Chapter 10
A Conceptual Framework for Security and Privacy in Edge Computing

Bragadeesh S. A. and Umamakeswari Arumugam

10.1 Introduction

Ubiquitous connectivity is the need of the hour with the ever-increasing volume of devices getting access to the Internet. Several key technologies drive the proliferation of IoT solutions across multifaceted application domains that are extensively discussed, researched, and adopted. The key challenge in IoT is processing the data from devices and performing meaningful interpretation to derive insights and take decisions.

Cloud computing has made possible the widespread adoption and proliferation of IoT. It has been the backbone of IoT deployments and applications which has helped in achieving primary network objectives like storage, communication, and computation. It also offers services that can be tailored according to user and application requirements. Cloud computing consists of a pool of resources, typically consisting of services like networking, storage, and computing, which are organized to cater the needs of multiple end users based on a multitenant model. The access to these resources is via standard mechanisms and is usually available across a network. The varieties of service offered by the cloud computing paradigm include SaaS (Software-as-a-Service) in which applications are offered as service, IaaS (Infrastructure-as-a-Service) which offers computing resources as a service, and finally PaaS (Platform-as-a-Service) which provides software and hardware tools for development. The widely adopted deployment models of cloud computing include public and private clouds in which organizations deploy cloud services to any end user or within their own cloud computing platform, respectively. Cloud computing is capable of providing the following value additions – elasticity, ubiquity, reduced

Bragadeesh S. A. (✉) · U. Arumugam
School of Computing, SASTRA Deemed to be University, Thanjavur, Tamil Nadu, India

F. Al-Turjman (ed.), *Edge Computing*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-319-99061-3_10

management effort, pay-as-you-use, and convenience which has been a driving force for the creation of a rapidly growing industry across the globe which has its worth in billions [9].

Regardless of all these benefits, there are few areas in which cloud computing does fall short of meeting the application requirements, which include increased network latency, jitter, lack of ability to access local contextual information, and lack of support for mobility of users. For an application that is delay sensitive, these requirements must be met. Due to these reasons, there has been an evolution of new computing paradigms such as fog computing, mobile cloud computing, and mobile edge computing, among others [2, 7]. Edge computing leverages the resources available on the local edge to meet the specific application requirements mentioned. Edge computing can bring the services offered by cloud computing to the network edge and the essential functionalities like communication, storage, and computation closer to the devices and users.

The primary objective of these computing technologies is to bring about the capabilities of cloud computing closer to the user or near the network edge. Normally most edge computing paradigms follow the structure as shown in Fig. 10.1. The edge layer devices as specified can be microdata centers, gateways, and dedicated

