1735–1748, Mar. 2024.

[32] S. Zhang, J. Chang, and B. Wang, "A multidimensional data aggregation scheme of smart home in Microgrid with fault tolerance and billing for demand response," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4639–4649, Sep. 2023.

[33] W. Yang, Z. Guan, L. Wu, X. Du, and M. Guizani, "Secure data access control with fair accountability in smart grid data sharing: An edge blockchain approach," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8632–8643, May 2021.

[34] C. Zhang, X. Luo, Q. Fan, T. Wu, and L. Zhu, "Enabling privacy-preserving multi-server collaborative search in smart healthcare," *Future Gener. Comput. Syst.*, vol. 143, pp. 265–276, Jun. 2023.

[35] W. Othman, M. Fuyou, K. Xue, and A. Hawbani, "Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12902–12917, Dec. 2021.

[36] L. Xue, R. Gan, and X. Lin, "The achilles' heel of license plate recognition parking enforcement: Balancing privacy protection and enforcement," *IEEE Internet Things J.*, vol. 11, no. 20, pp. 33164–33176, Oct. 2024.

[37] A. A. Khan et al., "Secure remote sensing data with blockchain distributed ledger technology: A solution for smart cities," *IEEE Access*, vol. 12, pp. 69383–69396, 2024.

[38] F. Oberti, A. Savino, E. Sanchez, P. Casasso, F. Parisi, and S. D. Carlo, "CAN-MM: Multiplexed message authentication code for controller area network message authentication in road vehicles," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 14661–14673, Oct. 2024.

[39] A. K. Roy, V. Varadaranjan, and K. Nath, "Efficient handover authentication protocol with message integrity for mobile clients in wireless mesh networks," *J. Inf. Security Appl.*, vol. 84, Jun. 2024, Art. no. 103806.

[40] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019.

[41] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of Things market analysis forecasts, 2020–2030," in *Proc. 4th World Conf. Smart Trends Syst. Security Sustain. (WorldS)*, 2020, pp. 449–453.

[42] J. Sun, G. Xu, T. Zhang, H. Xiong, H. Li, and R. H. Deng, "Share your data carefree: An efficient, scalable and privacy-preserving data sharing service in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 11, no. 1, pp. 822–838, Jan.–Mar. 2023.

[43] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5760–5772, Jun. 2020.

[44] C. Zhang et al., "BSFP: Blockchain-enabled smart parking with fairness, reliability and privacy protection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6578–6591, Jun. 2020.

[45] B. Tepe, D. Haberschusz, J. Figgener, H. Hesse, D. U. Sauer, and A. Jossen, "Feature-conserving gradual anonymization of load profiles and the impact on battery storage systems," *Appl. Energy*, vol. 343, Aug. 2023, Art. no. 121191.

[46] S. Stirapongsasuti, F. J. Tiausas, Y. Nakamura, and K. Yasumoto, "Preserving data utility in differentially private smart home data," *IEEE Access*, vol. 12, pp. 56571–56581, 2024.

[47] H. Attaullah et al., "Fuzzy-logic-based privacy-aware dynamic release of IoT-enabled healthcare data," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4411–4420, Mar. 2022.

[48] S. Zhao et al., "PPMM-DA: Privacy-preserving multidimensional and multisubset data aggregation with differential privacy for fog-based smart grids," *IEEE Internet Things J.*, vol. 11, no. 4, pp. 6096–6110, Feb. 2024.

[49] C. Chen, X. Hu, Y. Li, and Q. Tang, "Optimization of privacy budget allocation in differential privacy-based public transit trajectory data publishing for smart mobility applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 15158–15168, Dec. 2023.

[50] M. Khalil, M. Esseghir, and L. M. Boulahia, "Privacy-preserving federated learning: An application for big data load forecast in buildings," *Comput. Security*, vol. 131, Aug. 2023, Art. no. 103211.

[51] A. S. Sani, K. Meng, and Z. Y. Dong, "SComm: A real-time mutually authenticated secure communication framework for smart grids," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, 2021, pp. 1–5.

[52] R. Singh, A. D. Dwivedi, G. Srivastava, P. Chatterjee, and J. C.-W. Lin, "A privacy-preserving Internet of Things smart healthcare financial system," *IEEE Internet Things J.*, vol. 10, no. 21, pp. 18452–18460, Nov. 2023.

[53] W. Liu, X. Wang, and W. Peng, "Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing Internet of Things," *IEEE Access*, vol. 8, pp. 8754–8767, 2020.

[54] Z. Liu, Z. Cao, X. Dong, X. Zhao, H. Bao, and J. Shen, "A verifiable privacy-preserving data collection scheme supporting multi-party computation in fog-based smart grid," *Front. Comput. Sci.*, vol. 16, pp. 1–11, Jun. 2022.

