A Survey of Security Architectures for Edge Computing-Based IoT

Alessandro Carrega

TNT Lab – DITEN
University of Genoa

Information 1/2

- Lecturer: **Dr. Alessandro Carrega**.
  - *Email*: alessandro.carrega@unige.it.
  - *Skype*: alessandro.carrega@gmail.com.
  - *Telegram / Whatsapp*: **3487485497**.
- Duration: **20 hours**.
- Language: **English**.
- Lesson in site and remote (Teams).

Information 2/2

- Dedicated Teams channel:
  - **PhD STIET Cyber security approaches for Cloud/Edge Environments**

    https://teams.microsoft.com/l/team/19%3a-Dtnw_NHUAl1AjZZV4HixIifmU8gywbskeeQwSV--uk1%40thread.tacv2/conversations?groupId=bdafff5c-0ab9-44b2-aef2-5a14e1dd6e15&tenantId=6cd36f83-1a02-442d-972f-2670cb5e9b1a
- GitHub repository:
  - https://github.com/tnt-lab-unige-cnit/phd-stiet-cyber-security-approaches-cloud-edge-environments
- Optional homework.
  - Available in Teams and GitHub.
- Final Exam with 3 options:
  - **Theoretical**: *short survey with 3 papers*.
  - **Pratical**: *2 exercises*.
  - **Quiz**: *100 multiple choice questions (**60%** to pass the exam)*.

Security Threats 1/24

Malicious hardware/software injection 1/5

- Unauthorized software/hardware components to communication or EC node levels can be added by attackers that inject malicious inputs into EC servers.
- Adversaries able to exploit service providers to perform hacking processes on their behalf, such as bypassing authentication, stealing data, reporting false data, or exposing database integrity.
- Hardware injection attacks have several classifications.

Security Threats 2/24

Malicious hardware/software injection 2/5

Node replication

- Adversaries inject a new malicious node into an existing set of nodes by replicating one node’s ID number.
- Attackers will be able to corrupt, steal, or misdirect data packets arriving at malicious replica.
- Required access to extract cryptographic shared keys can be obtained by attackers causing severe damage to system.
- Implementing node revocation protocols, legitimate EC nodes can be revoked by node replicas.
- *Active* attack.

Security Threats 3/24

Malicious hardware/software injection 3/5

- If attackers gain illegitimate access to integrated circuits (ICs), they can appear as hardware trojan.
- Attackers will be able to control circuit and access data or even software running on these ICs.
- 2 types of Trojans
  1. *internally* activated Trojans: activated by satisfying a particular condition inside ICs;
  2. *externally* activated Trojans: activated using sensors or antennas that interact with outside world.

Security Threats 4/24

Malicious hardware/software injection 4/5

- Attackers can also camouflage by injecting a fake EC node into network or attack an authorized node to be able to hide at edge level.
- Counterfeit/modified EC node will work as a normal EC node to receive, share, process, store, redirect, or transmit data packets.
- Node is able to operate in a passive mode and only analyses traffic.
- *Passive* attack.

Security Threats 5/24

Malicious hardware/software injection 5/5

- Attackers gain unauthorized access and control of network, taking advantage of corrupted or malicious EC nodes, then inject misleading data packets or can block delivery of legitimate data packets.
- Attack can be launched using 3 different attack methods
  1. *insertion*: attacker inserts malicious packets (that seem legitimate) in network communication;
  2. *manipulation*: attacker captures packets, then change them;
  3. *replication*: previously exchanged packets between two nodes have been captured and replayed by attacker.

Security Threats 6/24

Side-channel attacks

- Compromise security and privacy of users by any accessible information that is not privacy-sensitive in nature, called side-channel information.
- Accessible information usually has some correlations with privacy-sensitive data.
- Attackers explore hidden correlations and extract desired sensitive information from side-channel information using specific algorithms or machine learning models.
- Most popular side channels in EC are: *communication signals*, *electric power consumption*, and *smartphone/proc filesystem* or *embedded sensors*.

Security Threats 7/24

Authentication and authorization attacks can be categorized into 4 types: 1/2

1. *dictionary* attacks: attacker utilizes a credential/password dictionary to crack into authentication of a system;
2. *attacks exploiting vulnerabilities in authentication protocols*: attackers discover design flaws of authentication protocols.
   Most widely adopted authentication protocols in edge computing are Wi- Fi-protected access (WPA/WPA2) and secure sockets layer (SSL)/transport layer security (TLS) protocols;

Security Threats 8/24

Authentication and authorization attacks can be categorized into 4 types: 2/2

3. *attacks exploiting vulnerabilities in authorization protocols*: attackers usually exploit design weaknesses or logic flaws existing in authorization protocols to gain unauthorized access to sensitive resources or perform privileged operations.
   Most widely adopted authorization protocol in edge computing is open authorization (OAuth) protocol;
4. *overprivileged* attacks, happen if an app or a device is granted stronger access rights or more than what is needed.