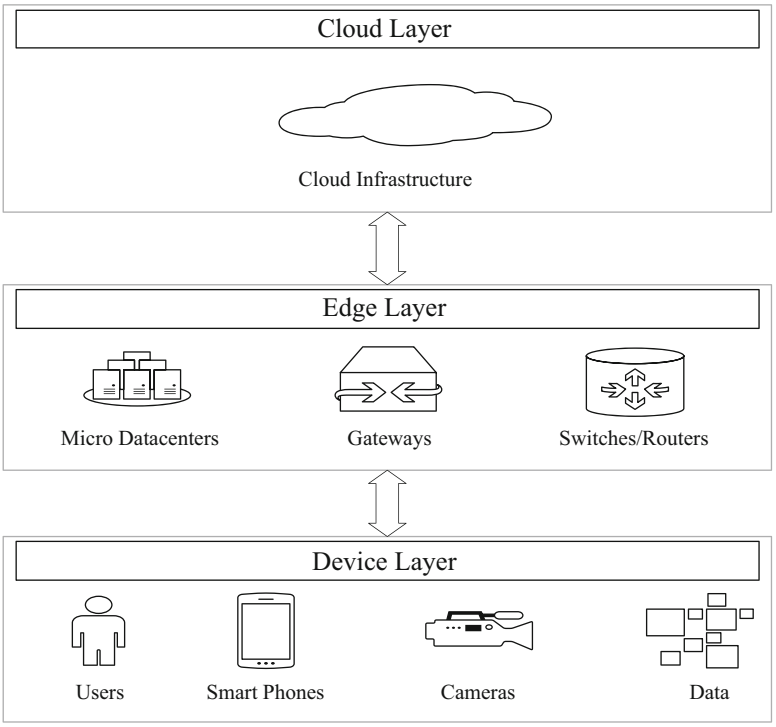

Fig. 10.1 Edge computing model

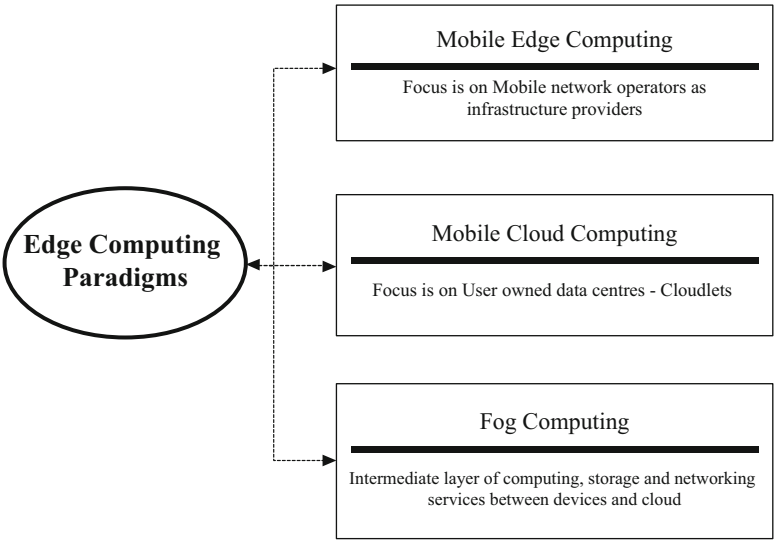

Fig. 10.2 Edge computing technology paradigms

routers/switches. Microdata centers are capable of functioning autonomously and collaborate with other such devices to offer services to end users, to third-party clients, and sometimes to the infrastructure providers too. They are still connected to the traditional cloud infrastructure which creates an opportunity to establish a hierarchical architecture to provide platforms for the management and registration of user services. An edge infrastructure which is owned by a single service provider referred to as trust domain can collaborate with other such trust domains, forming an environment where it is possible to serve multitude end users.

Figure 10.2 is helpful in pointing out the key functional differences in the different edge paradigms. A detailed comparison between the various edge paradigms is available in Sect. 10.2. There are several similarities among them. The architectures, services, mechanisms, and protocols applicable for one of them are applicable and can be adopted for the other.

The security and privacy mechanisms for edge computing paradigms are still in its emerging stage, and given the growing importance of the field, it is critical to identify the possible threats. It may not be possible to reciprocate the currently available tools and methods for security and privacy in cloud computing for edge computing owing to its specific attributes such as heterogeneity, low latency, location awareness, spatial distribution, and mobility. Even though some of these issues can be addressed using existing security schemes, new issues arise due to the above-mentioned special characteristics of edge computing. It might be even possible to adopt and analyze the existing security and privacy mechanisms that are implemented for other enabling technologies and related computing paradigms. Some of the enabling technologies which play a significant role in realization of edge

computing include virtualization technologies, wireless networks, peer-to-peer and distributed networks, and software-defined networking (SDN), among others [1, 2].

The rest of the content is organized as follows. Section 10.2 elucidates the similarities and differences between the various edge computing paradigms. Section 10.3 introduces the basic components of security and privacy for edge computing and summarizes the various threats that target the edge paradigm. Section 10.4 presents a framework for implementing security and privacy for edge paradigm. Section 10.5 highlights the various challenges involved in implementation of security and privacy solutions. Section 10.6 provides the concluding remarks and briefly talks about the future directions. It is our belief that this paper provides better clarity for researchers and users regarding the concepts of edge computing and tries to stress the importance of ensuring the security and privacy as a key requirement for application and system developers.

