electronics

Article

A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges

Abeer Iftikhar Tahirkheli [1], Muhammad Shiraz [2], Bashir Hayat [3], Muhammad Idrees [4], Ahthasham Sajid [5], Rahat Ullah [6], Nasir Ayub [2] and Ki-Il Kim [7,*]

1 Department of Computer Science, Bahira University Islamabad, Islamabad 44000, Pakistan; abeer_iftikhar@yahoo.com
2 Department of Computer Science, Federal Urdu University of Arts, Science and Technology, Islamabad 44000, Pakistan; drmuhammadshiraz@fuuastisb.edu.pk (M.S.); nasir.ayubse@gmail.com (N.A.)
3 Institute of Management Sciences Peshawar, Peshawar 25000, Pakistan; bashir.hayat@imsciences.edu.pk
4 Department of Computer Science and Engineering, Norowal Campus, University of Engineering and Technology, Lahore 54890, Pakistan; midrees10@uet.edu.pk
5 Department of Computer Science, Faculty of ICT, Baluchistan University of Information Technology Engineering and Management Sciences Quetta, Quetta 87300, Pakistan; ahthasham.sajid@buitms.edu.pk
6 Department of Electrical Engineering, Federal Urdu University of Arts, Science and Technology, Islamabad 44000, Pakistan; dr.rahat@fuuastisb.edu.pk
7 Department of Computer Science and Engineering, Chungnam National University, Daejeon 34134, Korea
* Correspondence: kikim@cnu.ac.kr

Citation: Tahirkheli, A.I.; Shiraz, M.; Hayat, B.; Idrees, M.; Sajid, A.; Ullah, R.; Ayub, N.; Kim, K.-I. A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics* **2021**, *10*, 1811. https://doi.org/10.3390/electronics10151811

Academic Editors: Farhan Amin, Seong Oun Hwang, Aftab Ali and Ikram Asghar

Received: 7 June 2021
Accepted: 16 July 2021
Published: 28 July 2021

Abstract: Cloud Computing (CC) is a promising technology due to its pervasive features, such as online storage, high scalability, and seamless accessibility, in that it plays an important role in reduction of the capital cost and workforce, which attracts organizations to conduct their businesses and financial activities over the cloud. Even though CC is a great innovation in the aspect of computing with ease of access, it also has some drawbacks. With the increase of cloud usage, security issues are proportional to the increase. To address these, there has been much work done in this domain, whereas research work considering the growing constrained applications provided by the Internet of Things (IoT) and smart city networks are still lacking. In this survey, we provide a comprehensive security analysis of CC-enabled IoT and present state-of-the-art in the research area. Finally, future research work and possible areas of implementation and consideration are given to discuss open issues.

Keywords: security; privacy; integrity; non-repudiation; threats; green consequences; challenges; mobile computing; edge computing; CC Security

1. Introduction

With the introduction of the IoT, every object is connected to the Internet to provide diverse types of services, like resource management, scalability, elasticity, power management, data storage, etc. Concepts of CC have been proposed to provide these services. CC provides many facilities, such as remotely accessing data, cost reduction, bandwidth, storage, and ease of access [1]. Its services can run over distributed networks without any interface, as shown in Figure 1. Cloud Service Providers (CSPs) require their software and hardware, while users have to install CC-based web applications [2]. Clouds provide us with interoperability and control sharing managed by different authorities, which is why trust matters for sharing sensitive data. Clouds have many types, like the public, private, community, and hybrid [3,4].

Edge computing is an emerging technology to bring computational and storage resources closer to the data source, which increases the responses time and saves the

limited bandwidth in response to the rapid growth of the IoT and the growing demands of advanced level services and applications. However, security, privacy, and protection of data in the edge-based nodes in the computing world are the significant challenges due to limited offered resources and vast sensitive user data over the edge nodes [5–7]. Traditional CC, which is used to support general computing systems, cannot meet the needs of IoT and mobile services due to issues, including location unawareness, bandwidth constraints, high operating costs, a lack of real-time services, and data privacy concerns [8]. These CC limitations pave opportunities for edge computing, where this technology is conceptualized globally to meet the runtime, as well as real-time growing demands of IoT and mobile devices or nodes [9–11].

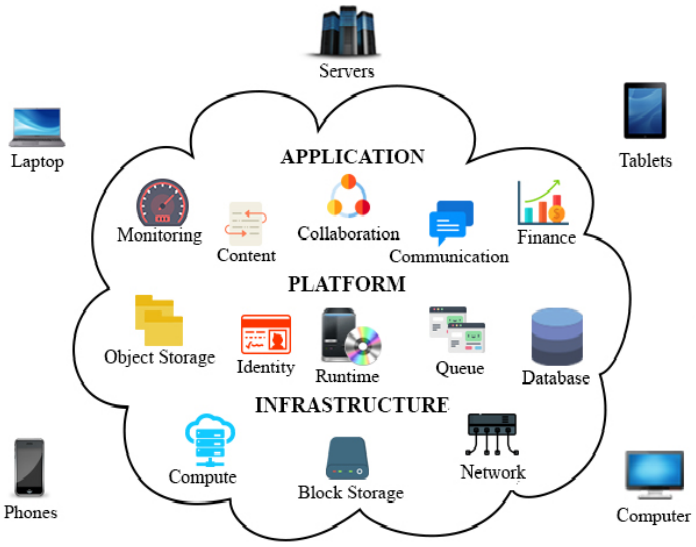

Figure 1. CC model.

Smart cities' networks have been designed to handle diverse fields of life, including transportation, electricity, healthcare, banking, and administration sectors [12,13]. There are various types of smart systems that have been implemented in smart cities, such as IoT, smart grids, Wireless Sensor Networks (WSN), and Intelligent Transportation Systems (ITS) [14–17]. All data communication in these edge-based smart systems is based on secure and trustworthy communication among all devices in smart cities [18–21]. There is an increasing need for high-level protection strategies in edge-based smart cities networks due to the large number of users involved, complex systems, and sensitive data [18,22]. One of the significant challenges for ensuring secure and consistent data communication over such networks is security [23–26]. In general, a single preventive measure would not be able to handle all security risks [27–29]. It forces the protection of priceless data by identifying threats in real-time, allowing for cost-effective detection and treatment [30,31]. Furthermore, due to the vulnerable nature of high-risk environments, a few threats and countermeasures/precautionary measures are difficult to assess [32].

Many companies are shifting towards CC. When data owners send their data to the CSP, they provide the right to use the data. CSP can misuse the data. Data integrity is essential when you have data online, like on a cloud, server, or fog, specifically related to your business, family, or health, and it becomes extremely important to secure it. In CC, the key challenges are privacy, protection, integrity, and non-repudiation, while, in smart city networks, security-based approaches are needed to increase the degree of trust for deployed nodes in smart cities based on their past experiences, directly or indirectly, to record and serialize all information, especially sensitive business-oriented data for decision making.

Existing security-based solutions, including authentication and cryptography-based solutions, provide security resolutions to a certain extent and cannot tackle various internal attacks. Mostly in academia, more emphasis is being put on the implementation of security frameworks in edge-based smart cities [33,34]. The basic concept behind the edge computing networks is to utilize a hierarchy of edge network-based servers with increased computational capabilities to handle the mobile and heterogeneous computational tasks typically offloaded by low-end edge devices (IoT and mobile devices). Edge computing can support evolving smart city applications by providing location-aware, bandwidth-sufficient, real-time, privacy-conscious, and low-cost services [35,36]. Edge computing has grown rapidly in recent years as a result of its advantages over CC. According to Statista's most recent survey, the demand for edge computing in the United States is expected to grow from $84.3 million in 2018 to $1031 million by 2025 [37]. According to a recent estimation globally, the total number of IoT-based devices had reached 11.2 billion in the year 2018, with a predicted forecast of almost 20 billion by 2020. On the one hand, edge computing offers a viable computing technology for smart city networks and beyond. On the other hand, its introduction is prone to creating more security and privacy risks by escalating the real-world attacking surfaces from several perspectives.

The majority of current research is focused on modeling security architectures without taking periodic node re-evaluation into account. Malicious nodes change their actions from time to time, dropping fewer data packets and having a higher data distribution ratio in the network. To deal with these issues in smart city networks against internal and external threats, a more robust approach for handling malicious nodes in the network is needed to address security and privacy concerns. This paper has done a comprehensive analysis of existing CC mechanisms over the smart city networks. We have set many parameters, such as scalability, portability, computation, non-repudiation, interoperability, data provenance, network life, and QoS parameters, related to traffic analysis. We have shown our analysis in the form of a table. The remaining part of this survey paper is organized as follows. In Section 2, related work and concepts of privacy and security models of CC are discussed, and the summarized table of CC is presented. In Section 3, candid analysis over the concept of CC security and its concerns, consequences, and challenges is done. In Section 4, deliberate discussion over the Privacy and Security in a cloud-based smart city network its threats, vulnerabilities, consequences, and challenges is done. In Section 5, open issues are deliberately discussed in detail, and, lastly, in Section 6, the work is concluded with recommendations and a futuristic way forward.

2. Privacy and Security Models of CC and Related Concepts

2.1. Related Work and Concepts

This section covers the deliberate discussion on existing work done in security and privacy aspects in CC.

(1) Security and Privacy Issues in CC:

Recently, researchers are of the opinion that, when the cloud is used for different purposes as storage data, it puts their sensitive data out there and allows users to enjoy network-based access to communication tools, like emails and calendars, use different tools, i.e., Microsoft office and Google Docs, through the internet, for application development and also testing the application and use for business, as well as for backup and restore the data. So, privacy and security are very crucial. A user uses the cloud for different purposes. Data is inexhaustibly put away outside the control of the data owner's machine. The absence of his insight for the data owner is how the information is utilized, and where the information is being put away. In this way, there is a need for the data owner to have more power over their data, such as the dimension of control they have when the data are being put away, individually or by machine [38].

Data owners do not want their data shared with anyone, and not used by anyone. Suppose the data owner wants to share the data with their colleagues. Data owners want strong privacy and security of data in the cloud. For data not accessed by the unauthorized

user, a solution is Secure-Data based on "XACML". The owner makes a data policy of data, and an application is run for monitoring the data of the cloud. The application does disable the option of print, save, etc. Data owners have full control of their data [39]. An Android app accesses data. When anyone wants to access the data, the IMEI of the device is used to identify the user. In this model, another method, ABE, is used for encryption, where the attributes of the user need to be matched with the attributes provided by the owner. Two-way authentication provides high security, as well as high privacy for cloud data [40].

Security and privacy are challenging issues in CC. To overcome these issues, a solution is proposed that based on "Unikernel" [41], a novel method for diminishing the Software attacks for a cloud-based framework, which, in the process, expels numerous attack vectors. They propose a framework that describes the formal approach for securing the cloud and describes the challenges of privacy and security. Privacy and security are also significant challenges in IoT, and the distributed nature of IoT makes them vulnerable [42]. Decentralized privacy and security can be archived by blockchain approach, but this approach needs more computational power and great energy, and IoT has limited resource and limited computational power, so blockchain is not appropriate for IoT devices [43].