Security Threats

Jamming attack

- Special type of denial-of-service (DoS) attack.
- Network will be flooded intentionally by attackers using counterfeit messages to exhaust communication, computing, or/and storage resources.
- Attack will make authorized users unable to use infrastructure of EC-based IoT network.

Security Threats 10/24

Most famous types of *distributed denial-of-service* (DDoS) attacks against EC nodes are outage attacks, sleep deprivation, and battery draining. 1/2

- In outage attacks, EC nodes do not perform their normal operations because of unauthorized access by attackers.
- In sleep deprivation, attackers overwhelm EC nodes with too many legitimate requests.
- Attack is very hard to detect. In battery draining, batteries of sensors, devices, or EC nodes are depleted; therefore, node failure or outage occurs.
- Most common DDoS attack at communication level is jamming transmission of signals, including continuous jamming over all transmissions and intermittent jamming by sending/receiving packets periodically by EC nodes.

Security Threats 11/24

Most famous types of *distributed denial-of-service* (DDoS) attacks against EC nodes are outage attacks, sleep deprivation, and battery draining. 2/2

- DDoS attacks in edge computing can be classified as flooding-based attacks and zero-day attacks.
- In flooding-based attacks (e.g., UDP flooding, SYN flooding, HTTP flooding), attacker tries to saturate server and shut down normal service of a server by flooding with malicious/malformed network packets.
- A zero-day attack is more difficult to implement. In zero-day DDoS attacks, attacker should find an unknown vulnerability, i.e., a zero-day vulnerability in code running on target edge device/server.
- These vulnerabilities can trigger memory failure/corruption, resulting in a service shutdown. A zero-day attack is also difficult to defend since it exploits a zero-day unknown vulnerability.

Security Threats 12/24

- *Physical attacks/tampering* happen when attackers can access EC nodes/devices physically.
- Attackers can extract valuable and sensitive cryptographic data, tamper with circuit, or modify software/operating systems.

Security Threats

- *Eavesdropping* or *sniffing* attacks occur when adversaries covertly listen to private conversations, such as usernames, passwords, etc., over communication links.
- Attackers will be able to gain crucial information about network, for instance, when sniffed packets contain control or access information of EC nodes, such as configurations and identifiers of nodes or passwords of shared network.

Security Threats

- EC nodes can reveal critical information even when they are not transmitting any data as nonnetwork side-channel attacks.
- For example, detection of known electromagnetic/acoustic signals or protocols from medical devices can lead to serious privacy issues since critical information about patient and device can be leaked.

Security Threats 15/24

- By redirecting, misdirecting, spoofing, or dropping data 1/2 packets at communication level, attackers can change routing information and affect how messages are routed.
- Routing information attacks can appear in different types
  1. *altering* attack: routing information will be modified by attacker, for instance, through routing loops or false error messages;
  2. *blackhole* attack: malicious node attracts all traffic by advertising shortest path to destination, then attacker processes packets sent to malicious node or just drops them;
  3. *gray hole* attack: kind of blackhole attack in which selective packets will be dropped;

Security Threats 16/24

- By redirecting, misdirecting, spoofing, or dropping data packets at communication level, attackers can change routing information and affect how messages are routed. 2/2
- Routing information attacks can appear in different types

4. *worm hole* attack: attacker records packets at one network location first, afterward will tunnel them to another location;
5. *hello flood* attack: attacker sends “HELLO PACKETS” to all other nodes using high transmission power malicious node claiming that it is their neighbour;
6. *sybil* attack: attacker uses/adds nodes with fake identities called sybil nodes that are able to out-vote genuine nodes in system.

Security Threats

- Attackers in *forgery* attacks inject new fraudulent data packets and interfere with receiver, which causes system damage or failure.
- Data packets can be inserted into communication links using methods such as inserting malicious data packets that seem legitimate, capturing then modifying data packets, and replicating previously exchanged packets between two EC nodes/devices.

Security Threats

- Neighbouring EC nodes communicate with each other to access or share data, but every node should only communicate with those nodes that need its data.
- In unauthorized control access, attackers can control whole neighbouring nodes if they gain access to one of unsecured EC nodes.

Security Threats

- Two types of *integrity attacks against machine learning* can happen in machine learning methods used in EC-based IoT

  1. *causative* attack: attackers change training process of machine learning models by manipulating or injecting misleading training data set;
  2. exploratory attack: attackers misuse vulnerabilities without changing training process.