10.2 Similarities and Differences Between Edge Paradigms

Table 10.1 gives an overall idea of how the edge paradigms differ from the traditional cloud structure. This comparison is necessary to understand the challenges that arise when we need to implement solutions in edge computing. It is evident that all the edge paradigms have the common goal of bringing the capabilities of cloud computing closer to the edge. They all provide in some way the multitenant virtualization infrastructure which helps in location-specific provisioning capabilities and access to nearby computational resources when required. We have taken into account MEC, MCC, and fog computing for our comparison [1, 5]. As mentioned earlier all of them have own similarities among them and uniqueness as well. They

Table 10.1 Differences between edge computing and cloud computing

Features	Cloud computing	Edge computing
Computational capacity	High	Medium to low
Size and operating mode	Centralized large servers	Distributed smaller servers
Applications	Delay tolerant, computationally intensive	Low latency, real-time operation, high QoS
Fronthaul/backhaul communication overhead	High	Low
Mobility support	Low	High
Management	Service provider	Local business
Deployment	Requires complicated deployment planning	Ad hoc deployment/minimal or no planning
User device	Computers, limited mobile devices	Mobile smart wearable devices
Network access type	WAN	LAN/WLAN

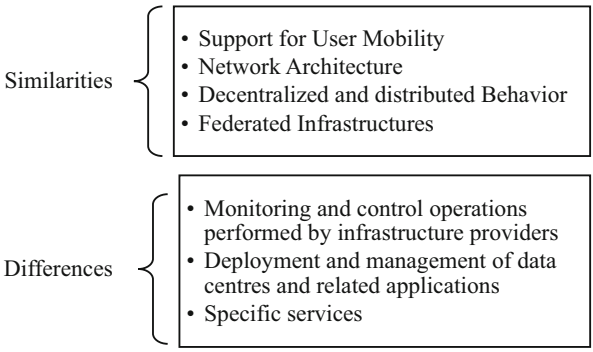

Fig. 10.3 Similarities and differences between edge paradigms

provide a similar set of benefits that are majorly due to the closeness of the edge data centers. The benefits are as follows:

- Low and predictable jitter and network latency
- Location-based context-aware information
- Support for scalability
- High availability of services

Figure 10.3 summarizes the similarities and differences between the edge paradigms. The predominant similarity is that all these techniques basically can provide support for mobility. They have consideration for device mobility and have specific management mechanisms that are located at the application level itself or use virtual instances of devices to accommodate for the same. The next similarity is the overall architecture which has support to enable the edge paradigms to behave as an extension of cloud infrastructure. The network elements act in a distributed and decentralized way capable of provisioning services and taking decisions autonomously. They can also cooperate with each other to reduce the dependency on the central cloud setup. The different edge data centers can exchange information among them and coexist to form a federated infrastructure.

Moving on to the differences, even though the edge paradigms have a common objective, they have few basic differences in the way they fulfill the objective. MEC deployments primarily focus on realization of 5G, whereas fog nodes can provide services to other applications which have their own servers, gateways, access points, and so on. In case of MCC, it is highly distributed in nature, and device instances can perform their own service provisioning. This difference in management and deployment of the data centers determines who will be service providers. Another difference is that the applications supported are determined by the choice of service providers. MEC provides support for operators to work closely with other third-party service providers, which enables for thorough testing and possibility for customized integration. This applies true even for fog computing also. The final difference is that MCC paradigm provides specific services that are not related to virtualization but enables support for execution mechanisms that are distributed in nature. This is highly beneficial for devices that have severe resource constraints.

Although there are differences, still the security and privacy techniques used for one paradigm can be easily adopted for the other.

10.3 Overview of Security, Privacy, and Threats in Edge Computing

As emphasized earlier, edge computing is not a one-to-one replacement of cloud computing, whereas it helps in augmenting and broadening the services of cloud computing. The principal services offered by edge computing include storage, computation, data sharing, and networking [12]. With respect to these four services, unique security and privacy requirements emerge as shown in Fig. 10.4.

10.3.1 Security in Edge Computing

The key attributes whenever we are trying to implement security solutions are authentication, integrity, confidentiality, trust, access control, data security, and privacy [1, 11]. The various components of providing end-to-end security and privacy are as follows.

10.3.1.1 Network Security

The configurations performed by the network administrator and the network management information must be secured and isolated from the normal data flow.

