SLIIT
Discover Your Future

Sri Lanka Institute of Information Technology

IOT Ecosystem Security

Individual Assignment

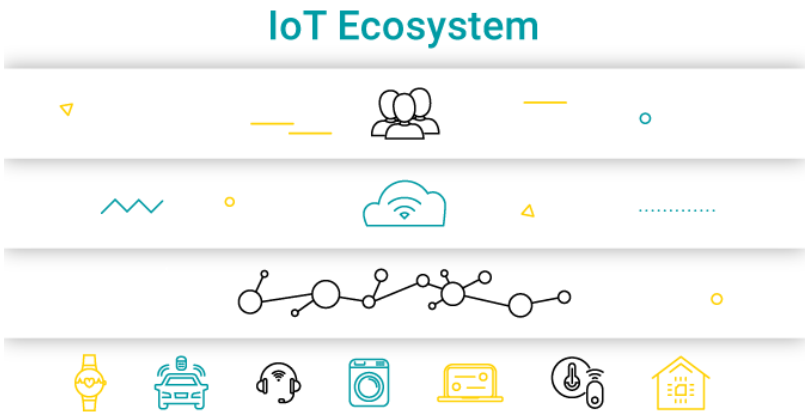
IE3032 – Network Security

Submitted by : IT20021870 || Dilshan K.N
Date of Submission : 14th March 2022

CONTENTS OF THIS TEMPLATE

What Is IOT Ecosystem

Internet of Things Ecosystem is a stunning network comprised of hardware, software, and applications that all interact and connect with one another via the internet and cloud technology. Through automation and machine learning, the Internet of Things connects devices, things, and software, as well as sharing information, enabling communication, allowing action and interaction.

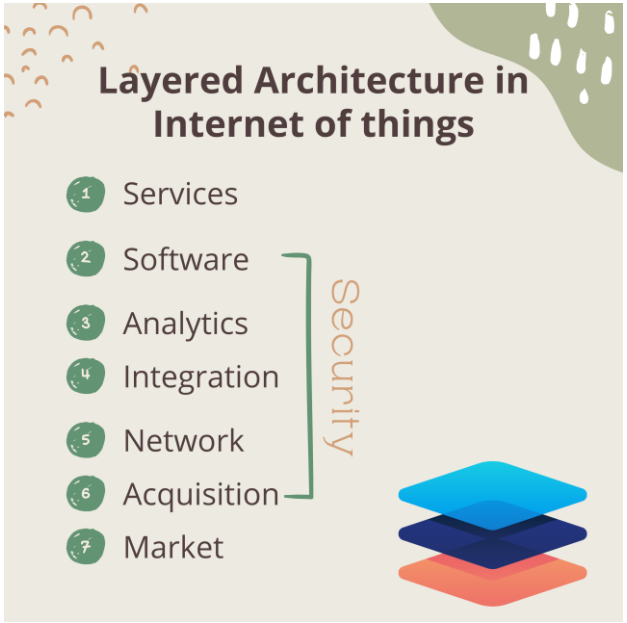


Layerd Architecture of IOT Ecosystem

Depending on the deployed key components & technologies, categorization of the IOT layers can be done.

Key Components :-

- Smart things
- Networks and Gateways
- Data Processing
- Middleware or IoT platforms
- Applications



IOT Security

- Ensuring the Confidanciality, Intergrity and Availability of the IOT ecosystem
- Identify the Vulnerabilities & threats assosiated with physical devices, systems, and networks.
- visibility, segmentation, and protection across the entire network infrastructure can meet IoT and security requirements.

Acqucisition Layer

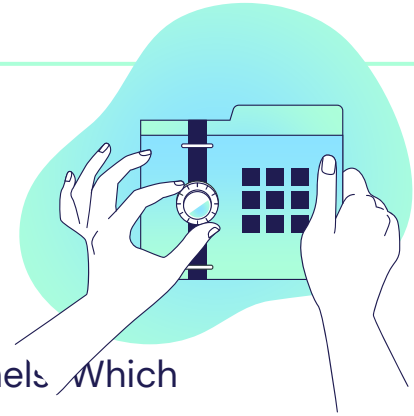
Data Acqucisition in IOT

- Charge of identifying objects and gathering information from them using sensors attached to the objects.
- Transform the information into digital signals.
- Usage of different types of sensors such as, temperature, gas, water quality, RFID, 2-D barcode, and so on.
- Sensors collect basic information about environmental changes, locations, temperature changes of human body and etc.