[55] S. Uppuluri and G. Lakshmeeswari, "Secure multiparty access and authentication based on advanced fuzzy extractor in smart home," *Soft Comput.*, vol. 28, no. 6, pp. 4899–4914, 2024.

[56] Y. Liu, D. He, M. Luo, H. Wang, and Q. Liu, "ATRC: An anonymous traceable and revocable credential system using blockchain for VANETs," *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, pp. 2482–2494, Feb. 2024.

[57] R. P. Parameswarath, P. Gope, and B. Sikdar, "User-empowered privacy-preserving authentication protocol for electric vehicle charging based on decentralized identity and verifiable credential," *ACM Trans. Manag. Inf. Syst.*, vol. 13, no. 4, pp. 1–21, Aug. 2022.

[58] N. D. Sarier, "Efficient biometric-based identity management on the blockchain for smart industrial applications," *Pervasive Mobile Comput.*, vol. 71, Feb. 2021, Art. no. 101322.

[59] J. Fattahi, "A federated byzantine agreement model to operate Offline electric vehicle supply equipment," *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 2004–2016, Mar. 2024.

[60] S. Liu, Z. Wan, Y. Yuan, Q. Dong, B. Yang, and F. Hao, "Efficient certificateless blind signature scheme with conditional revocation for mobile crowdsensing within smart city," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 15985–15997, May 2024.

[61] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, 2010.

[62] M. R. Alam et al., "A survey on IoT driven smart parking management system: Approaches, limitations and future research agenda," *IEEE Access*, vol. 11, pp. 119523–119543, 2023.

[63] C. P. Lee, F. T. J. Leng, R. A. A. Habeeb, M. A. Amanullah, and M. H. U. Rehman, "Edge computing-enabled secure and energy-efficient smart parking: A review," *Microprocess. Microsyst.*, vol. 93, Sep. 2022, Art. no. 104612.

[64] C. Pous-Sabadí, J. Meléndez, R. C. I Del Olmo, and J. T. Peinado, "Technology assessment for LoRaWAN-based time-limited smart parking: A case study," *IEEE Access*, vol. 12, pp. 158446–158470, 2024.

[65] M. M. Badr, W. A. Amiri, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, and W. Alasmary, "Smart parking system with privacy preservation and reputation management using blockchain," *IEEE Access*, vol. 8, pp. 150823–150843, 2020.

[66] S. Singh, D. Satish, and S. R. Lakshmi, "Ring signature and improved multi-transaction mode consortium blockchain-based private information retrieval for privacy-preserving smart parking system," *Int. J. Commun. Syst.*, vol. 34, no. 14, 2021, Art. no. e4911.

[67] C. Lai, Q. Li, H. Zhou, and D. Zheng, "SRSP: A secure and reliable smart parking scheme with dual privacy preservation," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10619–10630, Jul. 2021.

[68] Z. Li, M. Alazab, S. Garg, and M. S. Hossain, "PriParkRec: Privacy-preserving decentralized parking recommendation service," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4037–4050, May 2021.

[69] A. A. Khaliq, A. Anjum, A. B. Ajmal, J. L. Webber, A. Mehbodniya, and S. Khan, "A secure and privacy preserved parking recommender system using elliptic curve cryptography and local differential privacy," *IEEE Access*, vol. 10, pp. 56410–56426, 2022.

[70] S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-enabled secure framework for energy-efficient smart parking in sustainable city environment," *Sustain. Cities Soc.*, vol. 76, Jan. 2022, Art. no. 103364.

[71] A. Hakeem, R. Curtmola, X. Ding, and C. Borcea, "DFPS: A distributed mobile system for free parking assignment," *IEEE Trans. Mobile Comput.*, vol. 21, no. 12, pp. 4279–4295, Dec. 2022.

[72] L. Sun, S. Sun, and X. Yu, "PAA: A blockchain-based parking assistance alliance with user preference," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7367–7376, Jul. 2023.

[73] L. Dujić Rodić, T. Perković, M. Škiljo, and P. Šolić, "Privacy leakage of LoRaWAN smart parking occupancy sensors," *Future Gener. Comput. Syst.*, vol. 138, pp. 142–159, Jan. 2023.

[74] A. Jabbari and J. B. Mohasefi, "A secure and LoRaWAN compatible user authentication protocol for critical applications in the IoT environment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 56–65, Jan. 2022.

[75] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "ASAP: An anonymous smart-parking and payment scheme in vehicular networks," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 4, pp. 703–715, Jul./Aug. 2020.

[76] L. Wang, X. Lin, E. Zima, and C. Ma, "Towards Airbnb-like privacy-enhanced private parking spot sharing based on blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2411–2423, Mar. 2020.