(2) Issues in Cloud Services:

Organizations and different users use cloud services when they need the services. Cloud is work on a pay-as-you-use model. Users use the cloud to handle extra traffic without installing additional equipment. But the use of the cloud increases privacy and security issues. However, cryptography provides interesting solutions to various security and privacy issues [44]. In a cloud, data is saved. CSP is worried about the data integrity and privacy of data. CSP performs auditing of data with some interval and auditing the performed by third-party auditors (TPAs). TPAs performed auditing of the cloud data. They check the correctness of data; for auditing, they do not see the whole user's data, but there is a chance of losing the privacy of data.

Organizations for their financial and operational work use IT resources in the cloud. With the use of cloud services, many threats arise. To secure cloud adoption for the organization, a PaaS-based framework can be exposed as a service at the level of PaaS. This framework ensures integrity, confidentiality, and protection of data in case of an attack [45]. This framework also includes Context-Aware Security. Policies work with encryption, physical distribution, and query middle-ware [46]. CC offers several advantages, containing less IT costs, "flexibility", and "increased collaboration". But, on the other hand, there are increasingly different challenges for users and cloud service providers. Privacy can be achieved with encryption [47].

(3) Cloud Data Auditing:

Cryptographic algorithms for cloud data auditing are used that ensure the integrity and privacy of data [48]. Mobiles have limited resources, i.e., battery constraint, low computational power, low storage, etc. In this era, mobile devices have become a personal need. The power of mobiles can be increased by integrating the cloud with a mobile phone called mobile CC. All the functions are executed on the cloud, and, with few resources on mobile, users get great features, but the wireless network handles the communication between cloud and mobile. So, there is the big challenge of user data privacy and security. For data security, on Mobile CC, "distributed multi-cloud storage", "data encryption", and "data compression" are techniques that can be used. Data is divided into different parts that encrypt that data and send it to distributive multi-cloud to store huge data [49].

Many auditing mechanisms have been proposed for data confidentiality, integrity, and authenticity. For authenticity, key updating is critical, especially when digital certificates are expired. To overcome key updating, auditing the stored file on cloud zero-knowledge privacy mechanism introduced. For auditing, Sachem Water scheme and cryptographic techniques used. These techniques improve security and reduce computation and communication costs [50]. For Securing health data in transactions and access use, Learning-based Deep -Q-Network (LDQN) used. This technique prevents unauthorized access and analyzes malware activities. DLQN is efficient in terms of throughput, energy, malware

detection, lifetime, and error rate. It also minimizes error rate (0.12) and improves malware detection rate (98.79%) [51].

(4) Health Data Confidentiality Issue

In health records, personal attribute confidentiality has become a challenging task. Various techniques have been proposed to overcome this problem, like fine-grained sharing and attribute-based encryption (ABE). ABE has weak security and high computation overhead in cloud data. The partial encryption scheme is proposed, which supports online/offline validity and also reduces computation overhead. At the ad hoc MCC, assigning tasks is challenging. Server location and quality of services (QoS) are both challenging. To achieve differential privacy (DP), the R-PSD scheme was introduced, which ensures efficient location privacy and QoS. Use of a geocast mechanism overcomes search strategy [52].

With the adoption of IoT and cloud in health departments, health data is increasing daily. Managing cloud-IoT data is challenging. For efficiently managing big data, a new model has been proposed to optimize virtual machine selection (VMs). To optimize it, three different well-known optimizers are used. VMs execution time rate is 50% and retrieves data rate improved by 5.2% [53]. Exchange data is secured on the cloud using a third party. The third-party is responsible for encryption, decryption, and key exchanging. To restrict the third party, a two-layer encryption scheme applies. On the lower layer, the owner encrypts the data, while, on the upper layer, the third party applies encryption on scrambled data. This technique may be efficient in terms of computing, but it also has a single point of failure [54].

(5) IoT and Cloud Integration:

Be that as it may, a few shared points of interest from their combination have been recognized in writing. From one perspective, IoT can profit from the essentially boundless abilities and cloud-based assets to redress its mechanical requirements (e.g., capability, preparation, and vivacity). Specifically, the cloud offers a successful arrangement to execute IoT-based administration, management, and creation as the components and applications that advent the things or the information created by them. Further, the cloud is benefited by IoT in broadening out its degree of ability in managing the genuine things in a more dispersed and dynamic way, and for conveying new authorities and managements in immeasurable live circumstances [55,56].

The integration of cloud and IoT has some issues, thus needing global standards. Although mainstream researchers gave various standards of IoT and cloud standards, a reasonable need for standard conventions, models, and APIs are being requested with the end goal to encourage the interconnection among heterogeneous shrewd articles and the production of upgraded administrations, which understand the Cloud-IoT worldview: Energy-Efficient Sensing, New Protocols, Participatory Sensing, Complex Data Mining, Cloud Capabilities, and Fog Computing [57].

(6) Cellular Devices in CC:

Mobile devices, like cellular phones, are progressively turning into a necessary piece of an individual's routine life, encouraging them to play out various helpful assignments. The portable distributive computing environment coordinates versatile and cloud registration to extend their capabilities, which benefits and conquers their restrictions, for example, constrained memory, CPU power, and battery life. This research paper analyzes networked healthcare and the role of mobile CC, as well as big data analytics, in its enablement [58].

A cloudlet-based portable distributed computing framework to be utilized for social insurance huge information applications is depicted. The tools, techniques, and applications of huge information investigation are surveyed. We use a mobile phones for different purposes. The 3G and 4G technologies make our lives easier. With one click, we make purchases on the web and maintain our health through applications. In Reference [59], the author talks about organized social insurance frameworks, in addition to the job that portable distributed computing and enormous information investigation play in its enablement.

The inspiration and improvement of arranged social insurance applications and frameworks are exhibited alongside the selection of distributed computing in social insurance. Cloudlet-based mobile CC foundation is identified as a solution for healthcare big data applications. Big data analytic techniques, methods, and applications are examined. Healthcare and medical sciences applications compel vast sums, and large amounts of analytical, computational, and correspondence resources, including real-time accessibility, as well as complex access to a large amount of data, both within and outside the health care organization [60]. It emphasizes fundamental inspiration for the arrangement of healthcare frameworks where huge information, for example, understanding records, should be continuously investigated, and this can actualize effectively utilizing the cloud, as well as portable cloud frameworks [61].

Table 1 clearly shows a detailed analysis of different CC mechanisms. Achieving Integrity, Security, Privacy, and Non-Repudiation is a challenging task, with Accessibility, Portability, and Key sharing having main importance. Furthermore, the comparison between different research articles, along with their strengths and limitations, is discussed. Different authors used multiple/single access parameters (read/write/edit). Various authors have also used different data storage optimization methods. Table 1 further discusses the level of security used in different research articles. It is a clear view of the different CC infrastructure analyses used by different research articles.

2.2. Taxonomy Diagram

Figures 2 and 3 both collectively presents the taxonomy diagram that provides insight into the research classification. The independent boxes represent the name of a studied field, and the references of the studied document are provided, along with the name. Two boxes at the bottom constitute multiple boxes. Each area studied is mentioned, along with the references of papers studied.

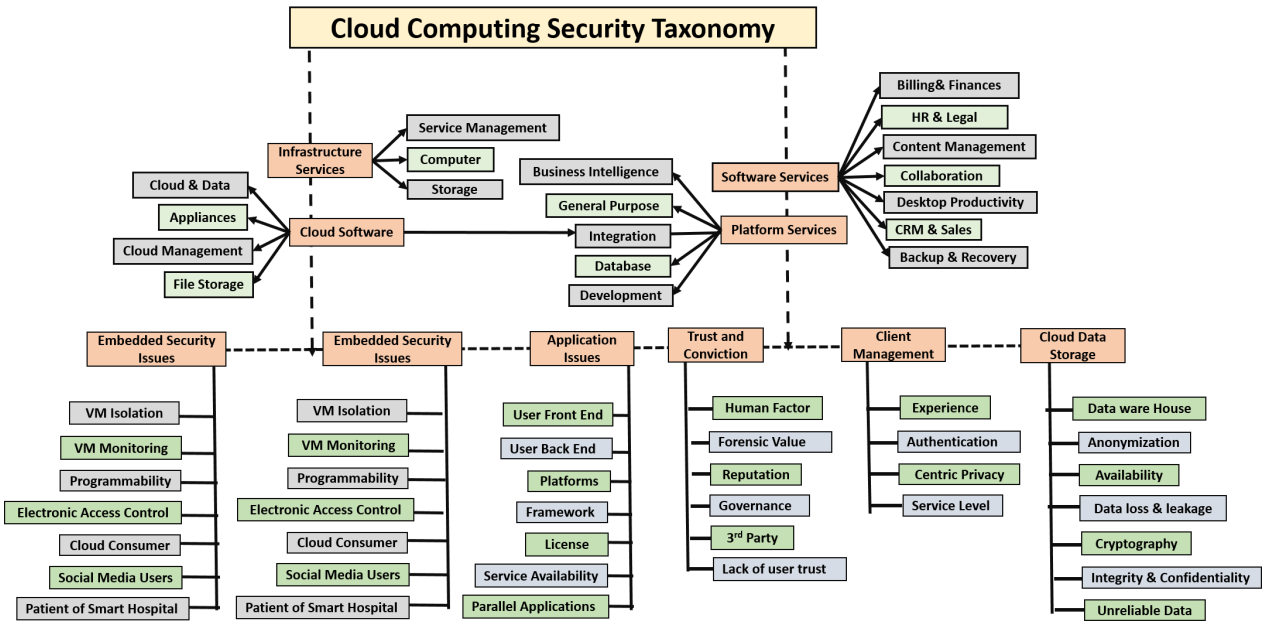

Figure 2. Classification of CC and cloud security.

Table 1. Analysis of different CC infrastructures.

Ref.	Data Storage Organization	Privacy	Data Owner	Portable	Type of Access	Techniques	Strengthens	Limitations	Confidentiality	Availability	Usability	Non-Repudiation	Integrity
[62]	EHR Cloud	Normal	Data Provider	Vary: Depends on organization	Vary	XML encryption and XML digital signature	Provides fully CIA and AAA	Limited Access Control	Yes	No	Yes	Yes	Yes
[63]	Interoperable EHR Cloud	Normal	Vary	Yes	Read/Write/Edit	RBAC, AES-256, SSO, MAC, SSL	Scalability, Interoperability	Not flexible with Access Control	No	Yes	Yes	No	Yes
[64]	PHR-based Cloud	Normal	Data Provider	Yes	Read/Write/Edit	ABAC, XML Security	An individual can control everywhere, provide integrity and confidentiality	Not implemented in real-time	Yes	Yes	Yes	Yes	Yes
[65]	Hybrid Cloud	High	Third-Party	Yes	View	ABAC, CP-ABE, K-Anonymity	Anonymize data, Fine-grained Access Control	It focuses only on who accesses the data	No	Yes	Yes	No	No
[66]	CC	Normal	User	Vary: Depends on the organization	Role-based Access Control	Attribute-based Encryption	Secure against chosen plain text attacks	Suitable for resource-limited mobile users in CC.	Yes	Yes	Yes	Yes	Yes
[67]	CSP (Hospital/Owner)	High	User	Yes	Role-based Access Control	ECDH, Digital signature	Strong against Man-in-the-middle, provides authentication	CA involve, Key generation complexity	Yes	Yes	Yes	Yes	Yes
[68]	Industrial Data Centric Cloud	High	Vary	Yes	Role-based Access Control	P2DS which contain four algorithms (SDAA, CDAA, A-SAC, and PDA)	User can access the data dynamically, provide higher level sustainability	Practically Implementation required	Yes	Yes	Yes	Yes	Yes
[69]	Medium EHR Cloud	Medium	CSP		Read/Write/Edit	CP-ABE	Provides high performance over storage and time overhead	Does not provide Non-Repudiation	No	Yes	Yes	No	Yes
[70]	Ad hoc Cloud Control	High	user	yes	Role-based Access Control	ABAC (XACML), XML Security	Provides fully CIA and AAA	Complex Access	Yes	Yes	Yes	Yes	Yes

