Carleton University

Systems and Computer Engineering Department
Internet of Things – SYSC 5809
Winter 2023

# IoT Security

**Presented by:**
**Mahmoud Selim | 101281147**
**Iman Alavi Fazel | 101261338**
**Aziz Al-Najjar | 101244840**
**Shakir Sayed | 101250615**

# Content

- Introduction
- IoT Security landscape
- IoT Layers attacks and their mitigations
- IoT Security Solutions using Blockchain and Edge computing
- Real life case studies for IoT attacks
- Conclusion
- References

# Introduction

- IoT is rapidly growing and expected to reach **650B$** market by **2026**
- With this growth, IoT is emerging in new areas and also integrating with already-existing fields such as the medical fields (IoMT), mission-critical applications (IoMCT), and others

➢ **Consequence?** Failure in IoT security can be more costly and can directly impact our daily lives

- Securing IoT infrastructure is inherently more challenging than traditional computing. Why? Heterogeneity of devices
- There are typically plethora of interconnected devices different devices, with different *hardware*, *software* and *communication protocols*

# Content

- Introduction
- IoT Security landscape
- IoT Layers attacks and their mitigations
- IoT Security Solutions using Blockchain and Edge computing
- Real life case studies for IoT attacks
- Conclusion
- References

# IoT Security Landscape

- IoT devices have characteristics that distinguish them from traditional computing devices such as desktop computers and servers (IoC)
- The key characteristics of IoT devices that facilitate security threats:

1. **Low-cost:** IoT devices are often designed to be low-cost, and may not follow the same security measurements of more costly devices
2. **Non-Standard Interfaces:** IoT devices may use non-standard interfaces, adding new methods for exploitation in addition to the already well-researched methods
3. **Cyber-physical Interaction:** IoT devices interact with the physical world, and they may be vulnerable to both physical attacks as well cyber attacks
4. **Long-Lived Devices:** Many IoT devices are designed to be operational for a long period of time, and subsequently, they may become vulnerable to new threats that emerge over time
5. **"Many-User" Devices with Unclear Authority:** Many IoT devices are used by multiple users with varying levels of authority, which can make it difficult to manage access and enforce security policies

# IoT Security Landscape (cont'd)

## 1. Low-Cost IoT Devices and Security Implications

- To reduce the costs, manufacturers usually use low-cost hardware and software solutions

➢ **Implications?**

- Weak hardware computational capabilities is the lack of processing power to run strong cryptographic algorithms
- This can result in **weaker encryption methods** that are more vulnerable to attacks that rely on breaking encryption mechanisms (Ex. A large class of devices cannot generate RSA keys with ≥2048 bits)
- Moreover, manufacturers may use generic software solutions which are often **not designed for security-critical applications**

# IoT Security Landscape (cont'd)

## 1. Low-Cost IoT Devices and Security Implications

➢ **Solution?**

- IoT service provides should adopt *software* and *hardware* that are specifically designed for IoT or real-time applications
- Examples:

1. Using devices that have **dedicated hardware capabilities** for cryptography algorithms (such as Microchip ATECC608A)
2. Adopting OSes such as *FreeRTOS* and *TinyOS* which are designed for real-time applications such as IoT, and configure/modify them specifically for their products