Vulnerabilities

- Intefereance of collecting data
- Insecure data transmission
- Insecure Ecosystem interfaces

Threats



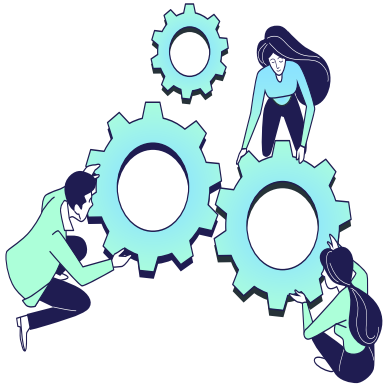
- Network snooping

Intruders intercept real-time traffic which transmit through unsecure channels. Which might lead to exposure the private information of legitimate users.

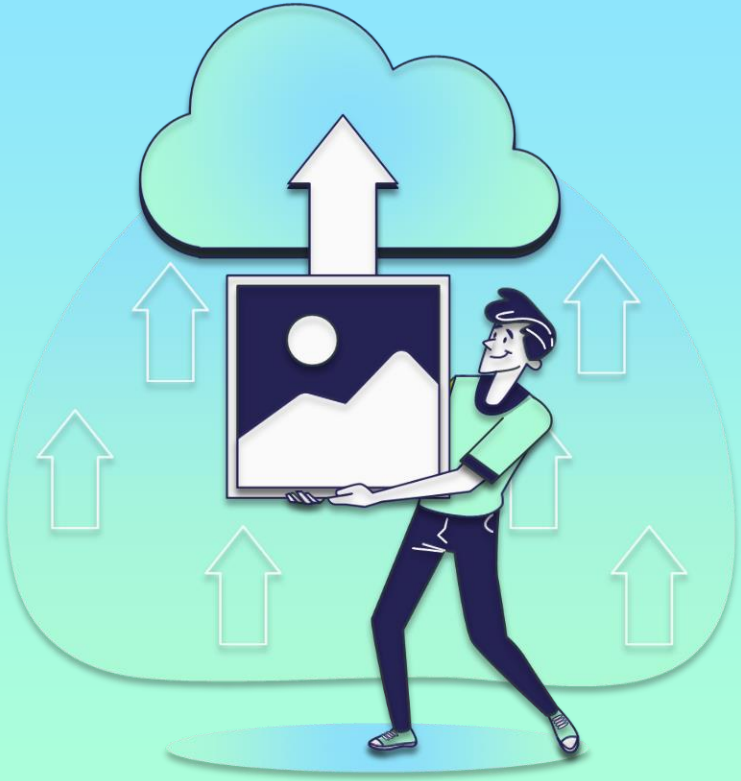
- Node Capture

Attackers try to gain full control over the root or key node. Then leak the Information including sender & receiver communication.

Counter-measures



- Active network monitoring
- Network segmentation
- Encrypt the network traffic

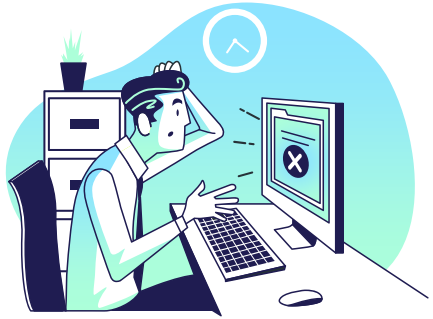


Network Layer

Networking on IOT

- Also known as Transport layer
- Bridged the acquisition and integration layers.
- The network layer serves as a link between the perception layer and the application layer by transmitting data obtained from physical objects via sensors.
- The method of transmission here can be wired or wireless, and it connects smart things, network devices, and networks.
- Attack to the Network layer may affect for information sharing and coordinate among devices.

