VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management

CSE3502

Digital Assignment 1

Edge computing security, attacks, preventive measures, tools, security standards and policies

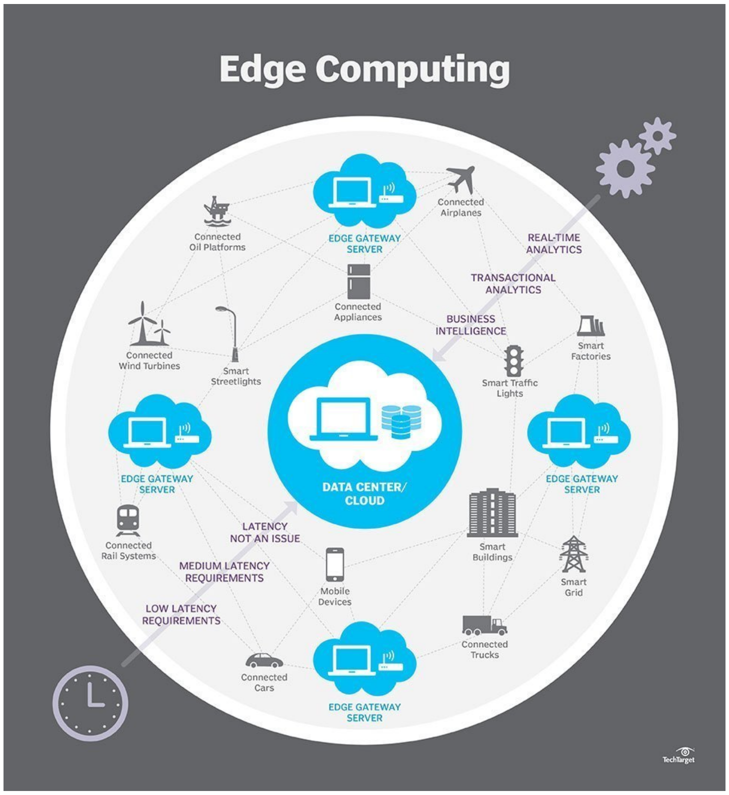
Slot : F2

Name : Kulvir Singh

Register Number : 19BCE2074

Introduction to Edge Computing

Edge computing is a distributed computing paradigm that brings computation and data storage closer to the sources of data. This is expected to improve response times and save bandwidth. As mentioned, it is an information technology infrastructure which is distributed in nature in which client data is processed at the periphery of the network, as close to the originating source as possible.
In simplest terms, edge computing moves some portion of storage and compute resources out of the central data center and closer to the source of the data itself. Rather than transmitting raw data to a central data center for processing and analysis, that work is instead performed where the data is actually generated -- whether that's a retail store, a factory floor, a sprawling utility or across a smart city. Only the result of that computing work at the edge, such as real-time business insights, equipment maintenance predictions or other actionable answers, is sent back to the main data center for review and other human interactions.



a summarizing diagram on edge computing technology as given by TechTarget
(https://www.techtarget.com/searchdatacenter/definition/edge-computing)

Security Risks for Edge Computing

As discussed above, for devices involving edge computing, the tip point devices are generally located off from the centralized servers and data storage server. Since IOT and also the linked edge computing devices are deployed faraway from the centralized data infrastructure, it makes it harder to watch from both a digital and physical security standpoint.

Listed below are the first security risks for devices and systems which use edge computing :

1) Protection of Stored Data and Proper Storage of Data
   Data that's gathered and processed at the sting lacks the hardened physical security of more centralized assets. By simply removing a Winchester drive from a grip resource, or by copying data from an easy memory device, vital information can potentially be compromised. and since of limited local resources, it will be tougher to confirm reliable data backup.

2) Authentication and Authorization
   Edge devices are often not supported by security-minded operations professionals, and plenty have very lax password discipline. In fact, hackers have sophisticated ways to compromise password protocols. In 2017 a “botnet barrage” (where bots were deployed to go looking for devices running default passwords) attacked 5,000 IoT devices at a university campus by 5,000 discrete systems, trying to find weak passwords.

3) Data Sprawl
   As companies deploy more and more edge devices to manage a wider array of operations, it gets harder to trace and monitor. Over time, devices may even outgrow boundaries of the sting, creating bandwidth overcrowding and endangering the protection of multiple devices. because it grows, IoT traffic also increases latency and may compromise security when data is shipped unprocessed.

Attacks, Vulnerabilities and Threats :

1) Injection of Malicious Hardware or Software
   Hackers seeking to corrupt, steal, alter, or delete data circulating within edge networks have some different hardware- and software-based tools at their disposal, particularly when it involves the infection and manipulation of edge nodes, or the servers and devices located at the sting.Attackers can inject unauthorized software and hardware components into the sting network that wreak havoc on the efficacy of existing edge servers and devices and even provide service provider exploitation, by which those entities providing the software and hardware solutions that make edge computing possible begin unwittingly executing hacking processes on the attacker’s behalf.