# IoT Security Landscape (cont'd)

## 2. Non-Standard interfaces

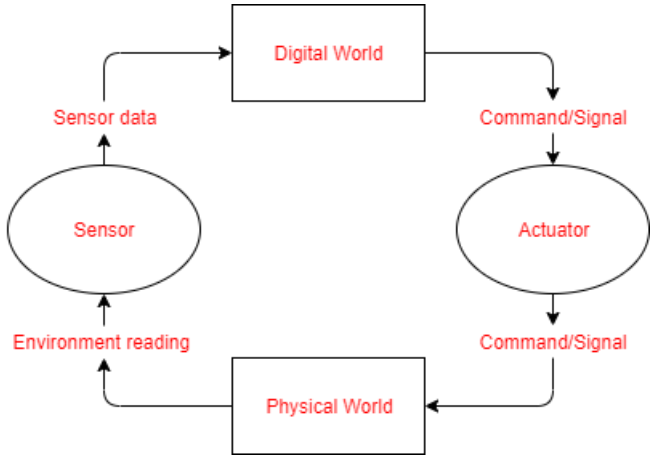
- IoT devices often demand alternative methods for **setup**, **configuration** and **usage**, such as using a cloud management service, smartphone app, or voice commands
- These novel interactions result in new attack surfaces that can be exploited by attackers. Examples of implications:
  1. IoT devices can take unintended sounds from the attackers as commands such as *Hidden voice commands*
     - Hidden voice commands refer to inaudible messages that cannot be detected by the human ear, but IoT devices can understand [7]
  2. Sensors such as temperature and noise can be exploited by attackers to generate false data or extract sensitive information from them

❖ Solution? For each new input interface, unique mitigation techniques should be adopted (*Will be discussed in the follow up sections*)

# IoT Security Landscape (cont'd)

## 3. Cyber-physical Interaction

- IoT devices link the physical environment to the digital space, and interacting with a system means that you are **impacting the physical world**.
- It is essential to adopt new security threat models
- These devices may be vulnerable to physical attacks such as tampering, theft, or destruction, in addition to cyber-attacks.
- To mitigate these risks, IoT devices must be secured against both cyber and physical attacks, including implementing physical security measures such as ***tamper-resistant hardware*** and ***secure enclosures***.



# IoT Security Landscape (cont'd)

## 4. Long-Lived devices

- Consumers expect their IoT devices to maintain their functionality and security for an extended period
- The risk of potentially unpatched vulnerabilities is a significant threat to devices that don't receive *regular software updates*, especially because of nature of "set-and-forget" in many IoT devices
- Solutions?

1. Out-of-date devices be identified using a standard methodology and be fixed on-site by the providers
2. **Push-based updates** should be used when applicable, where the update is initiated by the publisher or central server

# IoT Security Landscape (cont'd)

## 5. "Many-User" Devices with Unclear authority

- In IoC, roles are assigned to individual users based on the *context of their interaction*
- In contrast, devices in IoT belong to an environment and are generally not linked to specific users, such as *voice assistants* and *sensors*, thus being a "*many-user*" device

➢ **Consequence?** It is a challenge for IoT systems to distinguish between legitimate and unauthorized users

- In a many-user environment, solving the authorization problem remains a challenge, and there is no agreed-upon solution
- Possible solution is the use of AI to differentiate between authenticated and non-authenticated users (such as in the case of voice commands)

# Content

- Introduction
- IoT Security landscape
- IoT Layers attacks and their mitigations
- IoT Security Solutions using Blockchain and Edge computing
- Real life case studies for IoT attacks
- Conclusion
- References

# IoT Layers

- Security attacks are often analyzed according to the four-layered model of IoT they impact:

| | |
|---|---|
| 1 – Sensing Layer | • Comprised of *sensors* and *actuators* |
| 2 – Network Layer | • Technologies, protocols and devices that are used to send information from the sensing layer to the computational unit for further processing |
| 3 – Middleware Layer | • Database servers, processing units and other devices that help resource allocation, computing, and data storage |
| 4 – Application Layer | • The layer that the end-users interact with, such as a Smart Home application |

# Sensing Layer threats

## 1. Node capturing attack

- An intruder captures the sensors and extract the encoded information
- such as cryptographic keys and other sensitive information.
- Uses it to setup a malicious node as an authorized node

## 2. Malicious code injection

- “over the air update” feature
- Injection of malicious code to the sensors
- Forces a node to behave unexpectedly or use it to affect other nodes in the network.

