Edge-Computing Paradigm: Survey and Analysis on Security Threats

BY – DINKI CHITKARA
Test Engineer,QA

TABLE OF CONTENTS

ABSTRACT

The commencement of extensive applications of IoT devices in the world of information technology are generating massive amount of data. The deployment of various IoT devices/sensors within the complex interconnected networks give rise to raw data from sensors, processed and controlled data, decision making data providing intelligent solution etc. IoT provide a common platform (called IoT cloud) for all the networks and devices connected to those networks so that the analytics can be performed on data and valuable information can be extracted. Huge data traffic generated by IoT sensors and related processing pose an overwhelming load and cost on IoT cloud related to bandwidth, latency and resource scarcity. This in turn degrades the quality of service (QoS) and network performance. To cope with such issues, Edge Computing (EC) paradigms came into existence extending the cloud storage capacity and computational resources in near proximity to specific IoT devices. Although EC assisted IoT reduce the volume of data transition over cloud but continued with major risks associated with the security and privacy. Moreover, the expansion of service requirement triggers the security and efficiency issues.

CONTEXT

The need for offloading data to nearby edge nodes demands sufficient storage, lower transmission rates, and cost-effective computation. To fulfill all these services, edge nodes are equipped with varied enabling technologies like wireless sensor networking, lightweight virtualization, and task offloading from the cloud to the edge. All these factors contribute to lay the foundation for security threats.

This white paper intends to address:
1) Edge Architecture,
2) Edge security threats and various problems/challenges in edge computing and
3) Approaches for alleviating those issues.

Keywords-Edge Computing, Internet of Things, Cloud, IoT devices, edge devices, security threats, benefits, challenges.

INTRODUCTION

IoT has been around for a lot longer when the internet- a very essential component of IoT was invented. A wide range of applications requires implanting of sensors to exhibit intelligence like humans and make intelligent decisions by performing analytics on the produced Analog data by sensors. Before falling into the internet gateway for processing, the data is digitalized and aggregated by Data Aggregation System (DAS) and lastly, it falls into the realm of the IT cloud for further processing. Time-sensitive IoT services and applications, such as smart transportation, or smart city, would, nevertheless, experience unacceptable long delays as the computational servers are situated far away from the end-user. The idea behind edge computing is to cope up with these issues and provide a secure structured mechanism for serving critical data.

EDGE ARCHITECTURE

The science of installing cloud computing-like capabilities to the network's edge is known as edge computing. Recent researches in edge paradigms like Mobile Edge Computing, Mobile Cloud Computing, Cloudlet Computing intend conspicuous understanding to Edge Computing that shares a common functional structure.