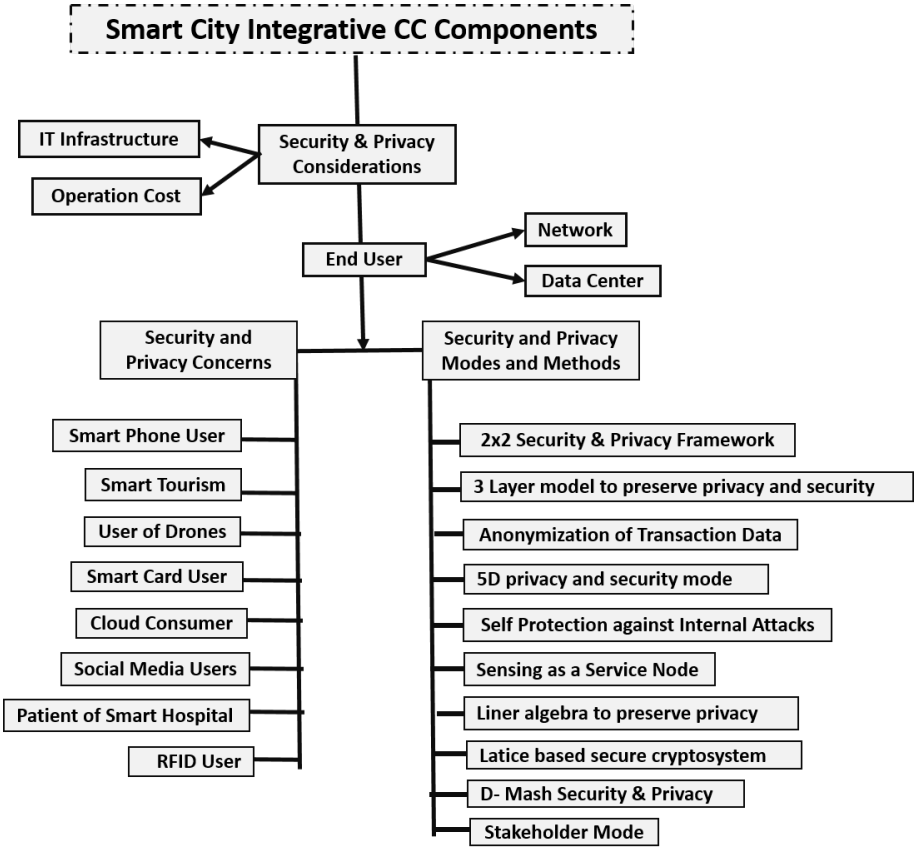

Figure 3. Classification of user-specific privacy concerns in CC domain of edge-based smart city networks.

3. CC Security: Concerns, Consequences, Challenges

3.1. CC Security

The perceived risks for CC include confidentiality, integrity, and availability as cybersecurity objectives. At the same time, cloud services are subject to local threats, as well as external ones. Similar to other ICT applications, the possible threats to CC services (including both sides, CSPs and CSCs) include but are not limited to: accidents, natural disasters, criminal organizations, hostile governments, and internal and external unauthorized and authorized cloud systems access (including intruders, employees at the CSPs, etc.). Multi-tenancy characteristics of the cloud service implementations and various cloud service models increase the risks on security and privacy of the end-users and their data.

Cloud security objectives are manifold and discussed as follows. Firstly, the Prevention of unauthorized access to CC infrastructure. This typically includes the implementation of logical separation of cloud resources (e.g., logical separation of cloud user workload on the same server in the cloud by using hypervisors in a multi-tenant environment). Secondly, the Protection of customer data from unauthorized access. This includes supporting Identity Management (IdM), so the CSCs will have a possibility to enforce policies on authorized access to their data and resources in the cloud. Thirdly, the Protection from threats from hardware and software used on the CSP or CSC side, including trustworthiness and reliability of the software and hardware. Fourthly, the implementation of security solutions into the design of Web applications for access to cloud resources. For example, the use of SSL/TLS, certificates, etc. [71].

Fifthly, the Protection of Web servers from attacks with the installation of Firewalls between the public Internet and cloud servers in data centers, applying patches to the software in use, etc. Sixth, the Deployment of access control and intrusion detection systems at the CSP. It includes restriction of physical access (of people, including unauthorized employees) to network and devices, disabling unused ports and services, applying for role-based access, minimizing the use of privileges, mandatory use of antivirus software,

and encryption of the end-to-end communication. Seventh, the precise definition of responsibilities regarding the security measures between the CSPs and CSCs. Finally, the Portability of the cloud solutions aiming to provide a possibility to the CSC to change the CSP when the provider fails to satisfy the requirements on confidentiality, availability, and integrity. Figure 4 essentially illustrates the key objectives and aspects of CC security [72].

Security solutions applied in the cloud services by the CSP may create differentiation in the cloud service offerings to customers, which may lead to price differentiation between different service packages offered to different types of CSCs (business, individual, etc.) [73]. Several laws apply to CC, which is country-specific, including telecommunication law, consumer protection law, competition law, and regulations on environmental and jurisdictional concerns. Certain cloud services (e.g., NaaS, CaaS) can fall directly into the regulated sphere of telecommunications regarding networks and services. OTT cloud services (e.g., SaaS, PaaS) provided through public access to the Internet (based on the network-neutral principle) are not treated as separate telecommunication services [74].

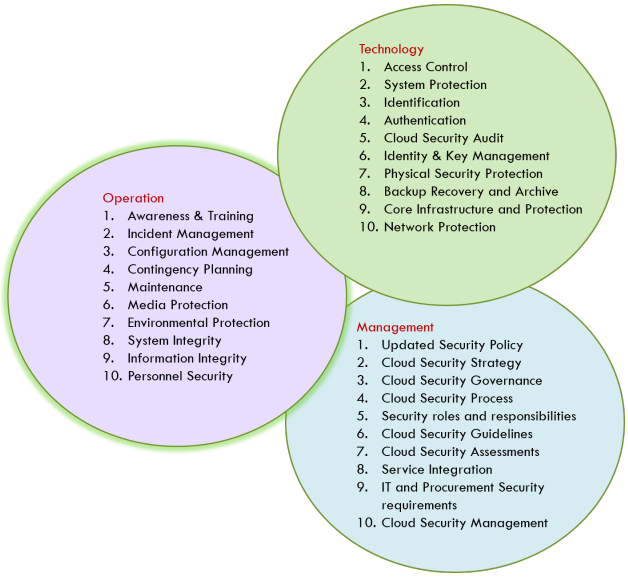

Figure 4. CC security aspects.

3.2. Attacks, Threats, Concerns, Consequences, and Challenges

In CC, with variations of underlying technologies, like IoT, Cloud of Things (CoT), and smart city networks, it is prone to suspect and face various security and privacy threats. Those circumstances and consequences include, by default, the hard-coded and weak credentials (e.g., in web cameras), difficulties to update firmware, and Operating Systems (e.g., in sensors) in the prevailing systems, lack of vendor's support for repairing, rectifying, and removing the vulnerabilities, vulnerabilities regarding the Web interfaces and GUIs over the inter/intra connected networks, encoding, coding, and, subsequently, the decoding errors (e.g., buffer overflow), plain or clear text transfer protocols (no ciphering/encoding/hashing) and presence of the unnecessary and unwanted open ports and sockets, DoS (Denial of Service) and Distributed DoS sensitivities and ↘ Physical theft or damage (it may happen to all physical things, not only limited to the IoT, CoT devices), and Ethical hacking and hijacking of presently installed systems (e.g., automobile control systems); in addition, Reconnaissance, Surveillance, Monitoring, and Interception of the data from unauthorized and unwanted modifications or changes (e.g., to automated healthcare delivery mechanisms, to automated inter-banking transactions) in them are considered [75].

Various security problems stem from a loss of control, lack of trust (mechanisms), and multi-tenancy that exist mainly in 3rd party management models. Finally, the self-managed clouds still have security, privacy, and trust issues that are not related to the

aforementioned security issues, and all these security issues and concerns are elaborated in the preceding paragraph. Over the cloud, the loss of the control is manifested as the consumer's loss of control, along with data, tools, applications, and resources distributed over the cloud located with the cloud service providers. Cloud service performs handling and management of user identity management, user's access control rules, security policies, and further enforcement. Consumers rely on the cloud service providers for assured security and privacy of data, resource availability, monitoring, and repairing of services and resources. In the cloud, lack of trust is manifested in a variety of ways. Putting faith in a third party necessitates taking risks. Defining the terms "confidence" and "risk", people believe, when it costs (J. Camp), they are two sides of the same coin (Economists view).

Trust is only required in high-risk circumstances, such as failed third-party management schemes. It is challenging to strike a balance between confidence and risk, as with Key Escrow (Clipper chip), and there is also the question of whether the cloud is on the same track [76]. The tension between tenants opposing goals was highlighted in the multi-tenancy issues in the cloud. Consumers or the Tenants share a pool of resources and have competing goals; how does multi-tenancy cope with conflict of interest, such as if tenants get along and play well together, and, if not, do we need to separate them by offering separation between consumers [77]? Theoretically, key security and privacy issues in the cloud can be summarized as loss of control and take back control, data and apps may still need to be on the cloud provided they can be managed in some way by the consumer, lack of trust, which can be increased by applying trust (mechanisms), technology, policy, regulation, contracts (incentives) topic of a future talk, multi-tenancy, and private cloud which takes away the reasons to use a cloud in the first place, and VPC which is yet not a separate system and strong separation.

3.3. Countermeasures against Security Threats and Attacks

The end-to-end security solutions between the CSP and CSC include specific Internet security solutions, such as SSL/TLS (e.g., HTTPS) or VPN access to the cloud (with IPsec). Another possibility for application layer security mechanism is the use of PKI (Public Key Infrastructure) mechanisms for the cloud [78]. Consumer-managed access control requires less trust in the CSP. In this case, Policy Decision Point (PDP) is in the CSC domain and Policy Enforcement Point (PEP) belongs to the CSP domain. Theoretically, the steps should be as minimizing the lack of security, privacy, and trust policy language, loss of control monitoring, lack of trust certification, loss of control utilizing different clouds, multi-tenancy in the cloud, etc. [79].

Minimizing the deficiency of security, privacy, and trust policy language is emphasized by consumers who have clear protection and security demands, so they do not have a voice or a say in how they have to meet them; this is where the position of the vendor or the cloud service provides comes in Reference [80]. At the moment, consumers cannot tell the service provider what they want (SLAs are one-sided). To communicate one's policies and goals, a standard policy statement is desired. All sides have agreed to that, and it has been upheld [81]. SLAs are represented using a standard vocabulary. It can be used to achieve an overarching security posture in an intra-cloud environment, creating policy statements that include major features, like a machine that is understandable (or at least process-able) [82].