## 3. False data Injection

- Altering the sensor reading and injecting unexpected errors
- Consequences:
  - Deviation of the application from expected behavior
  - DDoS (Distributed Denial-of-Service)

## 4. Sleep deprivation attacks (SDA)

- Disrupt nodes' scheduled sleep patterns
- Keep them awake constantly until they are shut down

## 5. Side-channel attacks

- Side-channel attacks use indirect methods to exploit the targets
- Ex: Timing attack:
  - The attacker obtain encryption keys by analyzing the timing information required for the execution of encryption algorithms

## 6. Eavesdropping and interference

- Most IoT devise communicate over wireless networks and are vulnerable to interception of both data transmission and authentication
- Attackers can also send noise data for interference

# Sensing Layer Mitigations Techniques

| | |
|---|---|
| **Code authentication schemes** | Used to prevent *Malicious code injection attacks.* These algorithms can detect changes to the content of memory. |
| **False data filtering algorithms** | Detect anomalies in sensors and prevent *false data injection.* |
| **Secure time stamp schemes** | Used to *prevent replay attacks* |
| **Energy harvesting methods** | are deployed to be used against *Sleep deprivation attacks*, where nodes use external source for their energy |

# Network Layer threats

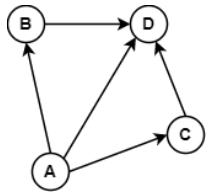
## 1. Routing attacks

Redirecting the communication channels during data transmission

### a. Sinkhole attack

- Creates an artificial fast path through a certain node, presenting to them as the optimal communication channel
- Common in Wireless Sensor Network (WSN)
- Ex: MiniRoute protocol: Each node has a table of link qualities of neighboring nodes

Nodes in a WSN




Before the attack (on B)

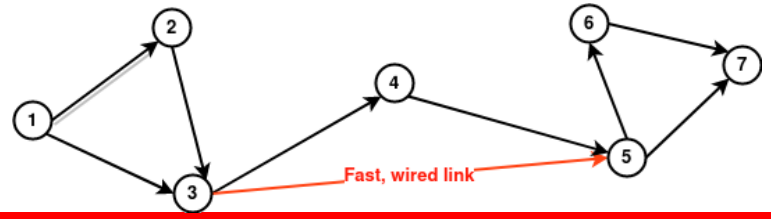
| Node | Link Quality |
|---|---|
| D | 170 |
| **B** | **50** |
| C | 130 |

After the attack (on B)

| Node | Link Quality |
|---|---|
| D | 170 |
| **B** | **255** |
| C | 130 |

### b. Wormhole attack

- Launched by two or more cooperative malicious nodes.
- It establishes a “better” communication link compared to the normal link quality.
- The idea is to forward the data from the victim node to the malicious code situated at the other end of the network.



# Network Layer threats

## 2. DoS/DDoS attack:

- Denial-of-Service (DoS) is done by flooding and overwhelming target servers with unwanted requests/traffic so that the server is unable to respond to legitimate requests. It disrupts the server's ability to communicate with a genuine node resulting in a disrupted service quality
- If multiple sources are used to launch the attack, then the attack is called Distributed-DoS (DDoS) attack.
- **SYN Flood**, **UDP Flood** are a well-known and a typical method carried out in networks

## 3. Sybil attack:

- Multiple fake identities, known as "sybil nodes" or "sybil devices“.
- Used to impersonate legitimate devices on an IoT network.
- Consequence:
  i. Normal users will receive limited access to resources
  ii. In the case of blockchain-based technologies, the attacker can carry out *51% attack*, which allows manipulation of the records or disrupt their operations.