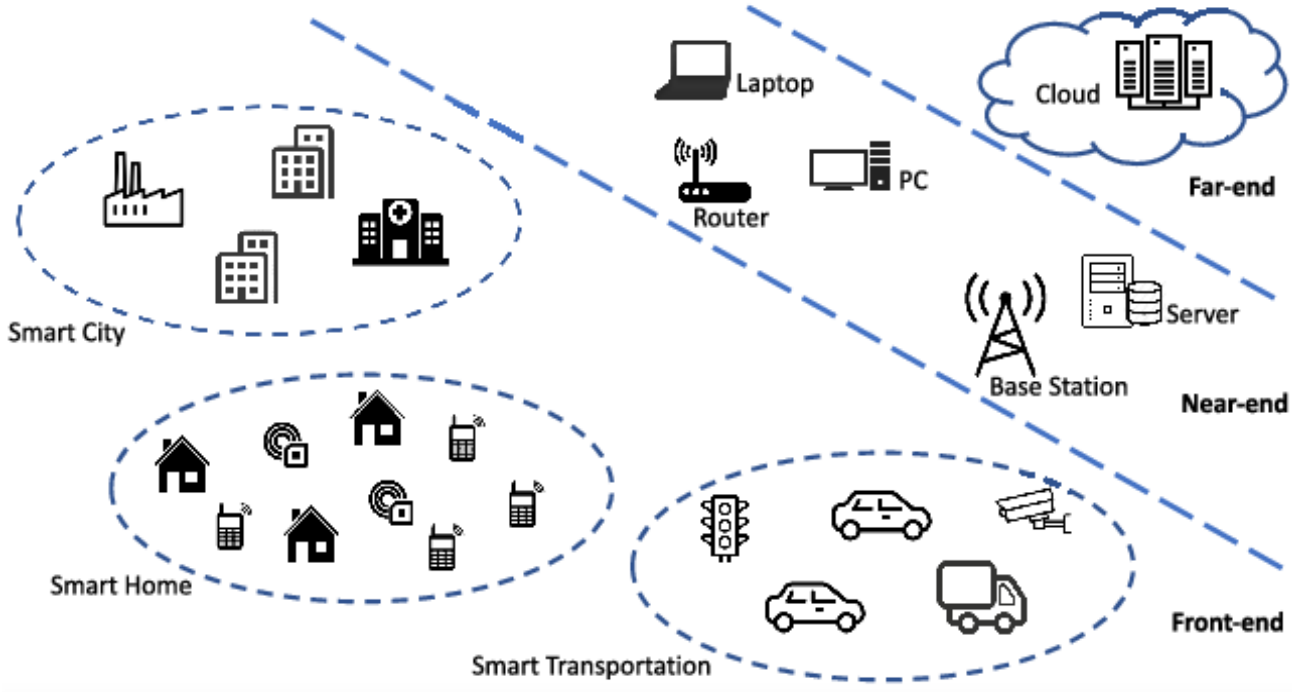

Figure 1: A typical architecture of edge computing networks.

Edge is a broad expansion of IoT. Edge framework is a multi-layer distributed computing mechanism circumscribing and positioning the workload between edge nodes. As shown in Fig. 1, the functioning of edge computing has distributed into three primary nodes: i) device edge, ii) local edge node [divided into edge server (application workload layer) and edge gateway (network layer) as mentioned above] and iii) cloud.

The edge devices which are deployed at the front end of architecture can be categorized into three main classes based on the limited computation that it offers: constrained devices, single-board computers, and mobile devices. The constrained devices category includes any IoT device used for different objectives, such as surveillance, automotive systems, and many others.

Various tools and technologies are deployed for the implementation of near end node. The Autonomous Distributed Cooperative Technology allocates tasks processing by distributing them among several edges. The huge amount of processing that is required for applications workload, is achieved by combined use of FPGA (Field Programmable Gate Array) with high power- saving CPU and additionally by optimum implementation of algorithms.

The computing paradigms whether it is edge or cloud has been driven by virtualisation technology like server virtualisation, OS-level Virtualisation (docker), traditional hypervisor virtualization, light weight virtualization.

PROBLEMS AND CHALLENGES

Despite the benefit, the deployment of edge computing will lift unintended security issues in different layers.

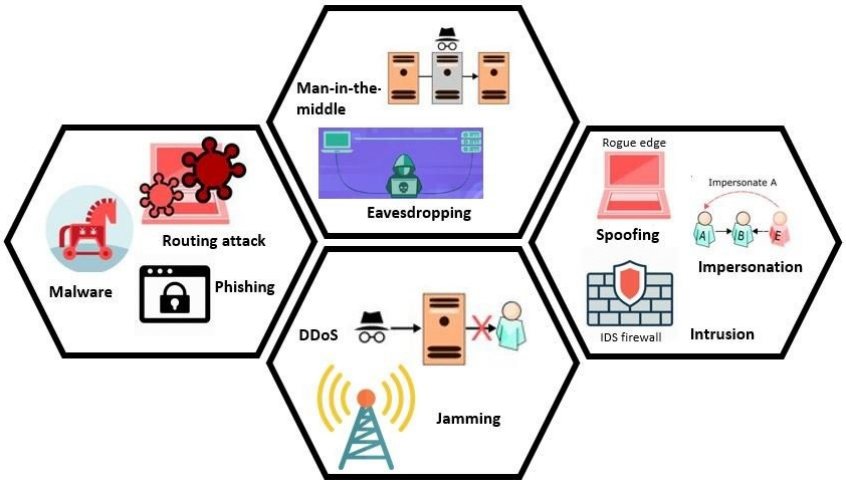

Figure 2: Security and Privacy attacks in Edge Computing.

I. SECURITY ATTACKS IN PHYSICAL LAYER

HARDWARE TROJAN ATTACK: Hardware Trojans have emerged as a significant security concern for integrated circuits. Such an attack will be accomplished by malicious alterations of circuit structure by untrusted fabrication facilities. These modifications provide a backdoor for the leak of sensitive information. The hardware Trojan attack could be triggered by some activation mechanism that activates the trojan's malicious behavior. Trojans have two types based on their activation mechanism; a) internally activated Trojans, which can be triggered and activated if a specific condition within the IC's is met, and b) Trojans that are activated by sensors or transceivers that interact with the outside world are known as externally activated Trojans. Furthermore, the hardware trojan attack can be active and passive.

CAMOUFLAGE: It is a type of passive attack where an attacker inserts counterfeit edge nodes to monitor the traffic of data packets flowing from sensor nodes to base stations. An attacker monitors which nodes are sending packets and then follow those sending the most packets. Near to this, the counterfeit node could be inserted which acts as a normal node for obtaining, processing, sending, or redirecting packets.