Vulnerabilities



- Insecure networks
- Improper validation for data integrity
- Weaker authentication mechanism
- Insecure data transmission
- Usage of risky protocols

Threats

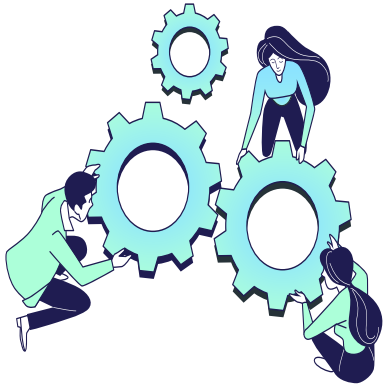
- Denial of service (DoS) attack

  By flooding the network resources with duplicate requests, a denial of service (DoS) attack prohibits the authenticated user from accessing the devices.

- Man-in-the-Middle Attack:

  MiTM attacks are becoming a serious danger to internet security because they alter real-time data communication between the sender and receiver.

Counter-measures



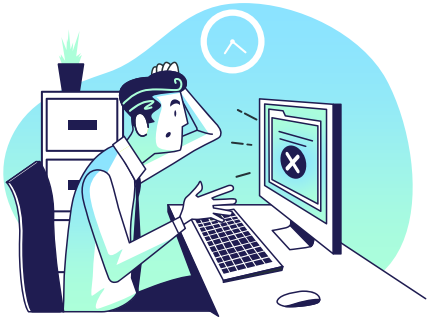
- Useage of TLS/SSL certifications
- Encrypt the network traffic
- Scale up the bandwidth
- Use of anti DOS / DDOS attack hardware & software
- Implement proper authentication mechanism

Intigration Layer

Data Integration in IOT

- IOT devices collect huge volume of data
- Integration of platforms, devices, applications and data
- Data integration engines use for support the dicision making
- Provide deeper insights depending on the different organization perspectives

Vulnerabilities

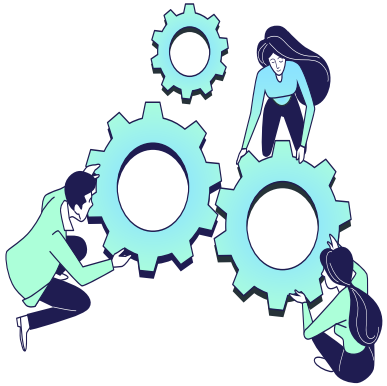


- Poor IOT device Mangment
- User privacy violation interactions
- Insufficient data protection implementation

Threats

- Sql injection attack
- prototype pollution attack

Counter-measures



- Deploy API security solutions
- Usage of Antivirus solutions
- Minimize data collection
- Make data annonemous

Analytics Layer

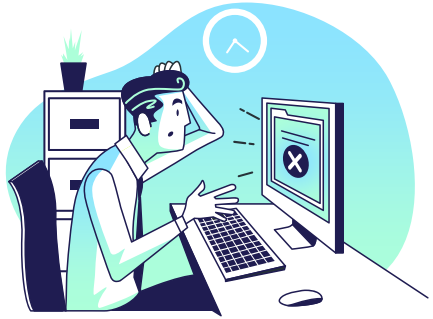
Analytics on IOT

- Data analytics is a process
- Perform different type of analytics methods

  Eg : streaming analytics , spatial analytics and etc.

- Provide supervision of services offered by IoT
- Create business models for visualizing the data
- Decision making