It is easy to merge, integrate, and compare; still, there is a need for developing separation among VMs, requiring geographical isolation between VMs, and so on, are the various examples of various policy statements. Likewise, there is a need for a validation tool to check that the policy created in the standard language correctly reflects the policy creator's intentions (i.e., that the policy language is semantically equivalent to the users' intentions) [83]. Curtailing the lack of trust certification includes certification or some form of reliable, autonomous, comparative assessment and detailed description of security features and assurance, Sarbanes-Oxley, DIACApP, DISTCAP, etc. (are they sufficient for

a cloud environment?), and 3rd party-based certified risk assessment gives additional assurance to cloud consumers [84].

Reducing the loss of control within the cloud includes the utilization of distinct cloud networks, analysis, monitoring, and management of access control [85]. Therefore, minimizing the loss of control in monitoring consists of situational awareness for the critical applications for the consumers of cloud services. In case of failure of underlying components, what is the effect of the failure on the presumed logical mission, and what would be the recovery measures taken by the consumers and the service providers that involve real-time monitoring and management tools for the cloud services customers specific to the application in use [86]?

The consumer and services provider have diverse system views in the cloud that enable them to monitor and access the components under their control. The cloud environment provides the mechanisms which enable the service providers to act over the attacks subject component capable to handle [77], in addition to remapping of the infrastructure in new or existing fault domains, and shutting down the aberrant components or targets in assisting consumers with porting if required the repairs and maintenance. Further, cloud enables the consumers to provide adaptive VM porting with remote attestation of target physical host network or machines, along with the ability to migrate the users' application to another cloud environment [80].

Minimizing the loss of control and multi-latency utilizing various cloud models and underlying network technologies includes the concept of not giving all authority to one domain or one controller; consumers prefer to use services from distinct clouds through an intra-cloud or multi-cloud architectures, while proposing such a risk is spread to accommodate and increase redundancy (per-task or per-application) among customers [87]. Increase the chance of mission completion for critical applications. In addition, the possible issues to consider, like policy incompatibility in combination with overarching policy, data dependency between cloud components, differing data semantics across clouds, knowing when to utilize the redundancy feature (monitoring technology), whether it is required to spread your sensitive data across multiple clouds, and redundancy, could increase risk of exposure [88].

Reducing the loss of control and access control includes and highlights access to the cloud, access to servers, access to services, access to databases (direct and queries through web services), access to VMs, and access to objects within a VM, which are all potential as layers of access control [85]. Some of these will be managed by the service provider, while the user or consumer will control others, depending on the implementation model. Furthermore, the provider must manage user authentication and access control procedures regardless of the implementation model to the cloud. Service providers also bear the responsibility of access control management in Federated Identity Management, which allows a user to place a high level of protection, privacy, and trust on the service provider in terms of access control policy's security, management, and maintenance [78].

When several users from various organizations with different access management policies are involved, it may be challenging. Consumer-managed access control and decision-making maintain control, requiring less provider trust (i.e., PDP is in the consumer's domain). Furthermore, a pre-existing trust relationship between client and cloud service provider is required, as well as a pre-negotiated standard way of describing, nominating, and allocating resources, users, and access decisions among cloud service providers and consumers [89]. It is vital to ensure that the cloud service provider credits the consumer's degree of access decision. It should be at least as secure as the standard access control model. Facebook and Google Apps both do this to some extent, but not nearly enough when it comes to the protection of patient health records [81].

Aggregate and localized host security initiatives are applications to visualize and accommodate the local host machines making part of the cloud infrastructure being outside the security perimeter [82], whereas cloud consumers are concerned over security, privacy, and trust on the cloud provider's sites, where they might forget the hardening of their

machines. Due to the lack of security on the local devices, malicious cloud providers could target local networks using these terminal devices. As a result, the possibility of compromising the cloud and its services for other users of mobile devices could be even greater.

Security mechanisms on mobile devices are frequently ineffective when opposed to, say, a desktop computer. Users misplace or have the device stolen from them. This initiative gives a possible intruder a simple way into a cloud system if a user depends on a mobile device to access cloud data. When mobile devices fail or are lost, the possibility of data loss increases [90]. Similarly, devices that connect to the cloud should have strong authentication and tamper-resistant mechanisms to establish strong separation between applications, trust methods for the operating system, and cryptographic functionality when traffic confidentiality is necessary.

3.4. CC Security Prospects in the Future Networks

Future networks should be developed and conceptualize for the safety and privacy of their end-users. The rationale for this lies in the targeted use of future networks in human society including mission-critical services, such as: ↘ intelligent landline, railway, and air traffic management, eHealth, emergency telecommunications, reliable services in disaster conditions, etc. On the contrary, security for further networks can be provided by using multi-level access control, that is, assurance of user identification, authentication, and authorization, which is in addition to the security requirements of the NGN. For example, network virtualization will bring many benefits to all actors, including providers and end-users, but it also raises new security threats. For example, a malicious user can monitor or control virtual resources even in cases when they are not allocated to that user [83].

3.5. Aggregate / Comprehensive CC Challenges

Various challenges can be summarized in three categories.

- Cloud Service Customers: These are the ambiguity in responsibilities, loss, and lack of trust, security and privacy, service unavailability, cloud service provider lock-in, misappropriation of the sensitive and intellectual data and property, loss of governing body, control, and software integrity
- Cloud Service Providers: Uncertainty in management, responsibility, and administration in shared cloud environments, inconsistency and conflict in security and data protection measures, jurisdictional conflicts, evolutionary risks, bad and worst process migration, integration, discontinuity in business, cloud service partner lock-in, supply chain vulnerability, software dependencies.
- Cloud Service Partners: These are ambiguities in responsibilities, monitoring, regulation, and misappropriation and forger ring of the intellectual property.

4. Security & Privacy Concerns in Cloud-Based Smart City Networks

4.1. Why Is Security & Privacy a concern in CC-Based Smart City?

The question of privacy concerns in the smart city has come into the picture since information and communication technology (ICT) developments have drastically increased. An integrative framework has been proposed in Reference [84] by Chourabi et al. to understand a smart city. The authors discuss eight factors that characterize a smart city. One of these factors is built infrastructure. In this domain, one of the technological barriers in e-government is privacy and security. The challenges in this dimension are threats from intruders, hackers, worms, Trojans, personal data privacy, and the cost of the solutions to provide security against all these. With the expansion of ICT, information flows have drastically increased, and, with this expansion in information flows, threats to information privacy have become a point of concern. In Reference [91], the author argues on the three potential threats to personal privacy that have been posed by smart cities: IoT, big data, and cloud.

As a case study to justify and correlate security objectives discussed in Section 3.1, the two cybersecurity approaches based upon privacy, security, and trust are to be discussed to testify how these objectives are mapped with the cardinals of security and privacy under the study domain. Secure Framework for Future Smart Cities (SEFSCITY) [92] is based on CC-based infrastructure, where IoT-based devices perform secure data transformation over IoT-based applications and a distributed computational model. Scholars in this paper proposed an architecture based upon multi-cloud and cloud federation approach, and then they proposed framework for implementing security and privacy protocol. It utilizes the Zero knowledge protocol, which is based upon Elliptic Curve Discrete Logarithm Problem employed in the security model. Security protocol allows mutual authentication among a CSP and CUs. In another case scenario, Nandita Sengupta [93,94] talks about cyber security in cloud-based smart cities. A two-phase cyber security system is designed for cloud-based smart cities in phases. In the first phase, the hybrid encryption is used, and, in second phase, the machine learning is used for intrusion detection to complete the cyber security system for IoT-based devices in smart city networks. The framework combines the two phases of security system with IDS and cryptography to make the employed environment smart and secure. Both these approaches ensure confidentiality, integrity, availability, non-repudiation, and usability in the data transactions.

4.2. Consequences of Security and Privacy Concerns in Smart City Networks over CC

(1) Bluetooth Technology:

Bluetooth technology has penetrated many devices, such as smartphones, navigation systems, hands-free sets in cars, etc. Bluetooth devices emit signals and readers of these signals can be placed at different locations, and devices' movement can be monitored. Digital forgetting is an IoT domain of research in these privacy concerns [79].

(2) Health Sector:

The privacy of a patient's health data is very important because a patient may face serious problems if their health information is disclosed and misused [80]. In this study, the authors have enlightened the fact that training in handling patient data must be provided to ensure privacy, but these training programs fade away when it comes to the importance and effectiveness of the use of security algorithms for access control, anonymity, and authentication.

(3) Big Data Analytic:

The widespread participation of all citizens makes the network-based smart city successful, but privacy concerns are a challenge to this achievement [52]. When research is carried out on big data analytic to characterize the trajectories followed by humans, privacy is a concern when data is not anonymous [81]. Such research data must be anonymized through analysis and confidentiality.

(4) Cloud Security System:

In Reference [82], the privacy attribute of a security service is termed as preserving privacy. In a cloud system, outsourcing makes the consumers lose control of their data. The authors have shown privacy as a separate attribute from security revealing its importance and understanding as a separate entity. Guaranteeing the confidentiality of user data in the cloud is required for privacy preservation [14]. It has been discussed that, even if the data is encrypted, critical information about the raw data can be revealed by the access patterns that each corresponding application exhibits. Not only should the encrypted data be unintelligent to unauthorized, but it should also hide the statistical properties of original data. Although cloud storage is a resource that facilitates the collection and mining of data due to integrating big data with cloud storage, this integration is a threat to privacy due to the involvement of a third party. And what if a security breach occurs, would the cloud service be fully accountable? Thus, it is a challenge to share the responsibility of data sharing with the government [83].

(5) IoT:

Privacy concerns in IoT at different layers, like the front end, back end, and network, have been summarized in Reference [84]. An entity's privacy needs to be protected at different stages, i.e., in a device, storage, processing, and communication.

(6) Smart Card:

Smart card provides an easy to use way of gaining a service. Smart card consolidation with the advancements towards the improved smart city has been discussed in Reference [2]. Many cities are now launching contact-less smart cards, but, with this gradual development in smart card technology, privacy concerns arise.

(7) Smart Tourism:

Current trends in smart tourism have been discussed in Reference [8]. One of the drawbacks of smart tourism is the lack of privacy protection. The location-based services provided by smart tourism, on one hand, are very useful for tourists, but, on the other end, they make the consumers vulnerable to privacy threats. The digital footprints of a traveler make it possible to perform data mining on the digital traces and exploit the privacy of information.

(8) Drones:

In the future, smart city drones (edge and CC-based nodes) are going to play a major role in goods transportation, mobile hot spots, and maintenance of security and surveillance of smart cities [9]. The use of drones also brings challenges and concerns about privacy. This paper presents the results of cyber-attacks using drones. This implies that drones are vulnerable to cyber-attacks and can be used in harmful and malicious ways to launch cyber-attacks. In DEFCON 21 [10], a DJI phantom mounted with a Wi-Fi pineapple was used by a researcher to sniff wireless signals using a virtual private network. The cost of drones is falling; therefore, UAVs are being launched in any territory for constant monitoring of that area. They can also cause danger to aircraft as in the near-collision incident of Boeing 737 in British airport [11].