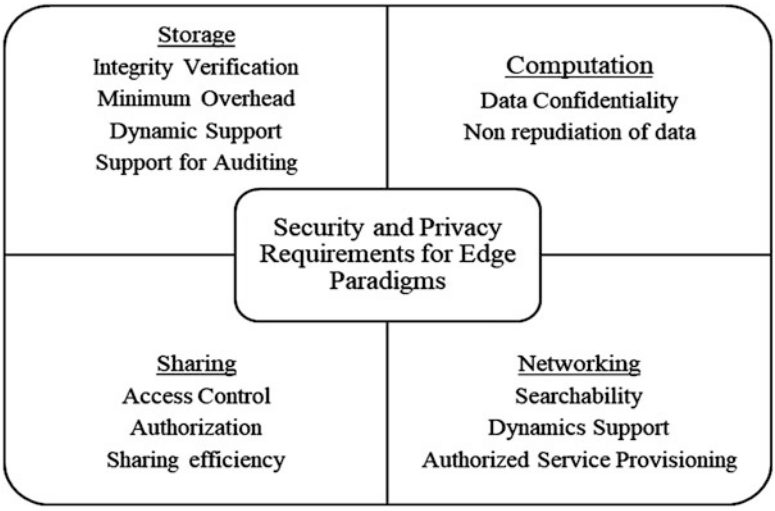

Fig. 10.4 Summary of security and privacy requirements for edge computing

This is required since the edge devices are distributed across the network and the cost of maintenance is high. However, a new network concept called software-defined networking (SDN) can come to the rescue. The benefits of SDN include but not limited to reducing the burden of management and implementation, improving the scalability of the network, decreasing the cost of maintenance, providing prioritization and isolation of network traffic, and enhancing the access control of network resources, cooperation, and network sharing.

10.3.1.2 Data Storage Security

Like cloud computing, the data storage in edge platform is also outsourced. It is tough to ensure data integrity since there are a lot of possibilities for data loss and data modifications. If the data present in one device is compromised, the attackers could easily abuse the data stored to fulfill their own needs. Hence, provision for data storage auditing should be done. Third-party auditing services are available, which are provided by the infrastructure providers, and the application users should be aware of the auditing policies. It is possible to use encryption techniques to ensure integrity, verifiability, and confidentiality of the data to check for untrusted network entities and allow the user to check the stored data. Since all data need not be essentially present on all the available storage resources, reduced latency and support for dynamic access are required.

10.3.1.3 Data Computation Security

The data computation performed at the edge servers and devices should be secured and verifiable. The security of computations can be ensured by using data encryption techniques, which prevents data visibility to any hackers/attackers. Since the microdata centers have the provisions to off-load some of the computations to other data centers, a mechanism to verify the computation results and establish trust between the two entities becomes a necessity. The computational accuracy should be verifiable by the user. Use of data encryption for the data that is being forwarded to the edge data centers from end devices and from one data center to another helps in ensuring data integrity and protection. One of the popular mechanisms to verify the data security is using data search technique in which a keyword-based search is performed in the encrypted data repositories. This enables users to securely search for user data amidst encrypted data. This helps in maintaining the secrecy of encryption.

10.3.1.4 End Devices Security

Since the end devices are typically less powerful and have limited access to the surroundings, they can be easily tampered with. Any hacker may try to take control

of a device and make it a rogue node to retrieve essential network management data. They can hinder the normal behavior by corrupting the device data and increase the frequency of data access by sending fake information. They can also use the end device to propagate false data across the network to potentially create discrepancies and disrupt the normal network behavior. Hence, proper efforts should be made for ensuring the security of the end device.

10.3.1.5 Access Control

Enforcement of access control mechanisms can provide dual benefits of security and privacy. Since the edge platform is distributed and decentralized in nature, a good access control policy acts as a defensive shield to mitigate unauthorized device and service access. Access control helps in realizing the interoperability and collaboration among microdata centers that are provided by different service providers and are separated across different geo-locations. A robust access control mechanism is required to meet the design goals, accommodate mobility, low latency, and interoperability.

10.3.1.6 Intrusion Detection

Intrusion detection techniques help in identifying malicious data entries and detect device anomalies. They can be used to carefully investigate and analyze the behavior of devices in the network and provide methods to perform packet inspection, which helps in early detection of denial-of-service attacks, integrity attacks, and data flooding, among others. The primary challenge when implementing intrusion detection for edge platform is to accommodate for scalability, mobility, and low-latency requirements.