Security Threats 20/24

- *Replay* attacks or *freshness* attacks: attackers capture and record data traffic for particular period of time and then use these historical data to replace current real-time data.
- Energy and bandwidth consumption of EC nodes and other adverse effects.

Security Threats 21/24

- *Insufficient/inessential logging* attacks can damage EC-based IoT systems when log files are not encrypted.
- System and infrastructure developers must log events such as application errors and attempts of unsuccessful/successful authorization/authentication.

Security Threats 22/24

- *Security threats from/on IoT devices* include mobile botnets, ransomware, and IoT malware.
- In 2017, over 1.5 million attacks were reported that originated from mobile malware.
- Threats can lead to data leakage/corruption or even application death.

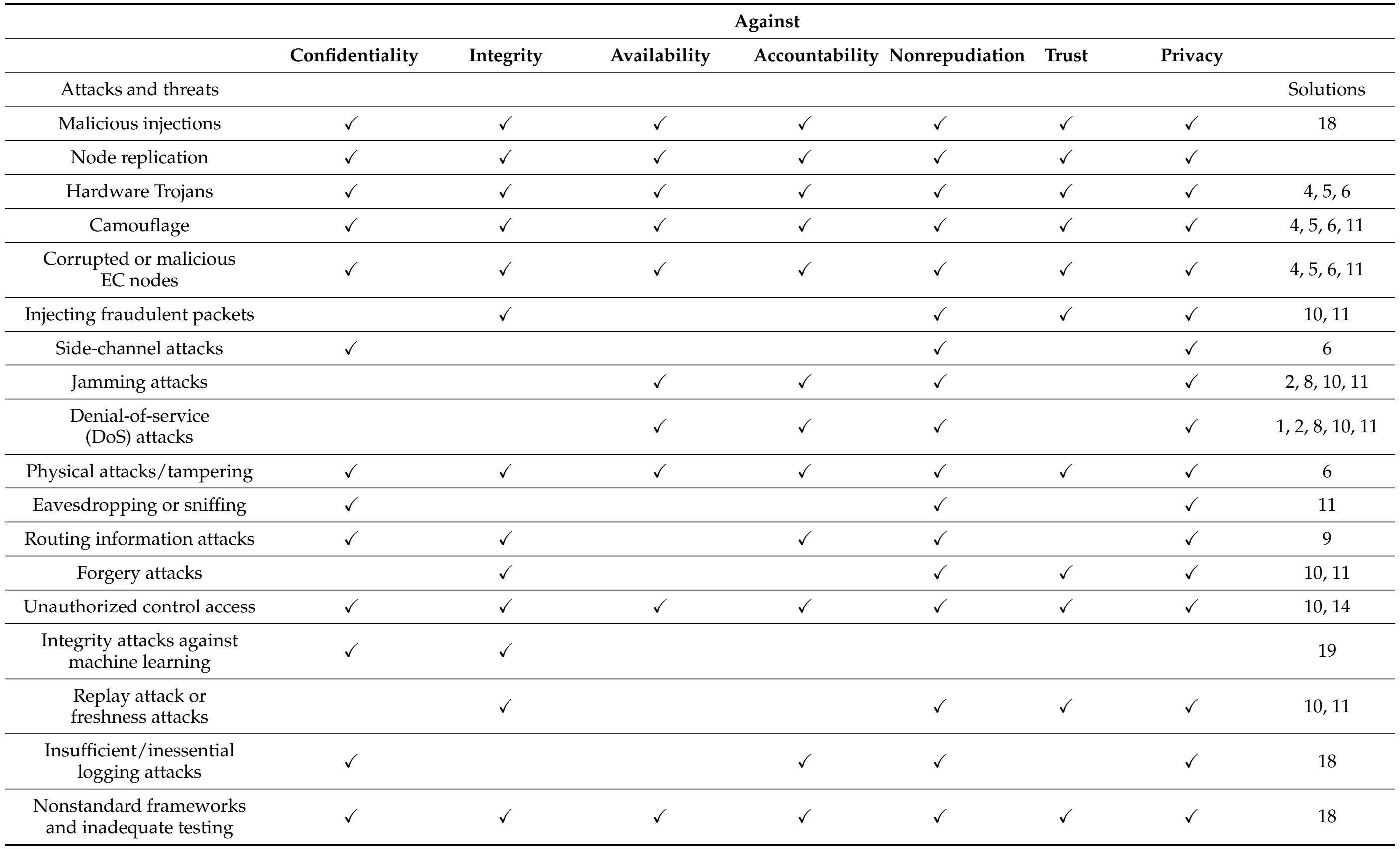
Security Threats 23/24

- *Nonstandard frameworks and inadequate testing* and coding flaws are able to cause serious security and privacy attacks.
- Nodes usually need to be connected to intermediate servers; therefore, compromise could be increased.
- EC-based system development is complicated procedure that needs to combine heterogeneous devices/resources created by diverse manufacturers.
- No standard framework or policy for implementation of EC-based systems.
- Some security and privacy flaws may stay undetected.