## 4. Unauthorized access:

RFID tags are vulnerable to unauthorized access, which enables an adversary to obtain, modify, or delete the information stored in them. Due to the absence of proper authentication mechanisms

# Network layer Mitigations Techniques

| | |
|---|---|
| Secure multiple routing protocols | Such techniques were designed recommended to defend against the **sinkhole attack** |
| Deploying additional hardware | **Wormhole attack** can be prevented by modifying the existing routing protocols to enhance their security in the route selection process, or deploying additional hardware such as GPS, antenna, etc. |
| **Securing networks against DoS/DDoS requires a combination of approaches.** **The main ones are:** | |
| Rate Limiting | Limiting the rate in which devices can send request through the network |
| Network Segmentation | Grouping IoT devices into different segments and isolate them from other ones |
| Device Authentication | Only authenticated devices may join the network |
| Traffic Filtering | Unwanted network access should be filtered |
| Cloud-based Protection | Advanced cloud infrastructure can detect abnormal traffics e.g., with the usage of AI/ML, and block them before reaching to IoT devices |

# Middleware Layer threats

## What is the Middleware layer in IoT?

The Middleware layer creates an abstraction layer between the network layer and the application layer. It contains the computing units and the storage units of the IoT application.

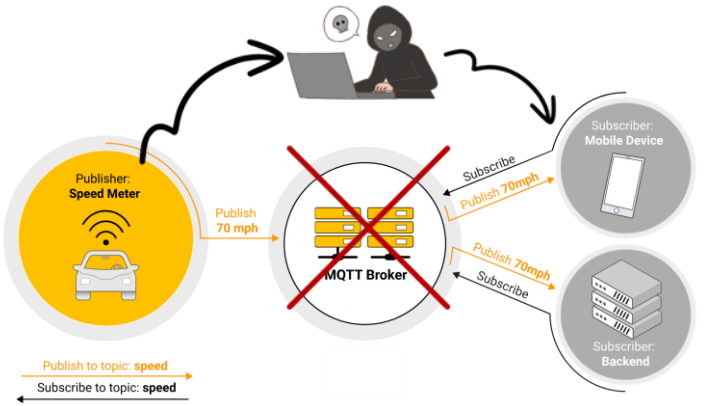
## Middle-ware layer **contains the:**

| | | | |
|---|---|---|---|
| API | Web Service | Datacenter | Cloud |

# Middleware Layer threats

## 1. Man-in-the-middle attack

- In this attack the adversary eavesdrops the communication between two targets.
- In the context of IoT, the MQTT protocol that acts as a proxy, uses a publish-subscribe model for communication between clients and subscribers.
- If the attacker gains control of the broker, they can act as a man-in-the-middle, gaining complete control of all communication.
- This attack is commonly carried out via: **ARP** (Address Resolution Protocol) **spoof, DNS/mDNS spoof, Rogue access point**




## 2. SQL Injection

- SQL Injection is a type of security vulnerability that allows an attacker to inject malicious SQL code into an application's backend and compromise the underlying database
- In IoT, the middleware layer is vulnerable due to its function as the communication channel between devices and the database

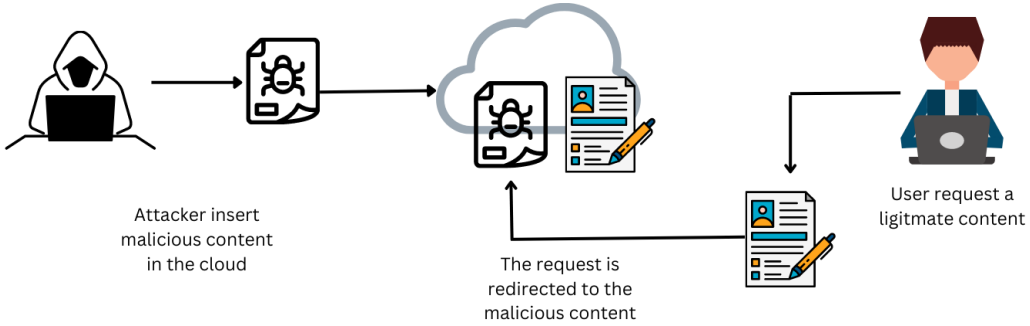

## 3. Signature Wrapping Attack

- SOAP is a widely used protocol in IoT for exchanging data which defines an XML syntax and their processing rules
- In the signature wrapping attack, the attacker breaks the signature algorithm and can modify the captured messages in the SOAP protocol without breaking the included signature.
- The attacker alters a message's digital signature, making it appear as though it was sent by a trusted source.