10.3.2 Privacy in Edge Computing

Privacy in edge computing can be enforced in a threefold manner: user privacy, data privacy, and location privacy. User privacy deals with protecting the privacy of user's credentials and their frequency of accessing the data. A potential hacker may observe the usage pattern and try to pretend to be legitimate user and access the necessary information. Hence, ensuring the privacy of user is required. Data privacy-preserving techniques may be available at the edge and cloud level, but making them available at the resource-constrained end device is a design challenge. This helps in avoiding unauthorized access of the network by hackers and helps in preserving the integrity of the network.

Since the edge data centers may be spatially distributed, ensuring location privacy is also a prime requirement. Since the location data can help in deciphering the

environment-related information, the choice of edge data centers has to be carefully planned. Identity obfuscation is a technique used to protect the identity of an edge device from the user even though the user is nearby. When more than one edge nodes are being used by an application, it is relatively easier for an attacker to isolate the location, since the proximity of edge nodes gives them an idea that the end device should be in between the edge nodes. Ensuring location privacy without affecting the computational overhead is of primary importance.

10.3.3 Nature of Threats in Edge Computing

Any possible attempt to disrupt the normal functioning of a network or a system is deemed as a threat. Only when we understand the nature of threats, it is possible to define security solutions for it. Hence, the basic knowledge about threats and how they can be mitigated is essential. All the possible threats in edge computing environment have been presented in Table 10.2.

Table 10.2 List of threats

Components	Possible threats
Data	Data replication
	Data manipulation
	Data deletion
	Illegal data access
	Eavesdropping
Network	Denial of service
	Man-in-the-middle
	Physical damage
	Service manipulation
	Rogue server
	Privacy leakage
	Jamming
	Congestion
	Black hole
Communication	Data loss
	Data breach
	Sniffing
	Message replay
	Impersonation
Services	Service manipulation
	Rogue infrastructure
	Privacy leakage
	Insecure APIs
Devices	Physical damage
	Misuse of resources
	Flooding
	Power failure

The threats can be grouped according to the component of the system they try to attack [6]. The implementation of solutions to these attacks can be made possible by a combination of security attributes such as authentication, confidentiality, integrity, availability, and privacy.

10.4 Framework for Security and Privacy in Edge Computing

Figure 10.5 represents the basic components of the proposed conceptual framework. The framework consists of a hierarchical structure in which the communication and exchange of data can be done using APIs. There are three levels: device management, security services, and application and infrastructure. The proposed framework aims to bring into account the necessary security and privacy requirements which are specific to edge computing platform. The framework can be implemented in an edge

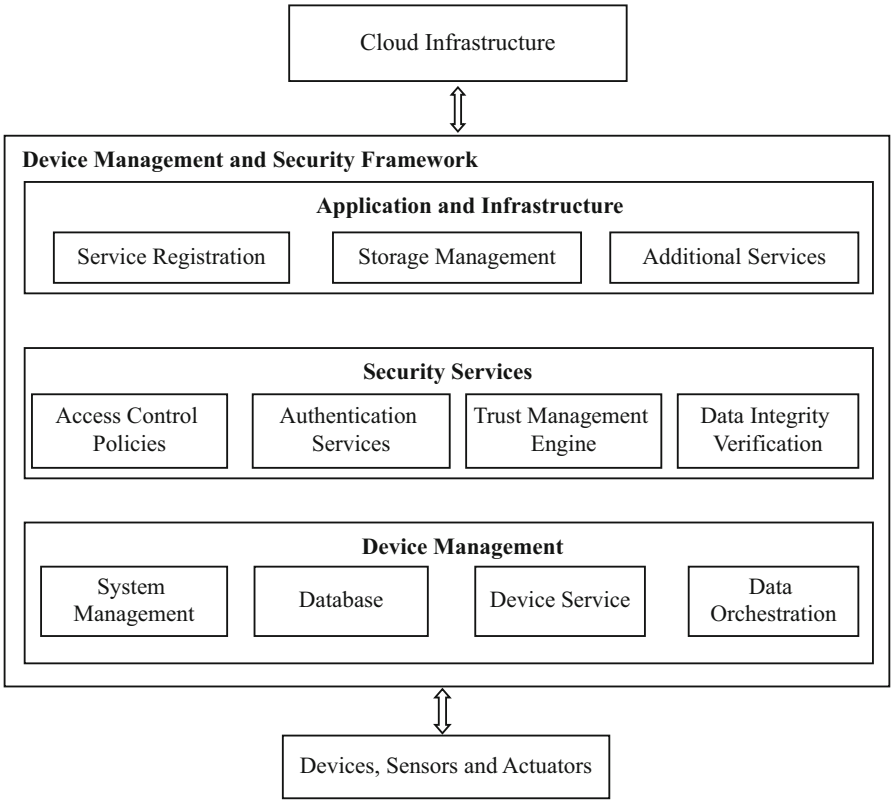

Fig. 10.5 Security and privacy framework for edge computing

gateway or a microdata center. The suitability of the framework for implementation in the resource-constrained end devices needs further investigation.