Security Threats 24/24

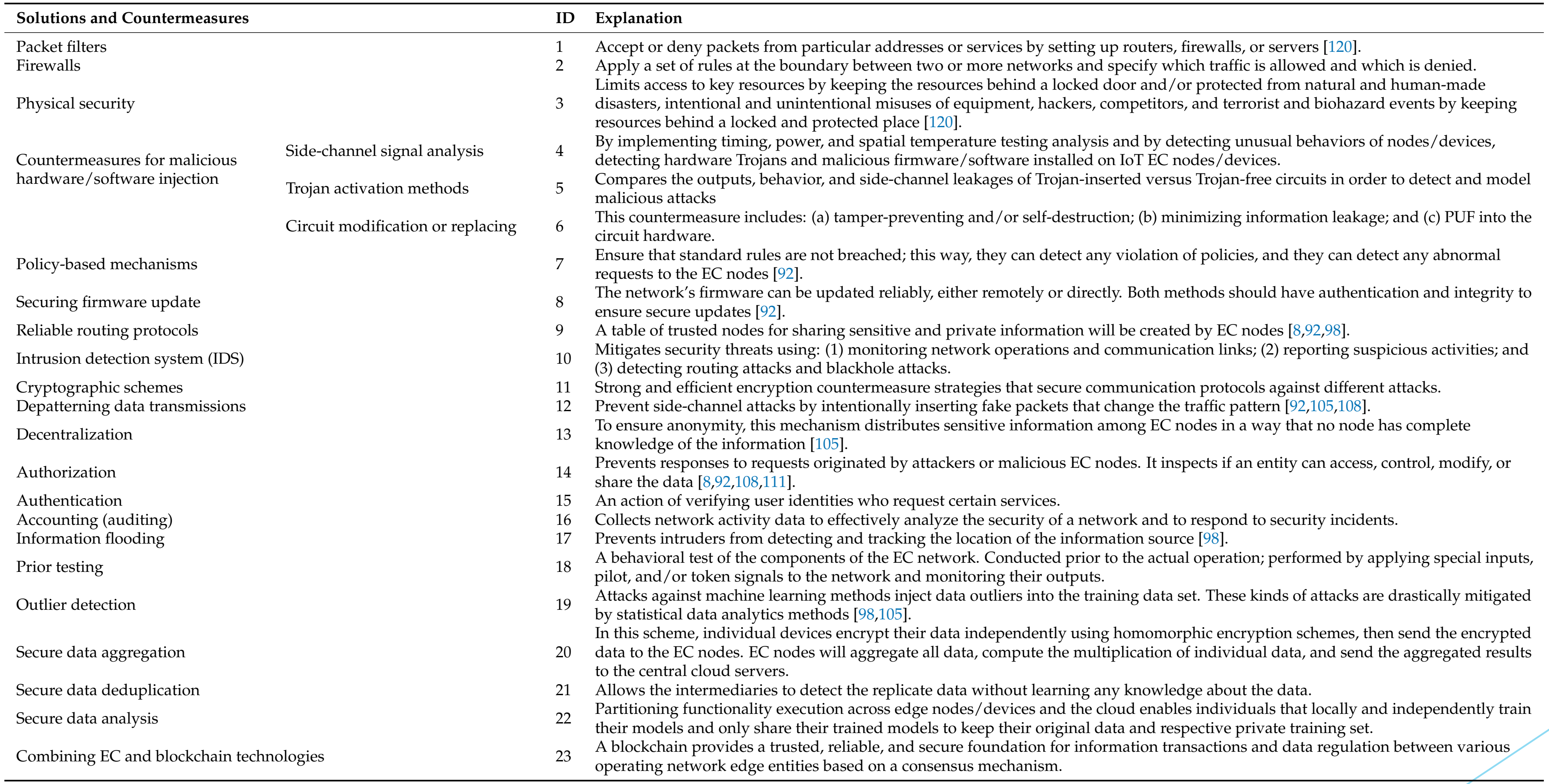
- Functionalities of EC nodes may need to extract personal data from information generated by user devices.
- Sensitive information (such as personal activities, preferences, or health status) that must belong to data owners could be shared with other users or network entities without any permission from data owners, which makes them vulnerable to intruders during data transmission/sharing, causing privacy leakage. Location awareness of EC nodes.
  - e.g., Wi-Fi hotspots and Base Stations (BSs) can be exploited by attackers, and then they can detect and track device's physical location or other sensitive information from physical location of EC nodes.
- If users connect to multiple EC nodes simultaneously to access particular service, physical location of user's device can be precisely detected using positioning techniques.