[77] M. Ibrahim, Y. Lee, H.-K. Kahng, S. Kim, and D.-H. Kim, "Blockchain-based parking sharing service for smart city development," *Comput. Elect. Eng.*, vol. 103, Oct. 2022, Art. no. 108267.

[78] M. Baza, A. Rasheed, A. Alourani, G. Srivastava, H. Alshahrani, and A. Alshehri, "Privacy-preserving blockchain-assisted private-parking scheme with efficient matching," *Comput. Elect. Eng.*, vol. 103, Oct. 2022, Art. no. 108340.

[79] T. Limbasiya, S. K. Sahay, and D. Das, "SAMPARK: Secure and lightweight communication protocols for smart parking management," *J. Inf. Security Appl.*, vol. 71, Dec. 2022, Art. no. 103381.

[80] D. An, Q. Yang, D. Li, W. Yu, W. Zhao, and C.-B. Yan, "Where am i parking: Incentive online parking-space sharing mechanism with privacy protection," *IEEE Trans. Autom. Sci. Eng.*, vol. 19, no. 1, pp. 143–162, Jan. 2022.

[81] G. Brenner, M. Baza, A. Rasheed, W. Lalouani, M. Badr, and H. Alshahrani, "DPark: Decentralized smart private-parking system using blockchains," *J. Grid Comput.*, vol. 21, no. 3, p. 43, 2023.

[82] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11169–11180, Nov. 2018.

[83] J. Ni, X. Lin, and X. Shen, "Toward privacy-preserving valet parking in autonomous driving era," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2893–2905, Aug. 2021.

[84] S. R. Pokhrel, Y. Qu, S. Nepal, and S. Singh, "Privacy-aware autonomous valet parking: Towards experience driven approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5352–5363, Aug. 2021.

[85] S. Xu, X. Chen, C. Wang, Y. He, K. Xiao, and Y. Cao, "A lattice-based ring signature scheme to secure automated valet parking," in *Proc. Int. Conf. Wireless Algorithms Syst. Appl.*, 2021, pp. 70–83.

[86] L. Hua, H. Jiang, J. Xiao, and M. Samie, "Cross-domain self-authentication based consortium blockchain for autonomous valet parking system," *IEEE Access*, vol. 10, pp. 87950–87961, 2022.

[87] D. Wang, Y. Cao, F. Yan, Y. Liu, D. Tian, and Y. Zhuang, "Secure long-range autonomous valet parking: A reservation scheme with three-factor authentication and key agreement," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3832–3847, Mar. 2023.

[88] N. Rozman, M. Corn, and J. Diaci, "Sharing economy: Implementing Decentralized privacy-preserving parking system," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2020, pp. 109–116.

[89] M. R. Momeni, A. Jabbari, and C. Fung, "A privacy-preserving and secure scheme for online payment in the realm of mobile commerce," in *Proc. IEEE Int. Conf. Cyber Security Resilience (CSR)*, 2024, pp. 367–372.

[90] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[91] X. S. Shen et al., "Data management for future wireless networks: Architecture, privacy preservation, and regulation," *IEEE Netw.*, vol. 35, no. 1, pp. 8–15, Jan./Feb. 2021.

[92] V. Sucasas, A. Aly, G. Mantas, J. Rodriguez, and N. Aaraj, "Secure multi-party computation-based privacy-preserving authentication for smart cities," *IEEE Trans. Cloud Comput.*, vol. 11, no. 4, pp. 3555–3572, Oct.–Dec. 2023.

[93] Y. Wu, H. Wang, Y. Zhuang, and Y. Zhang, "A shared charging channel for power and auxiliary batteries in electric vehicles," *IEEE Trans. Ind. Electron.*, vol. 71, no. 7, pp. 8202–8206, Jul. 2024.

[94] IEA. "Global EV outlook 2021." 2021. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2021

[95] "Markets and markets report on ev charging station market." 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/electric-vehicle-supply-equipment-market-89574213.html

[96] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Comput. Security*, vol. 112, Jan. 2022, Art. no. 102511.

[97] I. Rahman, P. M. Vasant, B. S. M. Singh, M. Abdullah-Al-Wadud, and N. Adnan, "Review of recent trends in optimization techniques for plug-in hybrid, and electric vehicle charging infrastructures," *Renew. Sustain. Energy Rev.*, vol. 58, pp. 1039–1047, May 2016.

[98] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP)," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1504–1533, 3rd Quart., 2022.

[99] C. Alcaraz, J. Cumplido, and A. Trivino, "OCPP in the spotlight: Threats and countermeasures for electric vehicle charging infrastructures 4.0," *Int. J. Inf. Security*, vol. 22, no. 5, pp. 1395–1421, 2023.