10.4.1 Device Management

The primary functionalities of the device management layer are to manage the end devices, create database, manage the services provide to the end device, and perform data orchestration operations. The status of the end devices, access control, maintaining integrity of the data stored, and providing the necessary data from service providers are all taken care by the device management layer. Network function virtualization (NFV) is one of the popular and emerging technologies which can perform the tasks mentioned above. NFV in convergence with SDN can help in realizing the full potential of edge computing platform. NFV provides virtualization of infrastructure services, orchestration, and management functionalities.

10.4.2 Security Services

The security services layer is the heart of the framework which performs the critical tasks such as creating, updating, and maintaining the access control policies. It also ensures authentication of devices, service providers, and the data that is communicated. It also makes use of a trust management engine which is used for accomplishing two objectives. It governs the privacy of the overall system and generates rules for implementing intrusion detection mechanism. The data integrity verification component performs the verification of data across the system and computations done by other edge devices. Establishment of well-defined APIs and integration of the modules with the application and device management layer help in improving the overall performance of the framework and achieving the edge computing specific requirements.

10.4.3 Application and Infrastructure

This layer is responsible for keeping track of the network-wide application interactions and governs the authentication policies for accessing the network devices. The service provisioning details of neighboring data centers and making the decision of whether cloud support is required or not are carried out by this layer. Also, the services offered by the infrastructure providers are monitored and provisioned for access to the end devices. This layer is significant because edge platform caters to multitenant application services, hence implementing security measures for it is an essential task.

10.5 Security and Privacy Challenges in Edge Computing

Edge computing has opened new arenas and created new opportunities to build solutions that can augment existing cloud-based solutions. In order to explore the full potential and bring about the widespread adoption of edge computing solutions, one key area of focus is how to secure the system components and how to ensure the privacy of user and organization data [6]. Figure 10.6 points out some of the major challenges that need to be addressed [3, 4, 8, 10]. The challenges can be summarized as below.

- The added security mechanism should not increase the computation overhead and hamper the storage space required for other system operations.
- Edge computing mechanisms use cache management techniques which are prone to side channel attacks; hence, care should be taken to prevent leakage of private and sensitive data.
- For applications that stream data continuously for monitoring and management purposes, hence due to increased number of devices, the volume data to be processed is typically large. To detect the anomaly, packet filtering mechanisms need to be implemented which might require additional memory and processing power.
- It is difficult to manage user identity, scalability, monitoring, performance, data security, and considering threats from insiders due to the large number of users who share the resources and application in the edge computing environment.