Security Threats & Solutions



	Against							
	Confidentiality	Integrity	Availability	Accountability	Nonrepudiation	Trust	Privacy	
Attacks and threats								Solutions
Malicious injections	✓	✓	✓	✓	✓	✓	✓	18
Node replication	✓	✓	✓	✓	✓	✓	✓	
Hardware Trojans	✓	✓	✓	✓	✓	✓	✓	4, 5, 6
Camouflage	✓	✓	✓	✓	✓	✓	✓	4, 5, 6, 11
Corrupted or malicious EC nodes	✓	✓	✓	✓	✓	✓	✓	4, 5, 6, 11
Injecting fraudulent packets		✓			✓	✓	✓	10, 11
Side-channel attacks	✓				✓		✓	6
Jamming attacks			✓	✓	✓		✓	2, 8, 10, 11
Denial-of-service (DoS) attacks			✓	✓	✓		✓	1, 2, 8, 10, 11
Physical attacks/tampering	✓	✓	✓	✓	✓	✓	✓	6
Eavesdropping or sniffing	✓				✓		✓	11
Routing information attacks	✓	✓		✓	✓		✓	9
Forgery attacks		✓			✓	✓	✓	10, 11
Unauthorized control access	✓	✓	✓	✓	✓	✓	✓	10, 14
Integrity attacks against machine learning	✓	✓						19
Replay attack or freshness attacks		✓			✓	✓	✓	10, 11
Insufficient/inessential logging attacks	✓			✓	✓		✓	18
Nonstandard frameworks and inadequate testing	✓	✓	✓	✓	✓	✓	✓	18

Security Solutions 1/15



Solutions and Countermeasures		ID	Explanation
Packet filters		1	Accept or deny packets from particular addresses or services by setting up routers, firewalls, or servers [120].
Firewalls		2	Apply a set of rules at the boundary between two or more networks and specify which traffic is allowed and which is denied.
Physical security		3	Limits access to key resources by keeping the resources behind a locked door and/or protected from natural and human-made disasters, intentional and unintentional misuses of equipment, hackers, competitors, and terrorist and biohazard events by keeping resources behind a locked and protected place [120].
Countermeasures for malicious hardware/software injection	Side-channel signal analysis	4	By implementing timing, power, and spatial temperature testing analysis and by detecting unusual behaviors of nodes/devices, detecting hardware Trojans and malicious firmware/software installed on IoT EC nodes/devices.
	Trojan activation methods	5	Compares the outputs, behavior, and side-channel leakages of Trojan-inserted versus Trojan-free circuits in order to detect and model malicious attacks
	Circuit modification or replacing	6	This countermeasure includes: (a) tamper-preventing and/or self-destruction; (b) minimizing information leakage; and (c) PUF into the circuit hardware.
Policy-based mechanisms		7	Ensure that standard rules are not breached; this way, they can detect any violation of policies, and they can detect any abnormal requests to the EC nodes [92].
Securing firmware update		8	The network's firmware can be updated reliably, either remotely or directly. Both methods should have authentication and integrity to ensure secure updates [92].
Reliable routing protocols		9	A table of trusted nodes for sharing sensitive and private information will be created by EC nodes [8,92,98].
Intrusion detection system (IDS)		10	Mitigates security threats using: (1) monitoring network operations and communication links; (2) reporting suspicious activities; and (3) detecting routing attacks and blackhole attacks.
Cryptographic schemes		11	Strong and efficient encryption countermeasure strategies that secure communication protocols against different attacks.
Depatterning data transmissions		12	Prevent side-channel attacks by intentionally inserting fake packets that change the traffic pattern [92,105,108].
Decentralization		13	To ensure anonymity, this mechanism distributes sensitive information among EC nodes in a way that no node has complete knowledge of the information [105].
Authorization		14	Prevents responses to requests originated by attackers or malicious EC nodes. It inspects if an entity can access, control, modify, or share the data [8,92,108,111].
Authentication		15	An action of verifying user identities who request certain services.
Accounting (auditing)		16	Collects network activity data to effectively analyze the security of a network and to respond to security incidents.
Information flooding		17	Prevents intruders from detecting and tracking the location of the information source [98].
Prior testing		18	A behavioral test of the components of the EC network. Conducted prior to the actual operation; performed by applying special inputs, pilot, and/or token signals to the network and monitoring their outputs.
Outlier detection		19	Attacks against machine learning methods inject data outliers into the training data set. These kinds of attacks are drastically mitigated by statistical data analytics methods [98,105].
Secure data aggregation		20	In this scheme, individual devices encrypt their data independently using homomorphic encryption schemes, then send the encrypted data to the EC nodes. EC nodes will aggregate all data, compute the multiplication of individual data, and send the aggregated results to the central cloud servers.
Secure data deduplication		21	Allows the intermediaries to detect the replicate data without learning any knowledge about the data.
Secure data analysis		22	Partitioning functionality execution across edge nodes/devices and the cloud enables individuals that locally and independently train their models and only share their trained models to keep their original data and respective private training set.
Combining EC and blockchain technologies		23	A blockchain provides a trusted, reliable, and secure foundation for information transactions and data regulation between various operating network edge entities based on a consensus mechanism.