Vulnerabilities

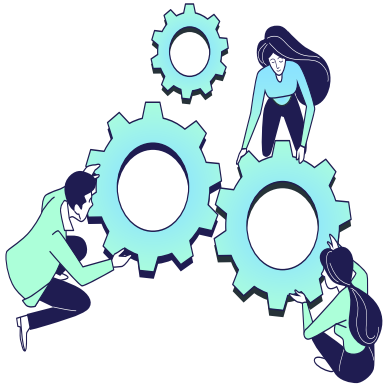


- Server software misconfiguration
- User privacy violation

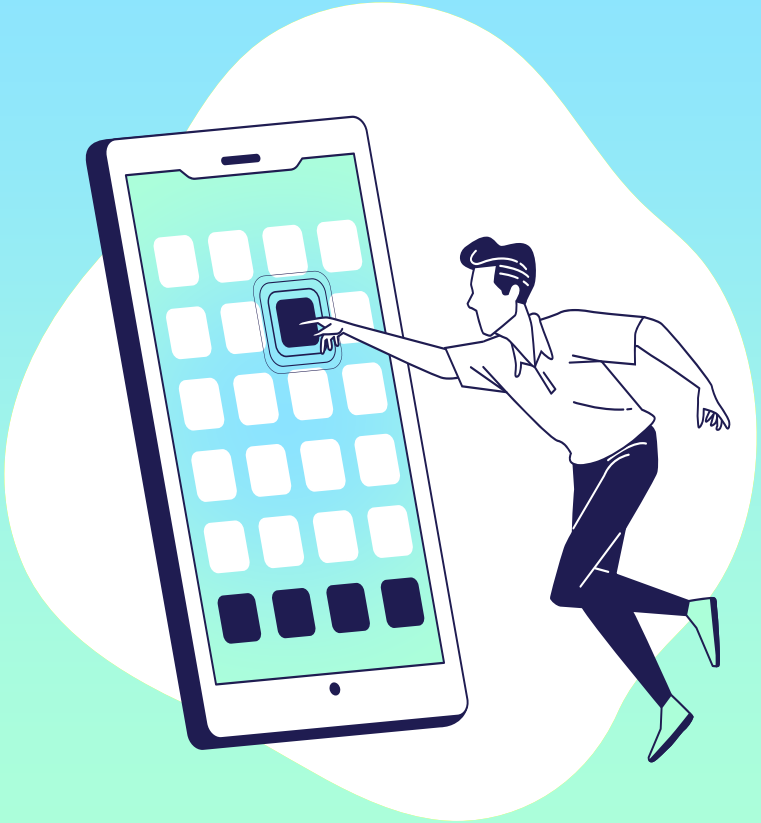
Threats

- Cloud malware injection
- Identity Theft
- Exhaustion attack
- Firmware attack

Counter-measures



- Conduct awereness sessions
- Regular checkout for software and firmware updates



Software Layer

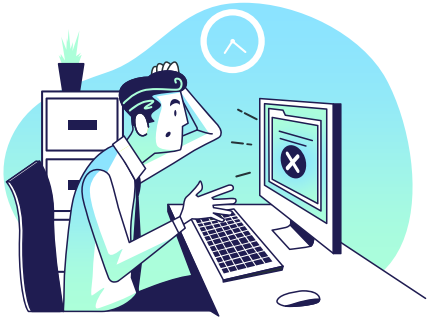
You could enter a subtitle here if you need it

Software layer on IOT

- Provide services to the applications depending on gatherd information from sensors.

Eg – smart cities, smart homes, smart health

Vulnerabilities

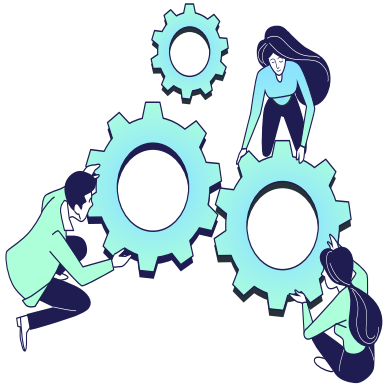


- Lack of secure update mechanism
- Sensitive data disclosure
- Use of third-party libraries
- Usage of weak computational devices

Threats

- Buffer overflow
- Cross site scripting
- Remote code execution

Counter-measures



- Data sanitization
- Input validation
- Implement web app firewall
- Secure handle of cookies

References

- https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security
- https://www.altexsoft.com/blog/iot-architecture-layers-components/
- http://jin.ece.ufl.edu/papers/HASS2018_IoT_Survey.pdf
- https://www.tdktech.com/tech-talks/securing-the-network-layer-against-malicious-attacks/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453/
- https://www.fortinet.com/resources/cyberglossary/iot-security
- https://www.intertrust.com/blog/owasps-top-10-iot-vulnerabilities-and-what-you-can-do/
- https://www.academia.edu/44820038/A_Survey_on_Internet_of_Things_Applications_and_Layered_Wise_Security_Issues
- https://www.fingent.com/blog/role-of-data-analytics-in-internet-of-things-iot/

THANK YOU..!