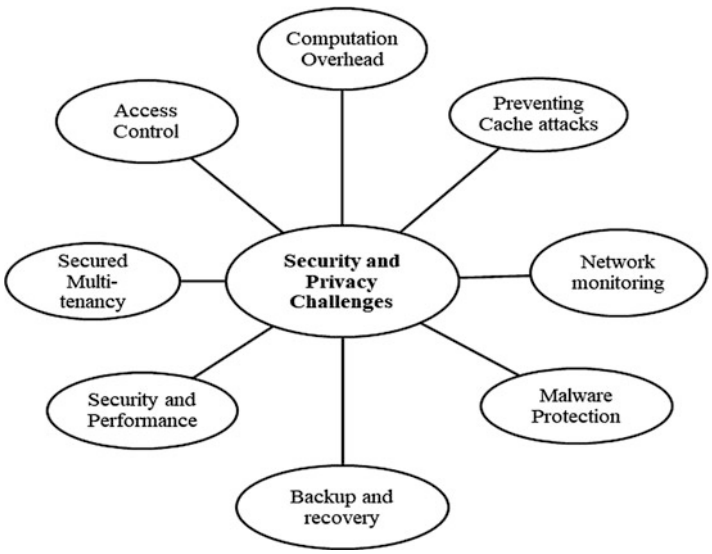

Fig. 10.6 Security and privacy challenges in edge computing

- The trade-off between application performance and security is solely dependent on the user or application's requirements; hence, establishing clear performance benchmarks without compromising security is important.
- Depending on the application and user requirements, the edge platform may have high data throughput and relatively lesser amount of data stored which may lead to problems for data storage and recovery.
- By using virtualization services, edge computing provides multitenant application access leads to exposing APIs to multiple users which may lead to insider attacks and data breaches.
- Due to the increased number of devices, implementing a common access control policy becomes a tedious task. Accounting for mobility of devices is also important.
- To ensure the privacy of user's data, the data privacy policies of the edge platform as well as the cloud infrastructure must be in sync which might lead to potential challenges. The privacy policies of different infrastructure providers may not be the same.

10.6 Conclusion

In this work, we have defined the various edge paradigms and listed out their similarities and differences. We have also made a comparison of edge computing with cloud computing to drive in the importance of new implementation challenges and approaches required for edge computing solutions. We have analyzed the various aspects of security and privacy for edge computing and also brought into light some of the possible threats. A conceptual framework for ensuring security and privacy in edge computing has been discussed along with various components involved in it. The reality to be considered here is that security and privacy solutions for edge computing are still in their nascent stages, and, hence, we have analyzed the possible challenges that might arise. This work is intended to be an eye-opener for developers and technology enthusiasts who are involved in developing security and privacy solutions for edge computing.

The future scope of this work is to develop a system which consists of a knowledge base, rule-based inference engines, and a decision support toolbox that could be added to an edge computing platform which helps in mitigating possible security attacks and ensures the privacy of user data.

Acknowledgment The authors wish to express their sincere thanks to the Department of Science & Technology, New Delhi, India (Project ID: SR/FST/ETI-371/2014), and express their sincere thanks to the INSPIRE fellowship (DST/INSPIRE Fellowship/2016/IF160837) for their financial support. The authors also thank SASTRA Deemed to be University, Thanjavur, India, for extending the infrastructural support to carry out this work.

References

1. N. Abbas et al., Mobile edge computing: a survey. IEEE IOT J. **5**(1), 450–465 (2018)
2. Y. Ai, M. Peng, K. Zhang, Edge cloud computing technologies for internet of things: a primer. Digit. Commun. Netw. **4**(2), 77–86 (2018)
3. F.A. Alaba et al., Internet of things security: a survey. J. Netw. Comput. Appl. **88**(April), 10–28 (2017)
4. A. Alrawais et al., Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput. **21**(2), 34–42 (2017)
5. A.V. Dastjerdi, R. Buyya, Fog computing: helping the internet of things realize its potential. Computer **49**(8), 112–116 (2016)
6. S. Khan, S. Parkinson, Y. Qin, Fog computing security: a review of current applications and security solutions. J. Cloud Comput. **6**(1), 19 (2017)
7. P.G. Lopez et al., Edge-centric computing: vision and challenges. ACM SIGCOMM Comput. Commun. Rev. **45**(5), 37–42 (2015)
8. B.A. Martin et al., OpenFog Security Requirements and Approaches, (November, 2017), pp. 1–6
9. R. Roman, J. Lopez, M. Mambo, Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges. Futur. Gener. Comput. Syst. **78**, 680–698 (2016)
10. J. Tan, R. Gandhi, P. Narasimhan, *Challenges in Security and Privacy for Mobile Edge-Clouds* (Parallel Data Laboratory, Carnegie Mellon University, 2013). http://www.pdl.cmu.edu/PDL-FTP/associated/CMU-PDL-13-113.pdf
11. S. Yi, Z. Qin, Q. Li, Security and privacy issues of fog computing: A survey, in *10th International Conference on Wireless Algorithms, Systems, and Applications*, ed. by K. Xu, H. Zhu (Eds), (Springer International Publishing, 2015), pp. 685–695. https://doi.org/10.1007/978-3-319-21837-3_67
12. Y. Guan, J. Shao, G. Wei, M. Xie, Data security and privacy in fog computing. IEEE Netw. **99**, 1–6 (2018)