Security solutions 2/15

- *Packet filters* protect network resources from unauthorized use, theft, destruction, or DoS attacks.
- Two kinds of packet filter policies:
  1. one policy denies specific types of packets and accepts all others;
  2. second one accepts specific types of packets and denies all others.

Security solutions 3/15

Firewalls

- Can be applied as software, hardware appliance, or a router with Access Control Lists (ACLs).
- Some types of firewalls are:
  - *static stateless packet filter* firewalls that check packets individually and are optimized for speed and configuration simplicity;
  - *stateful* firewalls that allow or deny traffic by tracking communication sessions;
  - *proxy* firewalls that inspect packets, have support for stateful tracking of sessions, and able to block malicious traffic or unacceptable content.

Security solutions 4/15

Effective *countermeasures* techniques for malicious hardware/software injection 1/2

1. *Side-channel signal analysis:* detects both hardware Trojans by implementing timing, power, and spatial temperature testing analysis, and malicious firmware/software installed on EC nodes/devices by detecting unusual behaviours of nodes/devices. For instance, a significant increase in their heat, execution time, or power consumption;
2. *Trojan activation methods:* compare outputs, behaviour, and side-channel leakages of Trojan-inserted versus Trojan-free circuits to detect and model malicious attacks;

Security solutions 5/15

Effective *countermeasures* techniques for malicious hardware/software injection 2/2

3. *Circuit modification* or *replacing:* effective solution against physical/hardware, Trojan, and side-channel attacks.

   a) *tamper-preventing* and/or *self-destruction* to prevent malicious attacks, EC nodes are physically embedded with hardware, or in worst case, EC nodes destruct themselves and/or erase their data

   b) *minimizing information leakage*: random noise or delay is added to data intentionally to implement a constant execution path code and to balance Hamming weights;

   c) *embedding Physically Unclonable Function* (PUF) *into circuit hardware*; enables device identification and authentication to detect Trojan attacks.

Security solutions 6/15

Intrusion Detection System (IDS) 1/3

- 2nd line of defence to mitigate security threats by
  1. *monitoring* network operations and communication links;
  2. *reporting* suspicious activities: for example, when predefined policies are breached or when invalid information is injected into system;
  3. *detecting* routing attacks (e.g., spoofing or modification of information) and *blackhole attacks.*

Security solutions 7/15

Intrusion Detection System (IDS) 2/3

- *Hierarchical Distributed Intrusion Detection System* (HD-IDS) based on fog architecture is a hierarchical protection detection that deploys multiple IDSs in different network layers and performs detection by multiple layers collaboratively with traffic analysis.
  - Real time and precise protections.
  - HD-IDS is mainly for detecting traffic injection attacks.

Security solutions 8/15

Intrusion Detection System (IDS) 3/3

- *Real-Time Traffic Monitoring System* (RTMS): inspects data packets and matches SQLI pattern in IDS database to form signature rules, avoiding workload of manually writing signature rules.
- RTMS detects traffic injection attacks more efficiently.
- Mainly updates traffic injection signature rules through historical attack data analysis: requires relatively low real-time requirements for rule updates.

Security solutions 9/15

Cryptographic schemes

- Strong and efficient encryption countermeasure strategies used to secure communication protocols against different attacks, such as eaves-dropping or routing attacks.
- Wide variety of encryption/decryption strategies that can enhance network security and privacy; applicable for wired networks.
- Since EC nodes are usually small sensors with limited resources (e.g., battery power, computing/processing capabilities, and storage memory, employing standard encryption/decryption techniques will cause high memory usage, delay, and power consumption.
- Architectures and ideas of several key cryptosystems: *proxy* encryption, *attribute-based.*

Security solutions 10/15

- In EC-based IoT environment, entities are required to be authenticated mutually with one another across different trust domains.
- Authentication mechanisms:
  - single/cross-domain;
  - handover.