[100] S. M. Danish, K. Zhang, H.-A. Jacobsen, N. Ashraf, and H. K. Qureshi, "BlockEV: Efficient and secure charging station selection for electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4194–4211, Jul. 2021.

[101] Z. Teimoori, A. Yassine, and M. S. Hossain, "A secure cloudlet-based charging station recommendation for electric vehicles empowered by federated learning," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6464–6473, Sep. 2022.

[102] S. Islam, S. Badsha, S. Sengupta, I. Khalil, and M. Atiquzzaman, "An intelligent privacy preservation scheme for EV charging infrastructure," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1238–1247, Feb. 2023.

[103] W. Hou, Y. Sun, D. Li, Z. Guan, and J. Liu, "Lightweight and privacy-preserving charging reservation authentication protocol for 5G-V2G," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 7871–7883, Jun. 2023.

[104] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou, and C. Su, "Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps," *IEEE Trans. Ind. Appl.*, vol. 58, no. 5, pp. 5616–5623, Sep./Oct. 2022.

[105] C.-M. Chen, Y. Hao, and T.-Y. Wu, "Discussion of 'ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps,"' *IEEE Trans. Ind. Appl.*, vol. 59, no. 2, pp. 2091–2092, May 2023.

[106] Y. Liang, Y. Liu, X. Zhang, and G. Liu, "Physically secure and privacy-preserving charging authentication framework with data aggregation in vehicle-to-grid networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 11, pp. 18831–18846, Nov. 2024.

[107] S. Kaur, T. Kaur, R. Khanna, and P. Singh, "A state of the art of DC microgrids for electric vehicle charging," in *Proc. 4th Int. Conf. Signal Process. Comput. Control (ISPCC)*, 2017, pp. 381–386.

[108] C. Liu et al., "Key security challenges for electric vehicle charging system," in *Proc. 2nd Int. Conf. Artif. Intell. Adv. Manuf. (AIAM)*, 2020, pp. 271–275.

[109] B. Save, A. Sheikh, and P. Goswami, "Recent developments, challenges, and possible action plans for electric vehicle charging infrastructure in india," in *Proc. 9th Int. Conf. Power Energy Syst. (ICPES)*, 2019, pp. 1–6.

[110] X. Zhang, C. Liu, K. K. Chai, and S. Poslad, "A privacy-preserving consensus mechanism for an electric vehicle charging scheme," *J. Netw. Comput. Appl.*, vol. 174, Jan. 2021, Art. no. 102908.

[111] H. Li, D. Han, and M. Tang, "A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3189–3200, Sep. 2021.

[112] S. Zhang, M. Ma, and B. Wang, "A lightweight privacy preserving scheme of charging and discharging for electric vehicles based on consortium blockchain in charging service company," *Int. J. Elect. Power Energy Syst.*, vol. 143, Dec. 2022, Art. no. 108499.

[113] P. Li, W. Ou, H. Liang, W. Han, Q. Zhang, and G. Zeng, "A zero trust and blockchain-based defense model for smart electric vehicle chargers," *J. Netw. Comput. Appl.*, vol. 213, Apr. 2023, Art. no. 103599.

[114] X. Wu, G. Li, and J. Zhou, "A lightweight secure management scheme for energy harvesting dynamic wireless charging system," *IEEE Access*, vol. 8, pp. 224729–224740, 2020.

[115] L. F. Roman and P. R. Gondim, "Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment," *Ad Hoc Netw.*, vol. 97, Feb. 2020, Art. no. 102004.

[116] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo, and Y. Park, "Robust authentication protocol for dynamic charging system of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11338–11351, Nov. 2021.

[117] Y. Wang, H. T. Luan, Z. Su, N. Zhang, and A. Benslimane, "A secure and efficient wireless charging scheme for electric vehicles in vehicular energy networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1491–1508, Feb. 2022.

[118] M. Abouyoussef and M. Ismail, "Blockchain-based privacy-preserving networking strategy for dynamic wireless charging of EVs," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 1203–1215, Jun. 2022.

[119] P. R. Babu, A. G. Reddy, B. Palaniswamy, and S. K. Kommuri, "EV-auth: Lightweight authentication protocol suite for dynamic charging system of electric vehicles with seamless handover," *IEEE Trans. Intell. Veh.*, vol. 7, no. 3, pp. 734–747, Sep. 2022.

[120] P. R. Babu, A. G. Reddy, B. Palaniswamy, and A. K. Das, "EV-PUF: Lightweight security protocol for dynamic charging system of electric vehicles using physical Unclonable functions," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 3791–3807, Sep./Oct. 2022.

