Fog Computing
2024/25 - Autumn 2025 - UiO

Security Issues

Prof. Paulo Ferreira

paulofe@ifi.uio.no

UiO/IFI/PT

Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. J. Ni, K. Zhang, X. Lin and X. Shen. IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601-628, 2018 (first quarter), IEEE. doi: 10.1109/COMST.2017.2762345.

Features of Fog Computing

- **Fog computing is a distributed framework that offers IoT applications at the edge of the network by leveraging edge resources**

- The **major feature of fog computing** is:
  - to **tackle the IoT data locally** by utilizing the **fog nodes placed near users** to bring about the convenience of data storage, computation, transmission, control and management

- **Compared with cloud computing, fog computing has five distinguished features**:
  - **location** awareness
  - **geographic** distribution
  - low **latency**
  - **large-scale** IoT applications support
  - **decentralization**

Fog-Assisted IoT Applications

- We have mentioned various **fog-assisted IoT applications according to different roles of fog nodes**, which contribute to the development of smart city, and its critical components, including **smart transportation, smart grid, smart e-healthcare and other related aspects**
- The Table in this slide illustrates the **fog assisted IoT smart-city applications**

Components	Fog-assisted IoT Applications
Smart Transportation	Traffic Management and Surveillance [24], Decentralized Vehicular Navigation [50], Smart Traffic Lights [57], Inter-state Bus Entertainment [57], Parking Sharing and Management [71], Road Surface Condition Monitoring [72].
Smart Grid	Home Energy Management [41], Microgrid Energy Management [41], Energy Consumption Collection [58], Smartphone Energy Saving [73].
Smart Healthcare	Wearable Big Data Analysis [25], Speech Treatments of Patients with Parkinson's Disease [25], Smart E-health Gateways [26], Fall Detection for Stroke Patients [40], Prediction of Sudden Cardiac Death [43], Patient Activity Tracking [58], Patient Care in Hospitals [58], Human Health Monitoring [74].
Others	Shopping Cart Management [7], Software and Credential Updating [10], Smart Industry Automation [24], Fog-radio Access Networks [38], [55], Finding A Missing Child [43], Local Content Distribution [53], Edge Content Caching [55], Indoor Location and Navigation [59], Fog-based Malware Defense [63], Fog-based Crowdsensing [75], Emergency Alert Service [76], Fog-empowered Anomaly Detection [77], Fog-based Proximity Detection [78], Fog-based Location Verification [79], Fog-based Vehicular Data Scheduling [80].

Video on Security in Fog Computing

https://www.youtube.com/watch?v=K2vLNtvJcQE

Security Threats of Fog Computing

Security Threats of Fog Computing (1/3)

- **Cloud computing is vulnerable to be hacked by external attackers** because of the centralized data storage and computing framework
- In the major cloud computing vendors, such as Google, Amazon and Yahoo, successively appeared large-scale **data leakage accidents**
- **Cloud security** has become an important factor **restricting** the development of cloud computing
- As a non-trivial extension of cloud computing, **fog computing is considered to be a more secure architecture than cloud computing**
- Firstly:
  - the **collected data is transiently maintained and analyzed on local fog node closest to data sources**, which **decreases the dependency on the Internet connections**
  - local data storage, exchange and analysis make it **difficult for hackers to gain access to users' data**
- Secondly:
  - the **information exchange between the devices and the cloud no longer happens in real-time**, so that it is **hard for eavesdroppers to discern the sensitive information of a specific user**

Security Threats of Fog Computing (2/3)

- However, **fog computing cannot be deemed to be secure**, since it **still inherits various security risks from cloud computing**
- In general:
  - the **fog nodes and clouds are honest-but curious**
  - they are **deployed by fog and cloud vendors** to offer specific services honestly to users for their own benefits
  - on one hand, **for monetary reasons, they may not deviate from the protocols agreed upon among the ones involved**,
  - on the other hand, **they may snoop on the content of maintained data and the personal information about data owners**
  - further, the **employees in fog or cloud service providers might acquire personal information about users**, resulting in the privacy leakage for users
  - in addition, the fog nodes or cloud servers **may become the major targets of hackers that use any possible method to reach their own goals unscrupulously**
- Therefore, the **fog nodes or cloud servers could be honest-but-curious, even malicious**