NODE REPLICATION: It is a type of active attack in which the attacker inserts a malicious node and breaks the security mechanism through replication. By copying (replicating) the node ID of an existing sensor node, an attacker attempt to add a node to an existing sensor network. A sensor network's performance can be accurately disrupted by a node replicated in this manner, packets can be corrupted or even misguided. Furthermore, if the attacker can acquire physical access to the entire network using other related attacks, he can copy cryptographic keys to replicated sensor nodes and insert the replicated nodes into strategic points in the network. The attacker could easily manipulate a specific segment of the network by inserting replicated nodes at strategic network points, perhaps by disconnecting it all together.

DENIAL OF SERVICE (DoS) ATTACK: There are three main types of Denial of Services attacks against edge devices. DoS occurs when the edge devices stop functioning its proper functioning due to battery drainage, sleep deprivation attack, or unchecked error in the manufacturing process. The limited energy capacity of edge devices due to small batteries makes them vulnerable to serious consequences such as failure to report an emergency. As we can see, with the help of this example that if an attacker can find a way to

drain a smoke detector's battery, the entire fire detection system will be disabled. Adversaries fill EC nodes with an unwanted set of legitimate requests in a sleep deprivation attack. This kind of attack is way more difficult to detect than a battery-draining attack.

MANIPULATIVE RFID (RADIO FREQUENCY IDENTIFICATION) ATTACK: This attack is against the RFID tags. RFID uses radar technology because there's no battery inside of this RFID tag. Since, this is a wireless communication, so many of the vulnerabilities like data capture between RFID tag and RFID reader. RFID attacks are used to extract and save information from tags for future analysis or manipulate the tags for further counterfeiting. If the RFID tag is an active tag that contains information that can be changed, adversaries can even spoof the RFID reader and send information to the tag that might modify the contents of that RFID tags itself. The adversaries can also interfere with frequencies associated with RFID communication creating a denial-of-service situation.

II. SECURITY ATTACKS IN COMMUNICATION AND NETWORK LAYER

This layer purpose to establish the connection between edge servers, edge devices, and the core framework(cloud) with wireless networks, data center network, and the internet along with various networking and routing protocols. The various attacks associated with this layer of communication are:

JAMMING ATTACKS: In this scenario, the edge nodes are exhausted with intentionally jamming the transmission of radio signals with the flood of fraudulent messages. This will affect the latency capabilities when authorized user unable to use the EC infrastructure to serve the demands of time- sensitive applications. Depending on the flow of counterfeit messages, jamming attacks can be divided into, i) intermittent jamming (also called as non- continuous jamming) in which jamming is periodic and as result, the nodes can send/receive packets periodically ii) continuous jamming that involves complete jamming and block away mostly every transmission .

INJECTING FRAUDULENT PACKETS: In this type of attack the attacker feeds fraudulent packets into the communication channel by three different techniques: i) insertion, ii) manipulation and iii) replication (also called replay). In an insertion attack, the attacker inserts a new malicious packet into the communication link. This attack invokes the ability for the malicious packet to act like the normal packet by generating and sending counterfeit

packets that seem admissible. In a manipulation attack, the communication link is accessed by the attacker to capture packets for manipulations. One of the security requirements to encounter security attacks is that of data freshness. Data freshness ensures that the transmitted data should not be replayed by changing the shared keys over time. However, propagation of the new key across the entire network takes time. In such a scenario, the adversary can implement the replay attack. If the system is unaware of the new key exchange, this attack can cause sensor malfunction. Generally, a stateless system, which does not keep a record of previous data packets are quite vulnerable to these species of attacks.

UNAUTHORISED CONVERSATION: In wireless sensor edge communication, the edge node required to communicate only to those nodes which can help with any sort of relative data. Else if the nodes are dedicated to each one of the other nodes, the attacker might be able to access the control on entire communication layer. This type of attack typically coils applications like smoke detector in home automation where the quick decision and action has to be taken to secure the entire infrastructure.

ROUTING INFORMATION ATTACKS: These attacks affect how messages are routed from source to destination. In this attack, attackers change the routing information by redirecting or dropping data packets at the communication level. Various attacks are launched by using malicious EC nodes. The malicious EC nodes might be: i) Black Holes, which simply drop all network's packets by attracting all the network traffic at the malicious node, ii) Gray Holes, a variation of the black hole which drains selective packets, iii) Worm Holes, in which attackers will first record packets at one network location then tunnels them to a different location, iv) Hello Flood, A malicious EC node broadcasts 'HELLO PACKETS' to all nodes claiming to be their fellow companions, v) The Sybil attack is defined as attackers using malicious technology to take on multiple identities illegitimately in order to outvote the system's original nodes.

III. SECURITY ATTACKS IN EDGE SERVER LAYER

The edge servers allocate multiple computation resources to the edge devices. Providing multiple management services to the end user, the edge data centers are integrated with various machine learning algorithms and multi-tenant virtualization technologies. As a repercussion, adversaries can implement several types of attack.