[121] T. Bianchi, A. Brighente, and M. Conti, "DynamiQS: Quantum secure authentication for dynamic charging of electric vehicles," in *Proc. 17th ACM Conf. Security Privacy Wireless Mobile Netw. (WiSec)*, 2024, pp. 174–184.

[122] P. Razmjouei, A. Kavousi-Fard, M. Dabbaghjamanesh, T. Jin, and W. Su, "DAG-based smart contract for dynamic 6G wireless EVs charging system," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 3, pp. 1459–1467, Sep. 2022.

[123] O. Sadeghian, A. Oshnoei, B. Mohammadi-ivatloo, V. Vahidinasab, and A. Anvari-Moghaddam, "A comprehensive review on electric vehicles smart charging: Solutions, strategies, technologies, and challenges," *J. Energy Storage*, vol. 54, Oct. 2022, Art. no. 105241.

[124] "Markets and markets report on wireless charging market." 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/wireless-ev-charging-market-170963517.html

[125] M. Amjad, M. F. I. Azam, Q. Ni, M. Dong, and E. A. Ansari, "Wireless charging systems for electric vehicles," *Renew. Sustain. Energy Rev.*, vol. 167, Oct. 2022, Art. no. 112730.

[126] N. Mohamed et al., "A comprehensive analysis of wireless charging systems for electric vehicles," *IEEE Access*, vol. 10, pp. 43865–43881, 2022.

[127] T.-V. Nguyen, H. Sun, H. Wang, and R. Q. Hu, "Authentication and PHY-security schemes for electric vehicle dynamic wireless charging," *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, pp. 1698–1712, Feb. 2024.

[128] J. Wang, S. Wang, K. Wen, B. Weng, X. Zhou, and K. Chen, "An ECC-based authentication protocol for dynamic charging system of electric vehicles," *Electronics*, vol. 13, no. 6, p. 1109, 2024.

[129] F. Li, X. Yan, Y. Xie, Z. Sang, and X. Yuan, "A review of cyber-attack methods in cyber-physical power system," in *Proc. IEEE 8th Int. Conf. Adv. Power Syst. Autom. Protect. (APAP)*, 2019, pp. 1335–1339.

[130] Q. Zhao, X. Qi, M. Hua, J. Liu, and H. Tian, "Review of the recent blackouts and the enlightenment," in *Proc. CIRED Berlin Workshop (CIRED)*, 2020, pp. 312–314.

[131] R. Lutolf, "Smart home concept and the integration of energy meters into a home based system," in *Proc. 7th Int. Conf. Metering App. Tariffs Electricity Supply*, 1992, pp. 277–278.

[132] "Smart home market." 2021. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/home-automation-market-100074

[133] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart homes," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 818–829, Feb. 2020.

[134] G. S. Poh, P. Gope, and J. Ning, "PrivHome: Privacy-preserving authenticated communication in smart home environment," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 3, pp. 1095–1107, May/Jun. 2021.

[135] S. Yu, N. Jho, and Y. Park, "Lightweight three-factor-based privacy-preserving authentication scheme for IoT-enabled smart homes," *IEEE Access*, vol. 9, pp. 126186–126197, 2021.

[136] D. Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home," *J. Inf. Security Appl.*, vol. 58, May 2021, Art. no. 102787.

[137] K. Nimmy, S. Sankaran, K. Achuthan, and P. Calyam, "Lightweight and privacy-preserving remote user authentication for smart homes," *IEEE Access*, vol. 10, pp. 176–190, 2022.

[138] C. Meij and Z. Geradts, "Source camera identification using photo response non-uniformity on WhatsApp," *Digit. Invest.*, vol. 24, pp. 142–154, Mar. 2018.

[139] W. Iqbal et al., "ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart homes," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9622–9633, Jun. 2021.

[140] S. Demir, Ş. Şimşek, S. Gür, and A. Levi, "Secure and privacy preserving IoT gateway for home automation," *Comput. Elect. Eng.*, vol. 102, Sep. 2022, Art. no. 108036.

[141] J. Camenisch et al., *Specification of the Identity Mixer Cryptographic Library*, IBM Res., Zurich, Switzerland, 2010.

[142] J. Pirayesh, A. Giaretta, M. Conti, and P. Keshavarzi, "A PLS-HECC-based device authentication and key agreement scheme for smart home networks," *Comput. Netw.*, vol. 216, Oct. 2022, Art. no. 109077.

[143] W. Iqbal, H. Abbas, B. Rauf, Y. A. Bangash, M. F. Amjad, and A. Hemani, "PCSS: Privacy preserving communication scheme for SDN enabled smart homes," *IEEE Sensors J.*, vol. 22, no. 18, pp. 17677–17690, Sep. 2022.