(9) Mobile Applications:

The privacy concerns linked to the actual online behavior of users have been analyzed in Reference [85]. In the systematic literature review in this paper, the authors have used the privacy paradox to explore different theories. The majority of papers studied by the authors focused on online media and social networks in the context of privacy paradox, but, when compared with the results, it comes up that the privacy paradox is even more complex in the context of mobile applications. An individual can restrict his/her profile on a social networking website to protect their data from intrusions and other security threats, but there are no such measures of protection available while downloading and during installation of mobile applications.

(10) E-Governance:

In Reference [86], the authors have discussed privacy concerns in E-governance. The design of a smart building has control systems that include water heaters and coolers, light and motion sensors, escalators, etc. These control systems interconnect with other systems, hence increasing the security and privacy concerns. The E-Government sector is facing challenges of privacy, trust, and availability.

(11) Online Social Networks:

The study carried out by authors in Reference [77] reveals how smart cities are affected by the risks associated with online social networks (OSN). An individual's privacy on an OSN consists of the individual's privacy of identity anonymity, personal space, and communication. Privacy concerns will certainly arise with the use of individual data.

(12) Bio-metrics:

Bio-metrics technology must be integrated into social media to authenticate individuals. Bio-metrics technology is used for identity verification and, hence, protects the privacy of the entity.

4.3. Attacks, Threats, and Vulnerabilities in CC-Based Smart City Network

Smart city network generates huge amounts of data and involved devices and processes are spread over a larger geographic area. Extraction, filtering, serialization, mining, and analysis of smart city huge data is challenging and requires a lot of human and material resources [34]. It is challenging to establish proper convergence and mapping of networking parameters among different layers of OSI model network stack over various data generation peers, like servers, gateways, workstations, sensors, accumulators, smart devices, and routers [71].

In smart city networks, the data transmission is susceptible to confront several attacks, such as cross-site scripting and side-channels, and its multi-latency can cause data leakage [22]. In smart city networks, due to the involvement of the smart grid over sensitive data, there is a dire need for high level security in all over the infrastructure. Security is the major challenge in achieving the accountable, reliable and consistent communication over the smart city networks [36,50].

Likewise, Robust network management in the cloud computing for smart city networks is the major challenge to tackle services delays, data loss during mining, lack of communication links with every node in centralized and distributive cloud computing, transmission delays, lost packets, and unstable connections, localized transmission, low latency, and low mobility services. Fog computing is introduced to overcome issues in cloud computing but there are still issues, like demand for robust and efficient communication links, exclusive and specialized network planning and management, and network security support and its integration, till each tier [24,33].

CC is a hot topic in the current era. After studying most research articles, we convexed the identified challenges of the smart city over CC in Table 2. Table 2 illustrates the identified threats and challenges to the CC domain in the smart city networks and the compromised security attributes related to the CIA triad [74]. Furthermore, the different authors have resolved many issues in their article work; however, they have not achieved some of the most important aspects. Most of the authors in Table 2 compromised on the integrity and confidentiality, which is the most important factor for the challenges, like IP Spooling, DDOS attack, phishing attack, backdoor, social engineering, Trojan horses and malware (ransomware), etc. The complete challenges, along with their description and author details, are enlisted in Table 2.

4.4. Countermeasures for Security & Privacy Concerns

(1) Sensing as a service model:

Sensing has been introduced as a service model in Reference [22]. The smart city and IoT have different origins, but the sensors make them move into each other. To preserve the privacy of sensor data, the sensor owner can define restrictions, such as who can access what data. In addition, sensitive information collected by sensors, such as location data, needs to be altered implicitly to anonymize the data.

(2) 5D model for privacy:

In Reference [26], Antoni Martínez-Ballesté et al. identify some privacy breaches in the context of smart cities. The concept of a smart city presents the citizen's privacy in the form of a model. A 5D model for the privacy of a smart city is proposed in the research. The five dimensions are identity, query, location, footprint, and owner.

(3) User Awareness:

In Reference [80], privacy protection mechanisms have been discussed. Prerequisites to the distribution of data are user awareness and consent.

(4) Security and Privacy protection in RFID:

Privacy protection in the RFID systems requires both physical and cryptographic mechanisms [23]. With the help of physical mechanisms, like kill code, Faraday's cage, and blocker tag, tags can be blocked and disabled when not in use. Cryptographic mechanisms have been proposed that help reducing the privacy risks. The proposed cryptographic mechanisms are hash lock, randomized id, efficient identification, and encryption.

Table 2. List of identified challenges in smart city over CC.

S.No	Ref	Challenges	Description	Compromised	S.No	Ref	Challenges	Description	Compromised Attributes
1	[23,31]	WS-Security	A significant specification which addresses the security for Web Services.	Integrity, Confidentiality	21	[23,33,70,73]	Physical security	The risk and basic fact that individuals or natural disasters may target the hardware components, regardless of the level of internal software and policy protection implemented.	Security, availability, non-repudiation
2	[67,73]	Phishing attack	The attacker's risk is that the victim will be sent to a bogus Web page (either through spoofed emails or DNS assaults) where they will be asked to enter their login credentials.	Confidentiality	22	[8,15,34,73]	WLANs security	Due to risk of WLAN openness, several security vulnerabilities, such as network eavesdropping, identity theft, and message manipulation, have become more prevalent.	Usability, Non-repudiation
3	[69]	Wrapping attack	Risk of utilizing XML-based signature for authentication or integrity protection.	Integrity Authentication	23	[44,70,77]	Direct attacking method	It deciphers the cipher text immediately rather than attempting to crack the encryption key.	Confidentiality
4	[10,16,85]	Injection Attack	Injecting a malicious service implementation or virtual machine into the cloud system is the goal.	Availability	24	[51,57,82]	Replay attack	A replay attack is a type of an assault on the network where a lawful data transaction is replayed or delayed deliberately or fraudulently.	Integrity
5	[10]	IP Spoofing	Risk of utilizing another person's authentication information, such as their user name and password, without permission.	Confidentiality	25	[31,73]	Man-in-the middle attack	It is a type of active eavesdropping in which the attacker establishes separate connections with the victims and passes communications back and forth between them.	Availability, Non-repudiation, Integrity
6	[44]	Tampering	Unauthorized tampering of permanent data or data transmission via a network.	Integrity	26	[34,42,53]	Reflection attack	It is a technique for breaking into a challenge response authentication system that use the same protocol in both ways.	Confidentiality, Non-repudiation

Table 2. *Cont.*

S.No	Ref	Challenges	Description	Compromised	S.No	Ref	Challenges	Description	Compromised Attributes
7	[37,42]	Repudiation	The possibility that a user may carry out an unlawful action in a system that lacks the capacity to track it down.	Audit ability	27	[91,92]	Interleaving attack	These attacks are alike man-in-the-middle attacks, except they can target protocols where all parties hold legitimate copies of each other's public keys.	Integrity, Confidentiality, Non-repudiation
8	[41]	Information Disclosure	User of a cloud access and reads a file without permission from a co-tenants workflow.	Confidentiality	28	[16,61]	Timeliness attack	Danger of not having a deadline is that the protocol will not know when the step is finished, which might cause issues.	Usability, Availability
9	[73]	Denial of Service	An adversary gains control of a tenant's VM and makes another's web server unavailable.	Availability	29	[14,60,73]	Self-adaptive storage resource management	Sensitive data which is under constant monitoring is required to be kept optimized, and application of dynamic control for the big size data specially during transactions on connection oriented media, scheduling of the transfer of data, scheduling for distribution and prediction matrix for performance over remotely access storage services.	Integrity, Confidentiality
10	[70]	Elevation of Privilege	An attacker bypasses all system protections in order to get access to the trusted system.	Confidentiality	30	[3,10,62]	Client monitoring and security	The storage service must be aware of the various client types and their access privileges.	Security, Availability, Non-repudiation
11	[75]	Lack of trust	Customers are becoming more discerning as the number of Cloud service providers grows. Finding it difficult to choose the finest and most suited suppliers from a numerous options.	Confidentiality	31	[25,70,73,83]	Completeness	To the fact that a data service provider must supply a user with all the entitled or authorized information to give access based on the allotted authorizations.	Availability, Usability, Non-repudiation

Table 2. *Cont.*

S.No	Ref	Challenges	Description	Compromised	S.No	Ref	Challenges	Description	Compromised Attributes
12	[42,62]	Weak Service Level Agreements (SLAs)	Vendor lock-in, weak security measures, data unavailability, hidden expenses, and nontransparent infrastructure may cause difficulties for consumers.	Availability, Confidentiality, Non-repudiation	32	[70]	Roll back attack	Data owner when updates the information to the new version then the malevolent service provider continues the supply of previous version to the user.	Availability, Usability
13	[42]	Perceived Lack of Reliability	Risk of not having clear information about whether availability is for a single server where a customer's virtual instance sits or for all servers located in data centers across the world.	Availability	33	[80,85]	Fairness	In order to acquire specific benefits throughout the data transmission operation, a malicious party may refuse to respond after obtaining evidence from another peer.	Confidentiality, Non-repudiation
14	[49]	Auditing	It is the process of analyzing and scrutinizing authorization and authentication records to see if they meet preset security standards and rules [50].	Security, Confidentiality	34	[56,64,72]	Data Loss or Leakage	A provider may keep additional copies of the data in an unethical manner in order to sell it to interested third parties.	Availability, Non-repudiation
15	[41,42]	Back-Door	It is a method of gaining access to a network by circumventing the network's control systems and entering through a "back door", such as a modem.	Usability	35	[50,52,64]	Computer Network Attack (CAN)	It is defined as Information disruption, denial, degradation, or destruction operations are described as activities that disrupt, deny, degrade, or destroy information. Computers and computer networks, as well as the computers and networks themselves, have residents.	Integrity, Confidentiality, Usability

Table 2. *Cont.*

S.No	Ref	Challenges	Description	Compromised	S.No	Ref	Challenges	Description	Compromised Attributes
16	[73]	TCP Hijacking	The attacker computer replaces the trusted client's IP address with its own, and the server continues the conversation as if it were with the trustworthy client.	Confidentiality, Integrity	36	[61,73,77]	Denial of service attack	The system's availability is destroyed.	Availability, Non-repudiation
17	[77,90]	Social Engineering	In this attack, social skills are used to acquire information, such as login credentials, like PIN numbers, which are to be used against the information systems.	Confidentiality	37	[35,36]	Data Security	Each enterprise's sensitive data remains within the enterprise's perimeter, subject to its physical, logical, and human security and access control regulations.	Security, Availability, Non-repudiation
18	[84,85]	Dumpster Diving	The act of obtaining information that has been abandoned by a person or organization.	Availability	38	[10,14]	Network Security	To avoid the loss of critical information, all data flow over the network must be protected and breach of information to be deprived.	Integrity, Usability, Security
19	[33,70,84]	Password Guessing	It is the most prevalent method of user authentication. Getting passwords is a popular and efficient attack strategy.	Confidentiality	39	[63,70]	Data locality	The possibility that the consumer is unaware of where his or her data is being stored.	Reliability, Usability
20	[55,78]	Trojan Horses and Malware	They conceal harmful code within a host software that appears to be beneficial.	Usability, Availability	40	[52,74]	Data integrity	Transactions across numerous data sources must be handled appropriately and in a fail safe manner in a distributed system to guarantee data integrity.	Integrity

(5) Data Aggregation:

Data aggregation is another means to protect the individual's privacy [87]. Application-specific data analysis can be performed in a cloud.

