All these devices are wirelessly connected to the patient’s smartphone, which always runs the frontend application component

It also interacts with neighboring lights to coordinate the green traffic wave. Based on this information the smart light sends warning signals to approaching ...

All these devices are embedded in, or wirelessly connected to, the patient's smartphone, which always runs the frontend application component. The backend ..

An external attacker is not equipped with key materials in a vehicular fog computing system, while an insider attack is one originating from compromised smart vehicles, fog nodes, or

Existing security research mainly focuses on the identification of potential attacks, threats, and vulnerabilities of fog-assisted vehicular applications.

Unlike existing vehicular networks, these units/nodes will have more functions and provide more diverse services for smart vehicles, such as navigation, video streaming, and smart traffic lights.

Smart vehicles play an important role as the key data generator in a vehicular fog computing system, due to their real-time computing, sensing (e.g., cameras, radars and GPS), communication, and storage capabilities

These include the traffic scheduling algorithms, ITLC and ATL, for controlling the traffic lights of an isolated traffic intersection and the entire road network , and a distributed real-time

A cloud server can be composed of several processing units, such as a rack of physical servers or a server with multiple processing cores. In each layer, nodes are divided into domains where a single IoT-fog-cloud application is implemented. For instance, a domain of IoT nodes is shown in dark green, and they communicate with a domain of fog nodes associated with the application.

Normally the fog nodes in one domain are placed in close proximity to each other, for example, in a single zip-code or in levels of a building. Each domain of fog nodes is associated with a set of cloud servers for a single application. The basic way in which IoT nodes, fog nodes, and cloud nodes operate and interact is as follows.

In this section, we introduce the framework in which fog nodes collaborate with each other to fulfill the requests sent from IoT nodes to the fog layer. However, when the fog node is busy processing many tasks, it may offload the request to some other fog nodes or to the cloud. The concept of Load Sharing is well studied in the literature , , and we borrow similar concepts for the design of the policy by which fog nodes collaborate. In this subsection, we discuss the decision fog nodes make for processing or offloading a task to other fog nodes.

Similarly, a license plate reading request in a recorded video of a vehicle, sent by a traffic camera to fog nodes is an example of heavy processing task

Although the IoT can play a central role in delivering a rich portfolio of services more effectively and efficiently to end users, it could impose security and privacy challenges. In the following, we summarize the major security and privacy challenges in IoT environments.

a. Authentication These resource-constrained devices can outsource expensive computations and storage to a fog device that will execute the authentication protocol.

While traditional PKI based authentication could solve the problem, it wouldn’t scale well for IoT systems.

b. Trust Trust models based on reputation have been successfully deployed in many scenarios such as online social networks. Kai Hwang and colleagues proposed a new approach to improve the trust in clouds, which combines security-reinforced data centers, data access, and virtual clusters directed by reputation systems. To design a trust model based on reputation in the IoT, we need to tackle how to maintain the service reliability and prevent accidental failures, handle and identify misbehavior issues, identify malicious behavior correctly, and bootstrap building a trust model based on reputation in large-scale networks.

c. Rogue Node Detection Their approach protects the networks from rogue access points even if the adversaries use customized equipment. A rogue IoT node has the potential to misuse users’ data or provide malicious data to neighboring nodes to disrupt their behaviors.

d. Privacy The privacy leakage of user information in IoT environments, such as data, location, and usage, is attracting the attention of the research community. Another privacy issue is the location privacy that can be used to infer the IoT device’s location. The last privacy issue is the protection of a user’s usage pattern of some generated data by IoT devices, such as in the smart grid. Many privacy-preserving schemes have been proposed in different IoT applications such as smart grids, healthcare systems, and vehicle ad hoc networks. IoT devices limit the techniques that can be used to deliver efficient and effective privacy-preserving schemes.

e. Intrusion Detection Intrusion detection techniques detect misbehavior or malicious IoT devices and notify others in the network to take appropriate actions. Most of the existing techniques in the IoT target a few attacks with low efficiency. Additionally, the complicated design of intrusion detection techniques that meets the limited resources in the IoT is another challenging task