Security Threats of Fog Computing (3/3)

- Specifically, an attacker may launch the following **attacks to disrupt the fog computing**:

- forgery
- tampering
- spam
- sybil
- jamming
- eavesdropping
- denial-of-service
- collusion
- man-in-the-middle
- impersonation

Security Threats of Fog Computing-forgery

- **Malicious attackers may not only forge their identities and profiles**, but also **generate fake information to mislead other entities**
- In addition, the **network resources, such as bandwidth, storage and energy, would be excessively consumed by the faked data**

- forgery
- tampering
- spam
- sybil
- jamming
- eavesdropping

- denial-of-service
- collusion
- man-in-the-middle
- impersonation

Security Threats of Fog Computing-tampering

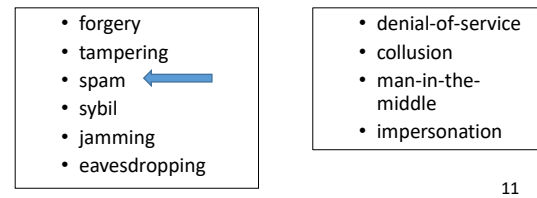
- A **tampering attacker could maliciously drop, delay or modify transmitting data to disrupt fog computing and degrade its efficiency**
- It is **difficult to detect** some tampering behaviors, since the **wireless channel condition and user mobility may result in transmission failure and delay**

- forgery
- tampering
- spam
- sybil
- jamming
- eavesdropping

- denial-of-service
- collusion
- man-in-the-middle
- impersonation

Security Threats of Fog Computing-spam

- **Spam data refers to the unwanted content**, such as redundant information, false collected data from users, which is **generated and spread by attackers**
- **Spam** would result in the **unnecessary network resource consumption**, **misleading social friends, and even privacy leakage**

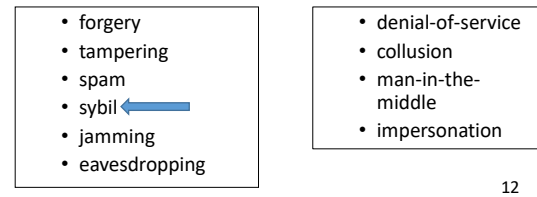


11

11

Security Threats of Fog Computing-sybil

- A Sybil attack is a type of attack on a computer network service in which **an attacker subverts the service's reputation system by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence**
- It is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder
- **Sybil attackers either manipulate fake identities** or **abuse pseudonyms** in order to **compromise or control the effectiveness of fog computing (subverts the service's reputation)**
- For example, they could **generate incorrect crowdsensing reports**, such that the **crowdsensing results may not be trustworthy**
- In addition, **sybil attackers could invade legitimate user's private information**



12

12

Security Threats of Fog Computing-jamming

- An **attacker deliberately generates a huge number of bogus messages to jam communication channels or computing resources**, such that other users are prohibited from normal communication and computation

- forgery
- tampering
- spam
- sybil
- jamming ⟵
- eavesdropping

- denial-of-service
- collusion
- man-in-the-middle
- impersonation

13

Security Threats of Fog Computing-eavesdropping

- **Malicious attackers listen on communication channels to capture transmitting packets and read the content**

- This type of network **attack is quite effective if the data lacks encryption**

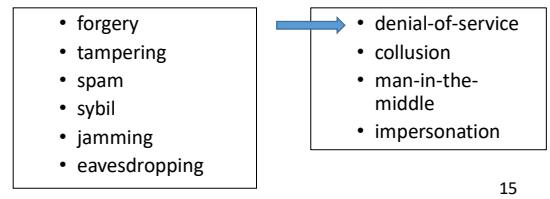
- forgery
- tampering
- spam
- sybil
- jamming
- eavesdropping ⟵

- denial-of-service
- collusion
- man-in-the-middle
- impersonation

14

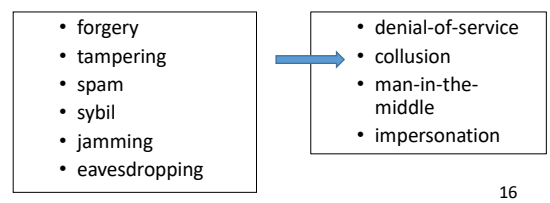
Security Threats of Fog Computing-denial-of-service