(6) Stakeholder model:

Security and privacy framework proposed by Zareen Khan et al. propose a stakeholder model of a smart city in which privacy aspects are dealt with according to the stakeholder's viewpoint [35]. User consent acquisition, freedom of choice and control, and anonymity technology are sources of preserving privacy [88]. Major stakeholders that are responsible for user privacy protection are individual consumers and non-consumers, device manufacturers, IoT cloud services and platform providers, third-party application developers, and government and regulatory bodies.

(7) 2×2 Framework:

A 2×2 framework proposed in Reference [5] hypothesizes which technologies and data applications are likely to raise the concerns of privacy. The four types of sensitivities people have about their data are represented as a 2×2 framework. These four dimensions are personal data for service purposes, personal data for surveillance purposes, impersonal data for surveillance purposes, and impersonal data for service purposes. The authors have explained how an innocent technology can be transformed into a sensitive one.

(8) Mobile Cloud Framework:

Data over-collection in smartphones has become a big cause of privacy leakage [6]. Data over-collection means that apps in smartphones collect more user data than their capacity. The authors have presented cases of data over-collection in smartphones, and a framework of mobile-cloud is presented that is a proposed scheme for data over-collection eradication.

(9) Changing Pseudonyms in Intelligent Transport System:

In an intelligent transport system, there is information of start and endpoints [85], and this may be required by an attacker to keep the vehicle track record for some malicious intention. A proposed solution to this issue is provided in Reference [78], where pseudonyms have to be changed frequently for the solution of location privacy.

(10) Homomorphic Encryption:

Homomorphic encryption is a very good solution in the e-health sector that provides privacy protection to patient's health data maintained in the cloud [89].

(11) 3-layer model:

The authors of Reference [39] have proposed the where, who, what model for location-based services. A three-layer model proposed in Reference [40], protects user privacy and introduces user-friendly systems.

(12) Linear Algebra:

The authors of Reference [38] have proposed a solution based on linear algebra. They have proposed two-party protocols and compute inner products, determinants, eigenvalues, and eigenvectors. These protocols produce the output results, while the privacy of the inputs is preserved.

(13) Continuous Streaming Data:

The traditional security technologies are not sufficient in the management of dynamic nature data; they can only deal with static data. It is a challenge to ensure privacy in continuously streaming data due to a large amount of data generation [81].

(14) Protection of DBMS from insider's attacks:

Database management systems can be secured from outside threats by the use of firewalls, password mechanism, penetration testing, etc., but the insider's intent is difficult to monitor [33]. The authors in this paper have provided a solution of self-protection against insider attacks through the implementation of policies. The authors enforce access control, encryption, and database auditing in their proposed model. The reason for enforcing these policies is to protect the database management system from malicious insider attacks.

(15) Anonymization of Transaction Data:

The transaction logs stored in a medium have many levels. An IT manager gets an insight into data that moves between levels. The authors in Reference [41] have proposed a novel techniques-based approach in which anonymized transaction data can be analyzed by the mining tools.

(16) D-Mash Model:

Due to its advantages, data as a service (DaaS) is an emerging area in the field of research [82]. Enterprises do not opt for DaaS because of the two threats linked to it: the threat of hackers and the threat of data privacy compromise. To prevent privacy leakage, one of the proposed privacy models is D-Mash. This is also known as data mash-up. By the virtue of this model, the data providers are enabled to integrate their relevant data on demand, while preserving data privacy [90].

(17) Lattice-based secure cryptosystem:

This system is proposed for healthcare in smart cities in Reference [83,84]. The authors have proposed a model for communication between doctors and patients and the cloud. The scheme is designed for constrained nodes of smart cities and works efficiently due to low computation and communication costs as compared to other schemes presently in use.

4.5. Tabular Analysis and Methodology Representations

The research carried out is summarized in two tables. Table 3 provides the list of smart city technologies and the privacy leakage consequences of each technology. It also illustrates the technology used by different authors, along with the security privacy concerns. Furthermore, recommendations and comments for different papers are also described in Table 3.

Table 4 enlists the studied models, frameworks, and methods that provide counter-measures of consequences, threats, vulnerabilities, and challenges of CC-based smart city networks discussed in Table 2. Different models, like the 2 × 2 framework, anonymized transaction techniques, privacy-preserving D-Mash, Stakeholder model, etc., are used by different authors. The purpose of using those models is to ensure security and privacy protection and enforce policies for access control, data privacy concerns, and encryption. Some framework is proposed by authors, which provide the practical solution to data privacy, privacy invasion, transportation of information, and effectively sharing the information. The detailed description of many methods/techniques proposed by many authors is described in Table 4.

Table 3. CC-based smart city technologies and security and privacy concerns.

Paper Reference	Technology	Security/Privacy Concerns	Recommendations /Comments
[1,2]	Radio frequency Identification (RFID)	Data from multiple RFID readers can be correlated to reveal the movement and social interactions of individuals.	Physical mechanisms can disable the RFID when not in use and cryptographic mechanisms can reduce privacy leakage and security breach risks when RFID is in use.
[5,6]	Intelligent Transport System (ITS)	The issue in this system is that an attacker can keep the vehicle track record.	Solution proposed is to change pseudonyms frequently for protecting location privacy.
[2]	Smart Card (SC)	This gradual development in SC technology has raised the threat of privacy leakage.	With the advancements in ICT, smart cards are also coming in newer and more advance versions as contact less SC.
[8]	Smart Tourism (ST)	The location-based services make the consumers vulnerable to privacy threats.	Information governance and privacy are the suggested major areas of research.
[9–11]	Drone Technology (DT)	Drones are not only prone to cyber-attacks but also they can be used to launch cyber-attacks. Their falling costs are making their use possible in malicious attempts.	Research is needed in order to not only make drones secure against security and privacy attacks but also they must not be able to be used in malicious intentions.
[6]	Smart Phones (SP)	Data over-collection in smart phones makes them vulnerable to privacy attacks.	A mobile cloud framework is presented to solve data over-collection problem.
[14,15]	Cloud Technology (CT)	The integration of big data with cloud storage is a threat to privacy due to the involvement of a third party. Data accountability is the problem in cloud services.	It is a challenge to share the responsibility of data sharing with the government.

Table 4. Security and privacy protection models and frameworks.

Reference Number	Model/ Method / Framework	Main Function / Purpose	Details
[22]	Sensing as a Service	Smart city and Internet of things are from different origin but sensors make them move into each other.	In this model, sensor data privacy is preserved if sensor owner defines restrictions to access.
[26]	5D model for privacy in smart cities	The proposed model has the quality of preserving privacy in the 5 dimensions; identity, query, footprint, owner, location.	This model is based on the proper handling of coexistent domains and secures transportation of information.
[5]	2 × 2 framework	The four types of sensitivities that people have about their data are represented as a 2 × 2 framework.	This framework is used to hypothesize if the smart city technologies provide privacy concern among citizens of the smart city.
[33]	Self-Protection Against Insider Attacks	Self-protection model of database management systems against insider's attacks is provided.	The self-protection model proposed by authors enforces the implementation of policies for access control, encryption, and database auditing.
[35]	Stake-holder model	The authors presented a framework based on the stakeholder model for providing secure and privacy aware services in smart cities.	Smart city is essentially comprised of citizens from different cadres and having different point of views. This model brings forth the necessity of dealing the aspects of data security and privacy from the point of view of different stakeholders.
[36]	A framework for privacy preserving D-Mash	To fulfill the request of a consumer, mashing the data from different sources is carried out. This involves the risk of revealing sensitive information of users.	The proposed DaaS mash up framework is an effective solution to data privacy concerns.
[38]	Linear algebra to preserve privacy	Privacy preserving of distributed data.	The proposed protocols are computationally efficient. Privacy invasion is protected.
[39,40]	A three-layer model of user privacy concerns	Guidelines have been developed for the construction of privacy-friendly systems.	Two approaches are distinguished: privacy by policy and privacy by architecture.
[41]	Anonymized transaction techniques	Raw data can be a cause of identity theft and information leakage. The anonymization of raw data is necessary.	Adaptive Differential Privacy algorithm has been proposed for sharing sanitized data instead of raw data.
[43]	Lattice-Based Secure Cryptosystem for smart healthcare	This privacy preserving technique is designed for constrained nodes of smart cities.	This scheme works more efficiently as compared to other schemes presently in use. Although the scheme is introduced for smart healthcare I smart cities, it can be practically implemented in other infrastructures of smart cities.

5. Open Issues

In this section, the open issues in the research in security and privacy challenges, countermeasures, and consequences of IoT-based smart city devices over the CC are comprehensively concluded. The aim is to offer an opportunity to encourage researchers for tangible and technical advancements and seeking for suitable proactive and reactive security and privacy solutions. Various issues are discussed in the proceeding paragraphs.

Lightweight security and privacy solutions are foresighted in the CC-based smart city networks due to restricted resource and storage capacity due to huge volumes of data with large customers. Lightweight encryption models will not emphasize efficiency or usability, but it ensures integrity, non-repudiation, and availability over the edge computing environment over CC, whereas the employment of the hardcore ciphering protocols ensures the confidentiality and authenticity especially useful in fog computing domain over the CC.

Obtaining the fine grain security and privacy features in the CC-based smart city networks, a real time auto update methodology is desired to be designed and deployed for preserving the security and privacy mechanisms for efficient and reliable resource and data sharing among the huge volume of customers being providing distinctly for the edge-based devices and fog computing layer. Various techniques could be to track the authenticity, accuracy, security, and privacy of the protection employed over the deployed CC-based mart city networks.

Likewise, the attacks and threats covered in various studies in this review are not fully explored and dealing with the designs of techniques, especially those related to authentication, non-repudiation and privacy prove-lance techniques. Such attacks and

threats are dangerous for maintaining the privacy and security of communicating edge and fog devices, leading to breaching sensitive operational and technical information to the malicious agents and actors.

It is also learned that various techniques are not catering for all aspects and cardinals of the security and privacy, like in Table 2, availability, usability, and non-repudiation are having fewer techniques where as the Confidentiality, authenticity, and integrity are considered more in single and also in combination with each other. Adhering to security and privacy requirements is vital; hence, future researchers should focus on developing mechanisms and approaches that consider these requirements or cardinals inappropriate composition. There is a dire need to investigate attacks and threats with sufficient priority in designing the solutions.

Despite the CC's ready-made security and privacy mechanism, it is relatively difficult to establish secure two-way communication for secure transactions among the edge devices and over the fog computing nodes. There is a requirement to investigate the probability of usage of lightweight key exchange algorithms to design and deploy IoT-based devices of a smart city over the edge, fog, and MCC environments, while catering to confidentiality, usability, integrity, availability, non-repudiation, and authenticity. Integration of the Intrusion Detection System (IDS) and SIEM to identify, detect, and give a proactive mitigation and protection against various attacks (discussed in Table 2) needs to be further researched and experimented for various layers of CC instead of only network layer. The study is required to be extended to virtual server, virtualization, application, Iaas/Saas/Paas, Host, and hard core (Data Center) level layers to stop the malicious entity not to intrude and propagate into the CC-based entire smart city networks, where design, development, and integration analysis is still an open and critical issue for the future research.