Security solutions 11/15

Accounting (*auditing*)

- Collecting network activity data to be able to effectively analyse security of a network and respond to security incidents.
- For networks with strict security policies, all attempts to achieve authentication and authorization by any person should be included in audit data.
- Logging "*anonymous*" or "*guest*" access to public servers is especially important.
  - All attempts by users to modify their access rights should also be logged in data.
- *Security assessment* is a further extension of auditing: network is examined from within by professionals trained in vulnerabilities exploited by network invaders.
- *Periodic assessments* of network vulnerabilities should be part of any security policy and audit procedure.
- *Specific plan* should be made for correcting deficiencies, which might be as simple as retraining staff.

Security solutions 12/15

Prior testing

- Behavioural test of whole and components of EC network (e.g., EC routers/nodes, servers, etc.) conducted prior to actual operation.
- Performed by applying special inputs, pilot, and/or token signals to network and monitoring their outputs.
- Identify possible attacks, simulate them, and evaluate their impacts on EC-based IoT.
- Defines which information must be logged and which is sensitive to be shared or stored.
- Input files should be inspected closely to prevent any malicious injection.

Security solutions 13/15

Secure data aggregation 1/2

- highly secure, privacy-preserving, and efficient data compression strategy.
- Individual devices encrypt their data independently using homomorphic encryption schemes - such as *Brakerski, Gentry, and Vaikuntanathan* (BGV) cryptosystem - then send encrypted data to EC nodes.
- EC nodes will aggregate all data, compute multiplication of individual data, and send aggregated results to central cloud servers.

Security solutions 14/15

Secure data aggregation 2/2

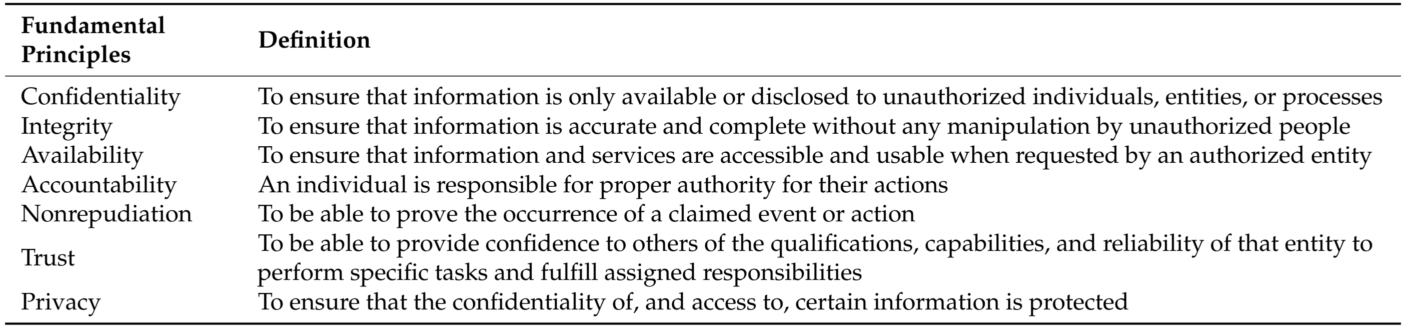
- Discarding replicate copies of data on intermediaries required to be able to save bandwidth in IoT networks.
- Disclose sensitive information to intermediaries or intruders.
- Data encryption is common to protect information and prevent data leakage.
- Not possible to detect replicate copies of data on intermediaries after encrypting data since all data will be transformed to random values.
- Secure data deduplication allows intermediaries to detect replicate data without learning any knowledge about data.