- An attacker disrupts the services provided by fog nodes to make them unavailable to its intended users, by **flooding the target fog nodes with superfluous requests**
- This **attack consumes network resources to prevent the requests from legitimate users from being fulfilled**
- A **fog node is pretty vulnerable to denial-of-service (DoS) attacks** compared with the cloud as its available resource is limited



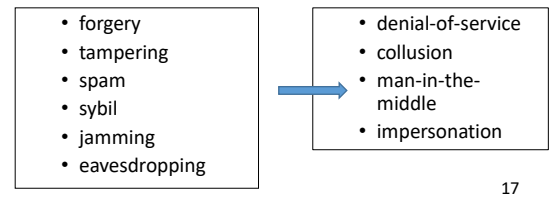
Security Threats of Fog Computing-collusion

- **Two or more parties collude together to deceive, mislead, or defraud other legal entities or obtain an unfair advantage**
- In fog computing, **any two or more parties can collude** to increase their attack capability, such as several fog nodes, IoT devices, IoT devices with the cloud, or fog nodes with IoT devices



Security Threats of Fog Computing-man-in-the-middle

- A malicious attacker **stands in the middle of two parties to secretly relay or modify the exchanging data between these parties**, however, **these two parties believe that they are directly communicating with each other**

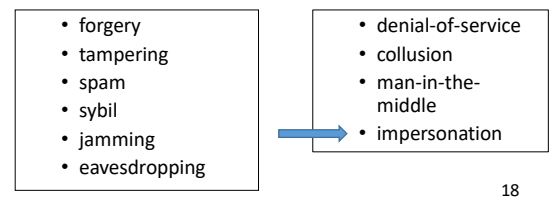


17

17

Security Threats of Fog Computing-impersonation

- A malicious **attacker pretends to be a legitimate user** to enjoy the services provided by fog nodes, or impersonates a legitimate fog node to **offer fake or phishing services to users**



18

18

Security Threats of Fog Computing - Privacy

- In addition, **privacy is a critical issue in fog computing as the users' sensitive data is involved in the collection, transmission, processing and sharing**
- **Data owners are not willing to expose their privacy to others**, but the leakage of privacy is oblivious
- A **user's privacy** may include four aspects, that is:
  - **identity** privacy
  - **data** privacy
  - **usage** privacy, and
  - **location** privacy

Privacy Threats of Fog Computing

Security Threats of Fog Computing-identity privacy

- The **identity of a user includes the name, address, telephone number, visa number, license number and public-key certificate** (i.e., any information can link to a specific user)
- Users' identities are **vulnerable to be disclosed from the information submitted to fog nodes for authentication**

- **identity** privacy
- **data** privacy
- **usage** privacy, and
- **location** privacy

Security Threats of Fog Computing-data privacy

- **Users' data may be exposed to an untrusted party** when they are maintaining fog nodes, and transmitting between two parties
- By analyzing these data, **various sensitive information can be obtained**, such as a user's preference, occupation, address, health status and political inclination
- For example, a **medical record poses the patient's health status**, and a **vote exposes the voter's political intention**

- **identity** privacy
- **data** privacy
- **usage** privacy, and
- **location** privacy

Security Threats of Fog Computing-usage privacy

- Usage privacy mainly refers to the **usage pattern with which a user utilizes the services offered by fog nodes**
- For example, the **readings of a smart meter may disclose the living habits of a family**, such as at **what time the residents go to sleep**, and at **what time they are not at home**, which **absolutely violates residents' privacy**

- **identity** privacy
- **data** privacy
- **usage** privacy, and
- **location** privacy