[144] L. Kane, V. Liu, M. McKague, and G. R. Walker, "Network architecture and authentication scheme for LoRa 2.4 GHz smart homes," *IEEE Access*, vol. 10, pp. 93212–93230, 2022.

[145] X. Xu, Y. Guo, and Y. Guo, "Fog-enabled private blockchain-based identity authentication scheme for smart home," *Comput. Commun.*, vol. 205, pp. 58–68, May 2023.
[146] H. Yang, Y. Guo, and Y. Guo, "Blockchain-based cloud-fog collaborative smart home authentication scheme," *Comput. Netw.*, vol. 242, Apr. 2024, Art. no. 110240.
[147] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.
[148] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "Access control and surveillance in a smart home," *High-Confidence Comput.*, vol. 2, no. 1, 2022, Art. no. 100036.
[149] H. Li, D. Han, and C.-C. Chang, "DAC4SH: A novel data access control scheme for smart home using smart contracts," *IEEE Sensors J.*, vol. 23, no. 6, pp. 6178–6191, Mar. 2023.
[150] X. Zhang, R. hua Shi, W. Guo, P. Wang, and W. Ke, "A dual auditing protocol for fine-grained access control in the edge-cloud-based smart home," *Comput. Netw.*, vol. 228, Jun. 2023, Art. no. 109735.
[151] S. Ameer, J. Benson, and R. Sandhu, "Hybrid approaches (ABAC and RBAC) toward secure access control in smart home IoT," *IEEE Trans. Depend. Secure Comput.*, vol. 20, no. 5, pp. 4032–4051, May 2023.
[152] A. Qashlan, P. Nanda, and M. Mohanty, "Differential privacy model for blockchain based smart home architecture," *Future Gener. Comput. Syst.*, vol. 150, pp. 49–63, Jan. 2024.
[153] J. Sun et al., "Forward-secure hierarchical delegable signature for smart homes," *IEEE Trans. Inf. Forensics Security*, vol. 20, pp. 3950–3965, 2025.
[154] J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 1–15, Jan. 2020.
[155] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.
[156] A. Shalaginov, A. Iqbal, and J. Olegård, "Iot digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications," in *Proc. 4th Int. Conf. Edge Comput. (EDGE)*, 2020, pp. 1–17.
[157] A. Iqbal, J. Olegård, R. Ghimire, S. Jamshir, and A. Shalaginov, "Smart home forensics: An exploratory study on smart plug forensic analysis," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, 2020, pp. 2283–2290.
[158] H. Barral et al., "A forensic analysis of the Google home: Repairing compressed data without error correction," *Forensic Sci. Int. Digit. Invest.*, vols. 42–43, no. 1, 2022, Art. no. 301437.
[159] K. Li, W. Ma, H. Duan, and H. Xie, "Multi-source refined adversarial domain adaptation with transfer complementarity infusion for IoT intrusion detection under limited samples," *Exp. Syst. Appl.*, vol. 254, Nov. 2024, Art. no. 124352.
[160] A. Bhardwaj, K. Kaushik, S. Bharany, and S. Kim, "Forensic analysis and security assessment of IoT camera firmware for smart homes," *Egypt. Inf. J.*, vol. 24, no. 4, 2023, Art. no. 100409.
[161] Y. C. Tok and S. Chattopadhyay, "Identifying threats, cybercrime and digital forensic opportunities in smart city infrastructure via threat modeling," *Forensic Sci. Int. Digit. Invest.*, vol. 45, Jun. 2023, Art. no. 301540.
[162] X. Liu, X. Fu, X. Du, B. Luo, and M. Guizani, "Machine learning-based non-intrusive digital forensic service for smart homes," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 2, pp. 945–960, Jun. 2023.
[163] "Impact of frostygoop ICs malware on connected OT systems." Accessed: July, 2025. [Online]. Available: https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology
[164] IMD. "IMD smart city index 2025." 2025. [Online]. Available: https://imd.widen.net/s/psdrsvpbk7/imd_smart_city_2025_report
[165] W. Yang and K.-Y. Lam, "Automated cyber threat intelligence reports classification for early warning of cyber attacks in next generation SOC," in *Proc. 21st Int. Conf. Inf. Commun. Security (ICICS)*, 2019, pp. 145–164.
[166] S. Chaudhary, "Driving behaviour change with cybersecurity awareness," *Comput. Security*, vol. 142, Jun. 2024, Art. no. 103858.
[167] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
[168] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100174.
[169] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.
[170] T. Sharma, M. R. Kumar, S. Kaushal, D. Chaudhary, and K. Saleem, "Privacy aware post quantum secure ant colony optimization ad hoc on-demand distance vector routing in intent based Internet of Vehicles for 5G smart cities," *IEEE Access*, vol. 11, pp. 110391–110399, 2023.
[171] D. J. Bernstein, T. Chou, and P. Schwabe, "McBits: Fast constant-time code-based cryptography," in *Proc. 15th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, 2013, pp. 250–272.
[172] M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," *Array*, vol. 15, Sep. 2022, Art. no. 100242.
[173] K. Kan et al. "Recent trends on research and development of quantum computers and standardization of post-quantum cryptography." 2021. [Online]. Available: https://www.imes.boj.or.jp/research/papers/english/me39-6.pdf
[174] "The NIST selected algorithms." 2022. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
[175] "The NIST final standards of post-quantum cryptography." 2024. [Online]. Available: https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved
[176] J. Kindervag et al., *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*, Forrester Res. Inc., Cambridge, MA, USA, 2010.
[177] V. Stafford, *Zero Trust Architecture*, document NIST SP-800, NIST, Gaithersburg, MD, USA, 2020.
[178] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.
[179] L. Xagoraris, D. Kogias, and P. Karkazis, "A review of zero trust security framework (ZTF) for sustainable and resilient smart cities," in *Proc. 27th Pan–Hellenic Conf. Prog. Comput. Inf. (PCI)*, 2024, pp. 269–273.
[180] F. Wang et al., "Privacy-aware traffic flow prediction based on multi-party sensor data with zero trust in smart city," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–19, Aug. 2023.
[181] Y. Zhao, H. Miao, W. Liu, S. Wang, and R. Zhang, "Research on security protection methods for state grid charging stations based on zero trust," in *Proc. 3rd Int. Conf. Energy Eng. Power Syst. (EEPS)*, 2023, pp. 943–946.
[182] "The 6G market size." Accessed: 2023. [Online]. Available: https://aws.amazon.com/marketplace/pp/prodview-tvcbqawfgems4
[183] Nidhi, B. Khan, A. Mihovska, R. Prasad, and F. J. Velez, "Trends in standardization towards 6G," *J. ICT Stand.*, vol. 9, no. 3, pp. 327–348, 2021.
[184] P. R. Singh, V. K. Singh, R. Yadav, and S. N. Chaurasia, "6G networks for artificial intelligence-enabled smart cities applications: A scoping review," *Telemat. Inf. Rep.*, vol. 9, Mar. 2023, Art. no. 100044.
[185] M. A. Akbar, A. A. Khan, and S. Hyrynsalmi, "Role of quantum computing in shaping the future of 6G technology," *Inf. Softw. Technol.*, vol. 170, Jun. 2024, Art. no. 107454.
[186] S. R et al., "A novel autonomous irrigation system for smart agriculture using AI and 6G enabled IoT network," *Microprocess. Microsyst.*, vol. 101, Sep. 2023, Art. no. 104905.
[187] A. Mukherjee, "Jamming vulnerability of terahertz wireless networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, 2022, pp. 426–430.
[188] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.
[189] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography algorithms for enhancing IoT security," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100759.
[190] "The NIST lightweight cryptography standardization." Accessed: 2018. [Online]. Available: https://csrc.nist.gov/projects/lightweight-cryptography
[191] A. Raza et al., "A lightweight group-based SDN-driven encryption protocol for smart home IoT devices," *Comput. Netw.*, vol. 250, Aug. 2024, Art. no. 110537.
[192] H. Noura, O. Salman, R. Couturier, and A. Chehab, "LESCA: LightwEight stream cipher algorithm for emerging systems," *Ad Hoc Netw.*, vol. 138, Jan. 2023, Art. no. 102999.
[193] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Gener. Comput. Syst.*, vol. 129, pp. 77–89, Apr. 2022.