Security and privacy awareness activities and programs are required to educate the citizens of smart cities and users of the IoT. Inculcation of the awareness about the security and privacy integration and implementation is the basic and mandatory requirement for working over the CC and IoT platform. It is all about understanding the risks and threats around the cyber world. It is to be taught that the hackers are deliberately trying to steal, misuse, and damage the users' information and that everyone be aware of the associated risks and that they work accordingly to protect them from these risks.

Security and Privacy vulnerabilities, threat consequences of the involved technologies must first be analyzed and addressed before they are installed and used in IoT and CC networks in different variations, like over edge, fog, and MCC. With the advancements in technology, new, improved and more reliable versions of software and hardware products/solutions are being developed that solve many previous versions, including privacy issues. Keeping this in view, the installed/deployed technology must be upgraded to the latest and safest one. Finally the study of blockchain technology to counter, access, mitigate, and protect the CC-based smart city networks on different textures of CC models, like edge, fog, and MCC, are still subject to more detailed research, interrogating, and design so that it could be utilized to provide a proactive and reactive approach against malicious entities to help achieving security compliance and achieving positive audit trails for authenticated compliance to security and privacy for generating more wealth and revenues.

6. Conclusions and Recommendations

CC and IoT are the most prevalent emerging technologies toward the future. CC has transnational nature and, therefore, has different issues on security and privacy, including technical, business, and regulation ones. Smart City Networks, IoT, and its web-based counterpart Web-of Things (WoT) will connect tens of billions of devices ranging from very small (tags, sensors) to very big (cars, homes, cities) that require security standards, policies, and strategies. With the advancement of CC technology, privacy and security concerns also arise. CC benefits and working with IoT. This review has tried to achieve and what methodology was adopted. Different CC techniques have been proposed to address these issues. This paper summarizes the different CC mechanisms for security, privacy, and trust-

based on different parameters. In the future, the identification of the network of various objects, threats, and attacks becomes crucial for security and privacy maintenance, and its implementation for identity management framework and other security mechanisms is desired and forecasted.

In this paper, the security and privacy concerns linked to CC, including smart city technologies, IoT devices, and platforms, have been discussed in detail. The security and privacy concerns vary for different stakeholders, depending upon their priorities and implementation/integration/deployment domain. The security and privacy protection models, methods, and frameworks have been explored and enlisted. These countermeasures are beneficial in the privacy protection strategy of IoT and CC integration, development, and deployment. In this review, it is learned and established that the identification of challenges to privacy and security and various mitigation techniques in computing the huge volume of cloud services in cloud computing is a challenging, crucial, and vulnerable task.

In the future, this research will be helpful in the development and implementation of a hybrid approach that will allow using salient features of each or some of the discussed methods and models. This hybrid design will provide security and privacy protections in the form of a single unified solution to smart devices in the domain of the smart cities over the CC solutions. It is also suggested that there is a dire need to find optimum and appropriate security and privacy solutions for the specific cloud services with respect to its utility and absorption in the industry with respect to edge, fog, and mobile cloud computing environments. It is also clear that, in the future, Artificial Intelligence (AI), along with Deep Learning (DL) techniques, could be considered for deep learning of cyber security attacks and threats analysis, like malware, Trojans, and various attacks, being faced by CC-based Smart city networks to counter the significant threats adversaries it may cause. However, security postures need to be developed to counter and prevent the CC-based smart city infrastructure against malicious internal and external exploiters, further creating repulsive actions against such.

Additionally, it is advised that future research in the domain of security and privacy in CC-based smart cities should be focused on solving the challenges identified and discussed in this review, which will invariably be beneficial to achieve and establish further smart city initiatives over the various CC environments.

Author Contributions: The research conceptualization and methodology were done by A.I.T., M.S., and R.U. The technical and theoretical framework were prepared by A.S. and M.I. The technical review and improvement were performed by B.H., N.A., and K.-I.K. The overall technical support, guidance, and project administration was done by K.-I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by research fund of Chungnam National University.

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

References

1. Elmaghraby, A.S.; Losavio, M.M. Cyber security challenges in Smart Cities: Safety, security and privacy. *J. Adv. Res.* **2014**, *5*, 491–497. [CrossRef]
2. Belanche-Gracia, D.; Casaló-Ariño, L.V.; Pérez-Rueda, A. Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. *Gov. Inf. Q.* **2015**, *32*, 154–163. [CrossRef]
3. Choudhary, A.; Bhadada, R. Emerging Threats in Cloud Computing. In Proceedings of the International Conference on Emerging Technology Trends in Electronics Communication and Networking, Surat, India, 7–8 February 2020; Springer: Berlin/Heidelberg, Germany, 2020.
4. Ijaz, S.; Shah, M.A.; Khan, A.; Ahmed, M. Smart cities: A survey on security concerns. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 612–625. [CrossRef]
5. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
6. Li, Y.; Dai, W.; Ming, Z.; Qiu, M. Privacy protection for preventing data over-collection in smart city. *IEEE Trans. Comput.* **2016**, *65*, 1339–1350. [CrossRef]
7. Smirnova, T.; Polishchuk, L.; Smirnov, O.; Buravchenko, K.; Makevnin, A. Research of cloudy technologies as a services. *Cybersecur. Educ. Sci. Tech.* **2020**, *3*, 43–62. [CrossRef]

8. Gretzel, U.; Sigala, M.; Xiang, Z.; Koo, C. Smart tourism: Foundations and developments. *Electron. Mark.* **2015**, *25*, 179–188. [CrossRef]
9. Vattapparamban, E.; Vattapparamban, E.; Güvenç, I.; Yurekli, A.I.; Akkaya, K.; Uluağaç, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In Proceedings of the Wireless Communications and Mobile computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016.
10. Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E.; Fansler, A.A. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS), Nashville, TN, USA, 17–21 September 2012; pp. 3591–3605.
11. Liberatore, S. How Do You Catch a Drone? with an Even Bigger Drone and a Giant Net. *Daily Mail*, 2015. Available online: http://www.dailymail.co.uk/sciencetech/article-3356746 (accessed on 7 June 2021).
12. Washburn, D.; Sindhu, U.; Balaouras, S.; Dines, R.A.; Hayes, N.; Nelson, L.E. Helping CIOs understand "smart city" initiatives. *Growth* **2009**, *17*, 1–17.
13. Caragliu, A.; Del Bo, C.; Nijkamp, P.J.J. Smart cities in Europe. *J. Urban Technol.* **2011**, *18*, 65–82. [CrossRef]
14. Tari, Z. Security and Privacy in Cloud Computing. *IEEE Cloud Comput.* **2014**, *1*, 54–57. [CrossRef]
15. Edwards, L. Privacy, security and data protection in smart cities: A critical EU law perspective. *Eur. Data Prot. L. Rev.* **2016**, *2*, 28. [CrossRef]
16. Fortino, G.; Russo, W.; Savaglio, C.; Shen, W.; Zhou, M. Agent-oriented cooperative smart objects: From IoT system design to implementation. *IEEE Trans. Syst. Man, Cybern. Syst.* **2017**, *48*, 1939–1956. [CrossRef]
17. Ai, Y.; Peng, M.; Zhang, K. Edge computing technologies for Internet of Things: A primer. *Digit. Commun. Netw.* **2018**, *4*, 77–86. [CrossRef]
18. Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: A survey. *Future Gener. Comput. Syst.* **2016**, *56*, 684–700. [CrossRef]
19. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
20. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A.; Khalil, I.; Guizani, M.; Al-Fuqaha, A. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2456–2501. [CrossRef]
21. Qureshi, K.N.; Bashir, F.; Abdullah, A.H. An energy and link aware next node selection protocol for body area networks. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018.
22. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Sensing as a service model for smart cities supported by internet of things. *Trans. Emerging Telecommun. Technol.* **2014**, *25*, 81–93. [CrossRef]
23. Qureshi, K.N.; Abdullah, A.H.; Ullah, G. Sensor based Vehicle Environment Perception Information System. In Proceedings of the 4 IEEE International Conference on Ubiquitous Intelligence and Computing/International Conference on Autonomic and Trusted Computing/International Conference on Scalable Computing and Communications and Its Associated Workshops, Bali, Indonesia, 9–12 December 2014.
24. Zhang, T.; Yan, L.; Yang, Y.J.W.N. Trust evaluation method for clustered wireless sensor networks based on cloud model. *Wirel. Netw.* **2018**, *24*, 777–797. [CrossRef]
25. Han, G.; Jiang, J.; Shu, L.; Niu, J.; Chao, H.C. Management and applications of trust in Wireless Sensor Networks: A survey. *J. Comput. Syst. Sci.* **2014**, *80*, 602–617. [CrossRef]
26. Martínez-Ballesté, A.; Pérez-Martínez, P.A.; Solanas, A. The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Commun. Mag.* **2013**, *51*, 136–141. [CrossRef]
27. Schumacher, M.; Fernandez-Buglioni, E.; Hybertson, D.; Buschmann, F.; Sommerlad, P. *Security Patterns: Integrating Security and Systems Engineering*; John Wiley & Sons: Hoboken, NJ, USA, 2013.
28. Qureshi, K.N.; Bashir, F.; Abdullah, A.H. Provision of Security in Vehicular Ad hoc Networks through An Intelligent Secure Routing Scheme. In Proceedings of the 2017 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 18–20 December 2017.
29. Fu, X.; Fortino, G.; Pace, P.; Aloi, G.; Li, W. Environment-fusion multipath routing protocol for wireless sensor networks. *Inf. Fusion* **2020**, *53*, 4–19. [CrossRef]
30. Stergiou, C.; Psannis, K.E.; Kim, B.G.; Gupta, B. Secure integration of IoT and cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 964–975. [CrossRef]
31. Aliero, M.S.; Qureshi, K.N.; Pasha, M.F.; Ghani, I.; Yauri, R.A. Systematic Review Analysis on SQLIA Detection and Prevention Approaches. *Wirel. Pers. Commun.* **2020**, *112*, 2297–2333. [CrossRef]
32. Pearson, S. Privacy, security and trust in cloud computing. In *Privacy and Security for Cloud Computing*; Springer: London, UK, 2013; pp. 3–42.
33. Chakrabarty, S.; Engels, D.W. A secure IoT architecture for Smart Cities. In Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016.
34. Khan, Z.; Pervez, Z.; Ghafoor, A. Towards cloud based smart cities data security and privacy management. In Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, London, UK, 8–11 December 2014.
35. Arafati, M.; Dagher, G.G.; Fung, B.C.; Hung, P.C. D-mash: A framework for privacy-preserving data-as-a-service mashups. In Proceedings of the IEEE 7th International Conference on Cloud Computing (CLOUD), Anchorage, AK, USA, 27 June–2 July 2014.

36. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge computing security: State of the art and challenges. *Proc. IEEE* **2019**, *107*, 1608–1631. [CrossRef]
37. Tabrizchi, H.; Rafsanjani, M.K. A survey on security challenges in cloud computing: Issues, threats, and solutions. *J. Supercomput.* **2020**, *76*, 9493–9532. [CrossRef]
38. Balani, Z.; Varol, H. Cloud Computing Security Challenges and Threats. In Proceedings of the 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Belrut, Lebanon, 1–2 June 2020.
39. Bratterud, A.; Happe, A.; Duncan, R.A.K. Enhancing cloud security and privacy: The Unikernel solution. In Proceedings of the Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, Athens, Greece, 19–23 February 2017.
40. Mo, J.; Hu, Z.; Chen, H.; Shen, W. An efficient and provably secure anonymous user authentication and key agreement for mobile cloud computing. *Wirel. Commun. Mob. Comput.* **2019**, *2019*. [CrossRef]
41. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), Kona, HI, USA, 13–17 March 2017.
42. Kaaniche, N.; Laurent, M. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Comput. Commun.* **2017**, *111*, 120–141. [CrossRef]
43. Hossain, M.S.; Muhammad, G. Emotion recognition using secure edge and cloud computing. *Inf. Sci.* **2019**, *504*, 589–601. [CrossRef]
44. Verginadis, Y.; Michalas, A.; Gouvas, P.; Schiefer, G.; Hübsch, G.; Paraskakis, I. Paasword: A holistic data privacy and security by design framework for cloud services. *J. Grid Comput.* **2017**, *15*, 219–234. [CrossRef]
45. Yu, Y.; Miyaji, A.; Au, M.H.; Susilo, W. *Cloud Computing Security and Privacy: Standards and Regulations*; Elsevier: Amsterdam, The Netherlands, 2017.
46. Kolhar, M.; Abu-Alhaj, M.M.; El-atty, S.M.A. Cloud data auditing techniques with a focus on privacy and security. *IEEE Secur. Priv.* **2017**, *15*, 42–51. [CrossRef]
47. Mollah, M.B.; Azad, M.A.K.; Vasilakos, A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. *J. Netw. Comput. Appl.* **2017**, *84*, 38–54. [CrossRef]
48. Li, Y.; Yu, Y.; Yang, B.; Min, G.; Wu, H. Privacy preserving cloud data auditing with efficient key update. *Future Gener. Comput. Syst.* **2018**, *78*, 789–798. [CrossRef]
49. Shakeel, P.M.; Baskar, S.; Dhulipala, V.S.; Mishra, S.; Jaber, M.M. Maintaining security and privacy in health care system using learning based deep-Q-networks. *J. Med. Syst.* **2018**, *42*, 186. [CrossRef] [PubMed]
50. Gong, Y.; Zhang, C.; Fang, Y.; Sun, J. Protecting location privacy for task allocation in ad hoc mobile cloud computing. *IEEE Trans. Emerg. Top. Comput.* **2015**, *6*, 110–121. [CrossRef]
51. Elhoseny, M.; Abdelaziz, A.; Salama, A.S.; Riad, A.M.; Muhammad, K.; Sangaiah, A.K. A hybrid model of internet of things and cloud computing to manage big data in health services applications. *Future Gener. Comput. Syst.* **2018**, *86*, 1383–1394. [CrossRef]
52. Xue, K.; Hong, J.; Ma, Y.; Wei, D.S.; Hong, P.; Yu, N. Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing. *IEEE Netw.* **2018**, *32*, 7–13. [CrossRef]
53. Tian, H.; Nan, F.; Chang, C.C.; Huang, Y.; Lu, J.; Du, Y. Privacy-preserving public auditing for secure data storage in fog-to-cloud computing. *J. Netw. Comput. Appl.* **2019**, *127*, 59–69. [CrossRef]
54. Lo'ai, A.T.; Mehmood, R.; Benkhlifa, E.; Song, H. Mobile cloud computing model and big data analysis for healthcare applications. *IEEE Access* **2016**, *4*, 6171–6180.
55. Hasson, F.; Keeney, S.; McKenna, H. Research guidelines for the Delphi survey technique. *J. Adv. Nurs.* **2000**, *32*, 1008–1015.
56. Liu, L.S.; Shih, P.C.; Hayes, G.R. Barriers to the adoption and use of personal health record systems, In Proceedings of the 2011 iConference, Seattle, WA, USA, 8–11 Febuary 2011; pp. 363–370.
57. Bahga, A.; Madisetti, V.K. A cloud-based approach for interoperable electronic health records (EHRs). *IEEE J. Biomed. Health Inf.* **2013**, *17*, 894–906. [CrossRef]
58. Hsieh, G.; Chen, R.-J. Design for a secure interoperable cloud-based Personal Health Record service. In Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, CloudCom 2012, Taipei, Taiwan, 3–6 December 2012.
59. Ahmadi, M.; Aslani, N. Capabilities and advantages of cloud computing in the implementation of electronic health record. *Acta Inform. Medica* **2018**, *26*, 24. [CrossRef]
60. Qiu, M.; Gai, K.; Thuraisingham, B.; Tao, L.; Zhao, H. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Gener. Comput. Syst.* **2018**, *80*, 421–429. [CrossRef]
61. Alshehri, S.; Radziszowski, S.P.; Raj, R.K. Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In Proceedings of the IEEE 28th International Conference on Data Engineering, ICDE 2012, Arlington, VA, USA, 1–5 April 2012.
62. Athena, J.; Sumathy, V.; Kumar, K. An identity attribute–based encryption using elliptic curve digital signature for patient health record maintenance. *Int. J. Commun. Syst.* **2018**, *31*, e3439. [CrossRef]
63. Seol, K.; Kim, Y.G.; Lee, E.; Seo, Y.D.; Baik, D.K. Privacy-preserving attribute-based access control model for XML-based electronic health record system. *IEEE Access* **2018**, *6*, 9114–9128. [CrossRef]

64. Lindsay, J.R. Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. *Secur. Stud.* **2020**, *29*, 335–361. [CrossRef]
65. Qadri, Y.A.; Ali, R.; Musaddiq, A.; Al-Turjman, F.; Kim, D.W.; Kim, S.W. The limitations in the state-of-the-art counter-measures against the security threats in H-IoT. *Cluster Comput.* **2020**, *23*, 2047–2065. [CrossRef]
66. Waheed, N.; He, X.; Ikram, M.; Usman, M.; Hashmi, S.S.; Usman, M. Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. *Acm Comput. Surv.* **2020**, *53*, 1–37. [CrossRef]
67. Khan, N.; Al-Yasiri, A. Cloud security threats and techniques to strengthen cloud computing adoption framework. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2018; pp. 268–285.
68. Fu, K.; Kohno, T.; Lopresti, D.; Mynatt, E.; Nahrstedt, K.; Patel, S.; Richardson, D.; Zorn, B. Safety, security, and privacy threats posed by accelerating trends in the Internet of Things. *arXiv* **2020**, arXiv:2008.00017.
69. Chen, M.; Zhang, Y.; Hu, L.; Taleb, T.; Sheng, Z. Cloud-based wireless network: Virtualized, reconfigurable, smart wireless network to enable 5G technologies. *Mob. Netw. Appl.* **2015**, *20*, 704–712. [CrossRef]
70. Pérez-Martínez, P.A.; Solanas, A. W3-privacy: The three dimensions of user privacy in LBS. In Proceedings of the 12th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing, Paris, France, 16–19 May 2011.
71. Mishra, A.; Gupta, N.; Gupta, B.B. Security Threats and Recent Countermeasures in Cloud Computing. In *Modern Principles, Practices, and Algorithms for Cloud Security*; IGI Global: Hershey, PA, USA, 2020; pp. 145–161.
72. David, B.; Dowsley, R.; van de Graaf, J.; Marques, D.; Nascimento, A.C.; Pinto, A.C. Unconditionally Secure, Universally Composable Privacy Preserving Linear Algebra. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 59–73. [CrossRef]
73. Chourabi, H.; Nam, T.; Walker, S.; Gil-Garcia, J.R.; Mellouli, S.; Nahon, K.; Pardo, T.A.; Scholl, H.J. Understanding smart cities: An integrative framework. In Proceedings of the 45th Hawaii International Conference on System Sciences, Maui, HI USA, 4–7 January 2012.
74. Smith, M.L. Viktor Mayer-Schönberger, Delete: The virtue of forgetting in the digital age. *Identity Inf. Soc.* **2009**, *2*, 369–373. [CrossRef]
75. Djigal, H.; Jun, F.; Lu, J. Secure framework for future smart city. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017.
76. Sengupta, N. Designing cyber security system for smart cities. In Proceedings of the Smart Cities Symposium 2018, Zallaq, Bahrain, 22–23 April 2018.
77. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
78. Farzandipour, M.; Sadoughi, F.; Ahmadi, M.; Karimi, I. Security requirements and solutions in electronic health records: Lessons learned from a comparative study. *J. Med. Syst.* **2010**, *34*, 629–642. [CrossRef]
79. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart cities of the future. *Eur. Phys. J. Spec. Top.* **2012**, *214*, 481–518. [CrossRef]
80. Xiao, Z.; Xiao, Y. Security and privacy in cloud computing. *IEEE Commun. Surv. Tutorials* **2013**, *15*, 843–859. [CrossRef]
81. Thoke, O. Cloud and Mobile Device Security: Challenges for 2016. Available online: Https://www.lifewire.com/cloud-mobile-device-security-challenges-3473908 (accessed on 17 May 2021).
82. Kumar, J.S.; Patel, D.R. A survey on internet of things: Security and privacy issues. *Int. J. Comput. Appl.* **2014**, *90*, 20–26.
83. Barth, S.; de Jong, M.D. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telemat. Inform.* **2017**, *34*, 1038–1058. [CrossRef]
84. Khatoun, R.; Zeadally, S. Cybersecurity and privacy solutions in smart cities. *IEEE Commun. Mag.* **2017**, *55*, 51–59. [CrossRef]
85. Moustaka, V.; Theodosiou, Z.; Vakali, A.; Kounoudes, A. Smart Cities at Risk!: Privacy and Security Borderlines from Social Networking in Cities. *Athena* **2018**, *357*, 25870072.
86. Zaman, F.; Raza, B.; Malik, A.K.; Anjum, A. Self-Protection against Insider Threats in DBMS through Policies Implementation. *Self* **2017**, *8*, 3. [CrossRef]
87. Cheon, J.H.; Kim, J. A hybrid scheme of public-key encryption and somewhat homomorphic encryption. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1052–1063 [CrossRef]
88. Zaman, A.; Obimbo, C.; Dara, R.A. Information Disclosure, Security, and Data Quality. In Proceedings of the International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Montreal, QC, Canada, 25–28 June 2018.
89. Schaffers, H.; Komninos, N.; Pallot, M.; Trousse, B.; Nilsson, M.; Oliveira, A. Smart cities and the future internet: Towards cooperation frameworks for open innovation. In *The Future Internet Assembly*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 431–446.
90. Spiekermann, S.; Cranor, L.F. Engineering privacy. *IEEE Trans. Softw. Eng.* **2009**, *35*, 67–82. [CrossRef]
91. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Kumar, N.; Das, A.K.; Saxena, N. LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. *IEEE Commun. Mag.* **2018**, *56*, 24–32. [CrossRef]
92. Perera, C.; Ranjan, R.; Wang, L.; Khan, S.U.; Zomaya, A.Y. Big data privacy in the internet of things era. *IT Prof.* **2015**, *17*, 32–39. [CrossRef]
93. Moreno, J.; Serrano, M.A.; Fernández-Medina, E. Main issues in big data security. *Future Internet* **2016**, *8*, 44. [CrossRef]
94. Smutny, Z.; Vehovar, V. Social informatics research: Schools of thought, methodological basis, and thematic conceptualization. *J. Assoc. Inf. Sci. Technol.* **2020**, *71*, 529–539. [CrossRef]