Security Threats of Fog Computing-location privacy

- Currently, **massive applications on mobile devices collect users' location information**
- It seems that **location privacy is a kind of privacy that we have to sacrifice in order to enjoy online services**, such as navigation and location-based services:
  - however, location privacy preservation is critical indeed
- From the collected location information, an attacker is able to **identify a user's trajectory, identity, points of interest**, etc., resulting in the **exposure of users' privacy**
- Unfortunately, it is **difficult to protect users' locations in fog computing:**
  - as a **user can access the services provided by the nearest fog node using IoT devices**, this **fog node can infer that this user is nearby** and far from other fog nodes
  - moreover, **if a user accesses multiple services offered by the fog nodes deployed at different locations, it may disclose the path trajectory to the fog nodes**

- **identity** privacy
- **data** privacy
- **usage** privacy, and
- **location** privacy

Summary of Security and Privacy in Fog Computing

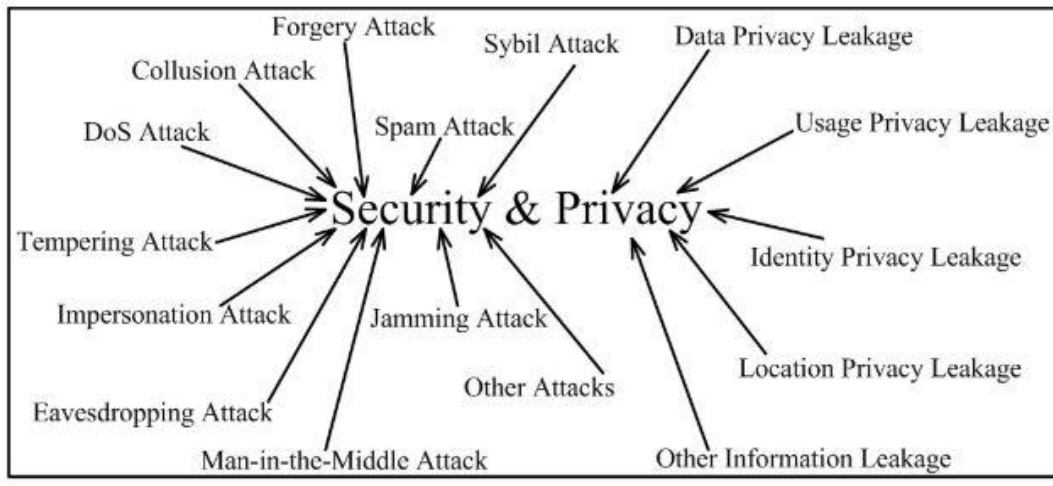
Security Threats of Fog Computing (1/3)

- **IoT devices are the major sources of security threats of fog computing**
- With the **increasing number of connected IoT devices**, the **vulnerability of IoT devices exacerbates users' concerns on security and privacy**
- Due to the **lack of sufficient security protection**, IoT devices are vulnerable to be hacked, broken or stolen:
  - these compromised devices can **become powerful and distributed sources to corrupt normal services**
- In October 2016, an Internet company, Dyn, was crippled by massive distributed DoS **attacks from a large number of unsecured Internet-connected devices**, such as home routers and surveillance cameras, which repeatedly disrupt the availability of Twitter, Netflix, Amazon and PayPal
- **IoT botnets will remain a huge threat** towards the network services
- Besides, **illegal network access frequently happens in a public environment**

Security Threats of Fog Computing (2/3)

- Kaspersky Lab detected almost **3.5 million pieces of malware on more than 1 million user devices in 2014**
- The **malware steals credentials** to gain access to the target hosted networks and services
- In summary, the **IoT devices have been a new weapon for hackers**, which **brings enormous security risks towards the availability and reliability of IoT services**, and thereby **triggers numerous security and privacy threats** towards the infrastructure of fog computing and cloud computing
- Due to the security and privacy threats in place (as shown in the Figure in the next slide) it is **crucial to build efficient and effective secure and privacy-preserving mechanisms in fog computing**
- **Without appropriate security and privacy protection, users may be unwilling to participate in IoT applications**, which prevents the success of fog computing

Security Threats of Fog Computing (3/3)



Conclusion

- Fog computing is a new **decentralized architecture** that revolutionizes the cloud computing by extending storage, computing and networking resources to the network edge for supporting extremely large-scale IoT applications
- However, **it is also confronted with traditional security threats**, which raise various new security and privacy challenges towards users