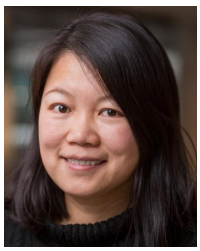
[194] M. Xu et al., "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 656–700, 1st Quart., 2023.
[195] Y. Wang et al., "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 319–352, 1st Quart., 2023.
[196] "Value creation in the metaverse." Accessed: Nov. 1, 2022. [Online]. Available: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-Metaverse
[197] C. Polona, M. T. André, and N. Maria. "Metaverse: Opportunities, risks and policy implications." 2022. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557
[198] I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, "Metaverse applications in smart cities: Enabling technologies, opportunities, challenges, and future directions," *Internet Things*, vol. 23, Jun. 2023, Art. no. 100884.
[199] D. S. Sarwatt, Y. Lin, J. Ding, Y. Sun, and H. Ning, "Metaverse for intelligent transportation systems (ITS): A comprehensive review of technologies, applications, implications, challenges and future directions," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 7, pp. 6290–6308, Aug. 2024.
[200] Y. Wang and J. Zhao, "A survey of mobile edge computing for the metaverse: Architectures, applications, and challenges," in *Proc. IEEE 8th Int. Conf. Collaboration Internet Comput. (CIC)*, 2022, pp. 1–9.
[201] S. Qamar, Z. Anwar, and M. Afzal, "A systematic threat analysis and defense strategies for the metaverse and extended reality systems," *Comput. Security*, vol. 128, May 2023, Art. no. 103127.
[202] S.-Y. Kuo, F.-H. Tseng, and Y.-H. Chou, "Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism," *Future Gener. Comput. Syst.*, vol. 143, pp. 179–190, Jun. 2023.
[203] B. R. Barricelli, E. Casiraghi, and D. Fogli, "A survey on digital twin: Definitions, characteristics, applications, and design implications," *IEEE Access*, vol. 7, pp. 167653–167671, 2019.
[204] S. Mihai et al., "Digital twins: A survey on enabling technologies, challenges, trends and future prospects," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2255–2291, 4th Quart., 2022.
[205] "Digital twin market size, share and industry trends growth analysis." Accessed: 2023. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html
[206] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan, and Y. Liu, "A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 14965–14987, Sep. 2023.
[207] W. Yang et al., "Semantic communications for future Internet: Fundamentals, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 213–250, 1st Quart., 2023.
[208] B. Nour, S. Mastorakis, R. Ullah, and N. Stergiou, "Information-centric networking in wireless environments: Security risks and challenges," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 121–127, Apr. 2021.
[209] D. Pasquini, D. Francati, and G. Ateniese, "Eluding secure aggregation in federated learning via model inconsistency," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, 2022, pp. 2429–2443.
[210] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 669–680, Jan. 2020.
[211] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane, and Y. Wu, "A platform-free proof of federated learning consensus mechanism for sustainable Blockchains," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3305–3324, Dec. 2022.
[212] M. Xue, Y. Zhang, J. Wang, and W. Liu, "Intellectual property protection for deep learning models: Taxonomy, methods, attacks, and evaluations," *IEEE Trans. Artif. Intell.*, vol. 3, no. 6, pp. 908–923, Dec. 2022.
[213] H. Hu, Z. Salcic, L. Sun, G. Dobbie, P. S. Yu, and X. Zhang, "Membership inference attacks on machine learning: A survey," *ACM Comput. Surveys*, vol. 54, no. 11s, pp. 1–327, Sep. 2022.
[214] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction APIs," in *Proc. 25th USENIX Conf. Security Symp. (SEC)*, 2016, pp. 601–618.
[215] Z. Pervez, Z. Khan, A. Ghafoor, and K. Soomro, "SIGNED: Smart city digital twin verifiable data framework," *IEEE Access*, vol. 11, pp. 29430–29446, 2023.
[216] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient federated learning and Permissioned blockchain for digital twin edge networks," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2276–2288, Feb. 2021.
[217] M. Hearn and S. Rix, "Cybersecurity considerations for digital twin implementations," *IIC J. Innov*, vol. 10, pp. 107–113, Jun. 2019.