INTEGRATED ATTACK AGAINST MACHINE LEARNING: The adversaries can launch attacks against the machine learning algorithm in which

attackers directly access the server or computing node where the learning algorithms are running, or the attacker might be able to pollute the training datasets by adding a sufficient number of malicious nodes to the lower-level layers.

INESSENTIAL LOGGING ATTACK: Maintaining logs of each entry is a nice approach to distinguish false access or intrusion. The developers should log events of credentials such as successful/unsuccessful validation attempts, successful/unsuccessful permission-requesting attempts, and application errors. Also, the logging should be encrypted to avoid unnecessary data leakage as this can additionally provide sensitive information to attackers might be helpful in launching side-channel attacks.

TAMPERING OR PHYSICAL ATTACK: Large distribution of edge data centers elevated the risk of physical attacks as they can be situated in unguarded buildings which will impact the security and integrity of processed and computed data, sensitive information can be extracted and the software are left modified for the benefit of attackers. Such a case can only happen when attacker sabotage the edge centers physically.

SOLUTIONS TO SECURITY ATTACKS

I. *TRADITIONAL NETWORKING*

As in traditional networks, the request of client travel from one router to another depending on the routing protocol like IGP, RIP and configurations assigned to individual router by controlling panel. The traditional networking approach are divided into two capabilities:
Control plane- it is often called as the brain of router in which routing protocols and certain services e.g., distributed network services are described. It also prepares routing table.
Forwarding plane- it checks the source IP of the packet from the interface and transmits it.

The following conclusions can be made when implementing traditional networking approach:

1) There is no predefined rule to transfer data packet from source to destination, it is decided by router to inhibit which of the underlying route at the time of packet transmission to destination.
2) *The router is an intelligent device which, with the help of routing table forwards the packet from one interface to another interface. Each router performs their own calculations, computations and updating signals.*

II. *SOFTWARE DEFINED NETWORKING*

In software-defined networking, the control panel is uprooted from the entire router network and the SDN controller is implanted into the network's core. An SDN switch consists of a packet forwarding plane that communicates to the centralized SDN via an open flow protocol. SDN Controller is defined as a centralized structure for the network that can communicate and command the rest of the network with the help of incorporated Software like load balancing software, security software, etc. SDN helps to monitor the whole network structure, ease the network processing and provide a secure mechanism for transmitting packets to a destination.

SDN efficiently works to alleviate the security attacks in the communication and network layer as discussed above. In Software-Defined networking, it is quite convenient to integrate IDS (Intrusion Detection System) to monitor data traffic and scan data packets so that malicious code can be detected for various applications to work correctly. Furthermore, VLAN ID can be used to isolate different types of traffic into VLAN groups, which can be utilized to further segregate malicious traffic for data security and prioritization.

However, the security of SDN controller is still a challenge to be addressed.

III. *HOMOMORPHIC ENCRYPTION*

Edge computing encounters many security challenges like fraudulent data injection, unauthorized communication which violates the confidentiality and integrity of data. In the traditional cryptographic techniques, the data is stored in an encrypted format and the manipulation is performed on the decrypted data. The encrypted data is not of any use to the adversaries and hackers, as it is translated into ciphertext or complex code, that can't be read by humans. But while encryption safeguards the private data as it's being stored or transferred, the data must be decrypted to be processed. This provides a window of opportunity for the data to be exposed making it vulnerable to cyber-criminals, attackers.

Homomorphic encryption is introduced by IBM in 2009 to combat this issue by allowing for computation to be done on encrypted data without even decrypting the ciphertext and the user may outsource computation or allow other entities to perform computation for the data without giving access to the raw data. Hence, message confidentiality is maintained while data processing. This encryption can be largely used for applications like healthcare, crypto-currency where privacy and confidentiality are paramount.

CONCLUSION

With the advancement of the Internet of Things, edge computing existed as a nascent technology that provides resource capabilities in a distributed fashion at the edge of the network, which has proven to be both efficient and effective in managing the ubiquitous influence of edge devices/ sensors.
Moreover, the rapid development of enabling technologies like lightweight virtualization and most advanced secure networking have formed factors for edge paradigms. This paper presents a survey on significant security threats occurring at different levels of edge architecture and it’s solutions.

REFERENCES

1) https://www.nec.com/en/global/techrep/journal/g17/n01/170105.html
2) https://www.kaspersky.co.uk/resource-center/threats/ddos-attacks
3) https://youtu.be/quuat3SHEMY
4) https://www.ibm.com/cloud/blog/architecting-at-the-edge
5) https://sdettech.com/the-future-of-iot-testing-emerging-trends-and-technologies/