Security solutions 15/15

Combining EC and blockchain technologies

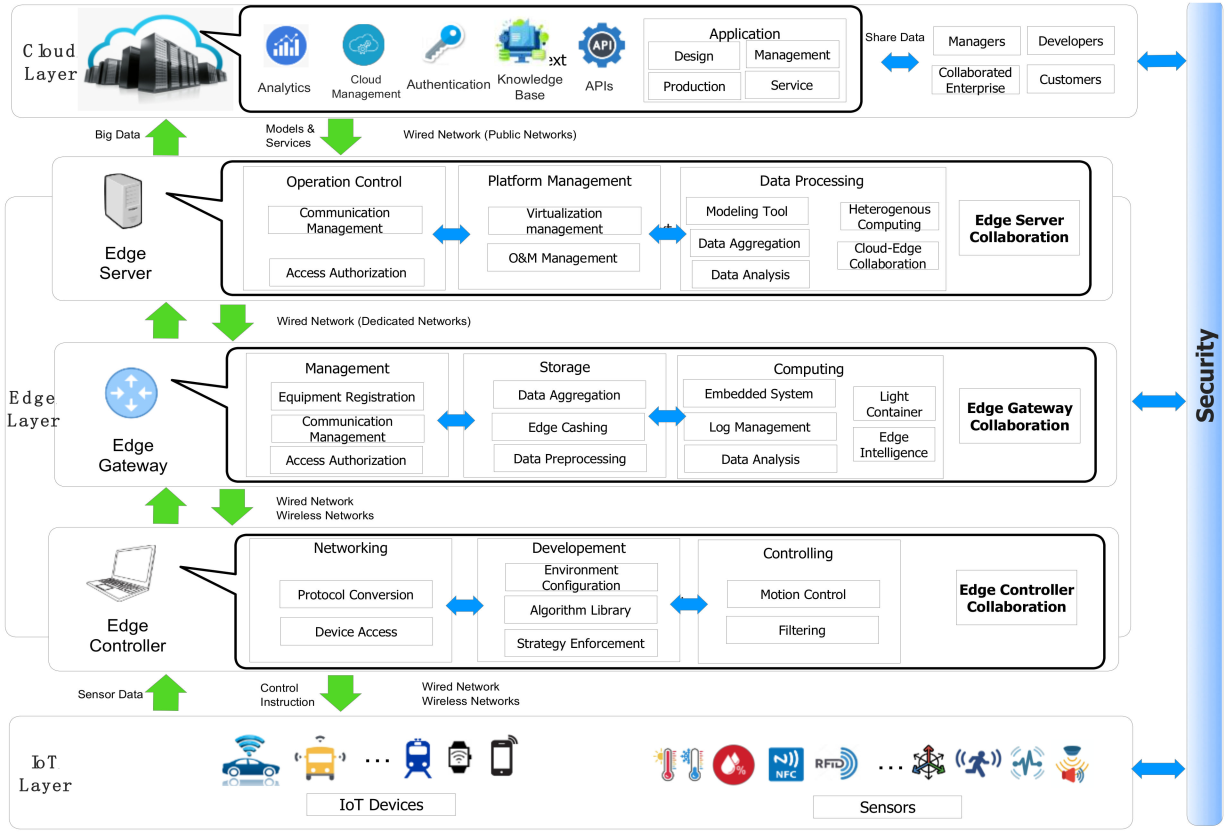
- Blockchain provides trusted, reliable, and secure foundation for information transactions and data regulation between various operating network edge entities.
- Decisions about correct execution of particular transactions are based on a consensus mechanism without depending on a trusted central authority between communicating IoT edge nodes.

Security Principles



Fundamental Principles	Definition
Confidentiality	To ensure that information is only available or disclosed to unauthorized individuals, entities, or processes
Integrity	To ensure that information is accurate and complete without any manipulation by unauthorized people
Availability	To ensure that information and services are accessible and usable when requested by an authorized entity
Accountability	An individual is responsible for proper authority for their actions
Nonrepudiation	To be able to prove the occurrence of a claimed event or action
Trust	To be able to provide confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities
Privacy	To ensure that the confidentiality of, and access to, certain information is protected

Secure architecture for edge computing-based IoT



C loud Layer

Analytics

Cloud Management

Authentication

ext Knowledge Base

APIs

Application

Design | Management

Production | Service

Share Data

Managers

Developers

Collaborated Enterprise

Customers

Big Data

Models & Services

Wired Network (Public Networks)

Edge Layer

Edge Server

Operation Control

Communication Management

Access Authorization

Platform Management

Virtualization management

O&M Management

Data Processing

Modeling Tool

Data Aggregation

Data Analysis

Heterogenous Computing

Cloud-Edge Collaboration

Edge Server Collaboration

Wired Network (Dedicated Networks)

Edge Gateway

Management

Equipment Registration

Communication Management

Access Authorization

Storage

Data Aggregation

Edge Cashing

Data Preprocessing

Computing

Embedded System

Log Management

Data Analysis

Light Container

Edge Intelligence

Edge Gateway Collaboration

Wired Network
Wireless Networks

Edge Controller

Networking

Protocol Conversion

Device Access

Developement

Environment Configuration

Algorithm Library

Strategy Enforcement

Controlling

Motion Control

Filtering

Edge Controller Collaboration

Sensor Data

Control Instruction

Wired Network
Wireless Networks

IoT Layer

RFID

NFC

IoT Devices

Sensors

Security