Mohammad Rasool Momeni (Graduate Student Member, IEEE) is currently pursuing the Ph.D. degree in information and systems engineering with the Concordia University, Montreal, QC, Canada.

He has served as a Faculty Member and an IT Security Specialist for nearly a decade. His research interests are cryptography, data and network security, and privacy-enhancing technologies.

Abdollah Jabbari (Member, IEEE) received the Ph.D. degree in information technology engineering from Urmia University, Urmia, Iran, in 2020.

He is currently a Research Associate with the Concordia University, Montreal, QC, Canada. His main research interests include applied cryptography, network security, and information security.



Carol Fung (Member, IEEE) received the bachelor's and master's degrees in computer science from the University of Manitoba, Winnipeg, MB, Canada, in 2005 and 2007, respectively, and the Ph.D. degree in computer science from the University of Waterloo, Waterloo, ON, Canada, in 2013.

She is currently an Associate Professor with the Concordia University, Montreal, QC, Canada.

Dr. Fung serves as an Associate Editor for several leading journals, including IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT and *Elsevier Computer Networks*.

Raouf Boutaba (Fellow, IEEE) received the M.Sc. and Ph.D. degrees in computer science from Sorbonne University, Paris, France, in 1990 and 1994.

He is currently the University Chair Professor and the Director of the David R. Cheriton School of Computer Science with the University of Waterloo, Waterloo, ON, Canada. Additionally, he holds the Rogers Chair in Network Automation.

He is a Fellow of the Engineering Institute of Canada, the Canadian Academy of Engineering, and the Royal Society of Canada.