2) Routing Information Attacks

There are 4 main routing information attacks that are discussed below :

a) *Black Holes*

During a region attack, incoming and outgoing network data packets are simply deleted, ensuring that they never reach their destination. This decreases throughput and might increase latency if the information has to be retransmitted. The lower the throughput and also the higher the latency, the more serious the network performs.

b) *Gray Holes*

A gray hole attack is sort of a region attack but instead involves gradually and selectively deleting data packets during a network. this sort of attack is more sophisticated than the part attack, and per se, may be harder to spot.

c) *Wormholes*

A wormhole attack involves recording packets at one network location, tunneling them to a different, and replaying them. in step with a study conducted at the University of British Columbia, a strategic placement of a wormhole can disrupt a mean of 32 percent of all communications across a commercial hoc network.

d) *Hello Flood Attack*

Finally, there’s the Hello Flood attack, within which a malicious node broadcasts hello packets to nodes claiming to be their neighbor, causing general routing confusion within the network.

3) Distributed Denial of Service (DDoS) Attacks

Distributed denial of service (DDoS) attacks, whereby an existing network resource is overwhelmed with traffic from other compromised resources within the network, are another edge computing security risk to bear in mind of. In their paper, the IEEE researchers highlighted three famous DDoS attacks disbursed nervy computing devices, specifically: outage attacks, sleep deprivation attacks, and battery draining attacks.
An outage attack has occurred when a DDoS attack causes nodes to prevent functioning altogether. A sleep deprivation attack is when adversaries overwhelm nodes with legitimate requests that keep them from entering a power-saving state, which greatly increases power consumption. Battery draining attack, or barrage attack, can cause an outage by sapping certain nodes or sensors of their battery life through the continued re-execution of energy-demanding programs or applications.

4) Physical Attacks and On-Site Tamper

Physical tampering of devices may be a likely possibility in a foothold computing architecture, counting on their location and level of physical protection from adversaries. Edge computing, by its very nature, creates an increased attack surface by locating computational resources closer to data sources. Although an increased attack surface creates more ground to hide for physical attackers seeking to compromise entire edge

networks, the very fact that there’s a greater number of devices during a greater number of places also makes physical attacks that much easier to hold out.
Once physical access is gained, attackers can: extract valuable and sensitive cryptographic information, tamper with node circuits and alter or modify node software and operating systems software and operating systems

Preventative Measures

Some of the counter measures for edge computing security attacks are listed below :

- Side-channel signal analyses, which detect hardware trojans using timing, power, and spatial temperature analyses. Basically, this method detects malicious firmware or software installed edgy nodes by identifying unusual system behaviors, like increases in execution time and power consumption.

- Trojan activation methods, which compare Trojan-afflicted integrated circuits with non-Trojan-afflicted circuits to detect and model malicious attacks

- Circuit modification or replacing, which could be a series of countermeasures that gives protections at the circuit level and even allows the node to self-destruct within the event of an attack

- Establishing reliable routing protocols and implementing a high-quality intrusion detection system (IDS) that monitors for malicious traffic and detects policy violations can function as effective countermeasures against routing information attacks. Nodes with reliable routing protocols can create a table of trusted nodes for sharing sensitive information, the researchers say, and an adequate IDS can detect common routing information attacks, like black holes.

- For sleep deprivation and battery draining attacks, the security professionals suggest policy-based mechanisms. These are established to ensure that standard rules within the network are not broken. Basically, they control the behavior of devices within a network. So, if a sleep deprivation or barrage attack is initiated, a predefined security policy will identify it as suspicious or unusual, allowing administrators to contain the attack quickly.

Tools :

In this section, a few tools that can be used for detecting attacks and vulnerabilities of edge computing systems as well as the mitigation of attacks are listed.

Intrusion Detection Systems :

An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system.

Trojan Killer by Grind Soft Anti Virus Solutions:

A tool which is deployed to kill the Trojan virus that has infected the system and exterminate it.

Inspector Side Channel :

A tool which analyses the side channel attacks and gives a detailed report about it. This product was developed by riscure.

Important Points for POLICY DEVELOPMENT of Edge Computing Security Features

- **People**
  Human-Computer Interaction is the basic step for providing a robust policy for edge computing security. Individuals must be trained on cyber security tactics, learnings must be constantly re-enforced, and there must be a change in cultural mindset on the importance of edge computing security.
- **Procedures**
  Proper governance should be taken care while handling the edge computing devices. The usage of these devices should be governed by the procedures that are accepted by the client as well as the host.
- **Process**
  A set of processes should be defined for the devices in case of a security breach. A systematic approach to incident response and incident handling should be laid out so that the attacks can be prevented or mitigated.
- **Quality Check and Product Control**
  Regular testing and auditing of the devices to the security features applied should be carried out by performing dummy attacks and other auditing processes.

References

https://identitymanagementinstitute.org/edge-computing-security-and-challenges/
https://arxiv.org/ftp/arxiv/papers/2008/2008.03252.pdf
https://www.sciencedirect.com/science/article/pii/S1877050919317181
https://www.kaspersky.com/blog/secure-futures-magazine/edge-computing-cybersecurity/31935/
https://internetofthingsagenda.techtarget.com/tip/Edge-computing-security-risks-and-how-to-overcome-them
https://www.ibm.com/cloud/what-is-edge-computing
https://www.techtarget.com/searchdatacenter/definition/edge-computing