# Middleware layer threats (cont'd)

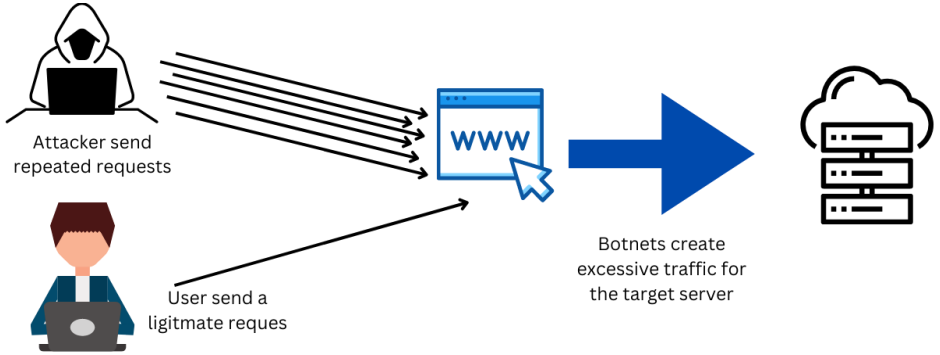
## 4. Cloud Malware Injection:

- A major threat which targets the Infrastructure as a Service (IaaS) clouds is its exposure to malware
- This attack is carried out by setting up a valid service which users connect to.
- Consequently, the adversary can gain access to sensitive information of the IoT users, as well as to disrupt their services




## 5. Flooding Attack in Cloud:

- Cloud services, similar to services in the network layer, can be a target of DoS attacks
- In this scenario, the services employed on the cloud as receive a flood of request from the adversaries which affects the QoS (quality of service) and the load of the servers.
- Flooding a targeted machine or application, or service with lots of requests until regular traffic becomes challenging to process, resulting in denial-of-service to other requesters



# Middleware layer mitigation measures

| 1. MiTM | 2. SQLi | 3. Signature wrapping | 4. Cloud Malware Injection | 5. **Flooding Attack in Cloud** |
|---|---|---|---|---|
| • Encrypting communications<br>• Using secure authentication protocols<br>• Implementing firewalls | • implement firewalls<br>• Sanitize data<br>• Use parameterized queries<br>• Follow secure coding practices.<br>• Validate user input to prevent malicious inputs from being processed. | • Implement secure signature algorithms such as proper Xpath filtering<br>• Validate digital signatures regularly<br>• Enforce secure communication protocols. | • Regularly update software and hardware<br>• Implement security solutions such as firewalls<br>• Encrypt data and implement strict access controls. | • Implement rate limiting and filtering<br>• Detect and isolate infected devices<br>• Use secure communication protocols. |

# Application layer threats

Common attacks that target the application layer:

## 1. Sniffing Attacks

- Sniffing attack (similar to man-in-the-middle) refers to the intercepting of the traffic by the adversary
- In contract to MitM, Sniffing attack is passive and does not change the network traffic

## 2. Malicious virus/worm

- An attacker can introduce malicious self-propagating attacks, such as worms or Trojan horses, into IoT applications to gain access to or manipulate sensitive data. Effective defensive measures such as strong firewalls and virus detection systems should be implemented to prevent and combat these types of attacks in IoT applications.

# Application layer concerns (cont'd)

## 3. Access Control Attacks

- Access control involves allowing authorized individuals to handle authenticated entities
- This form of attack on the application layer is particularly effective, because once the access is compromised, then the complete IoT application may become vulnerable.
- Common methods include:
  - Buffer overflow
  - Cross-site-scripting (XSS)
  - Password attacks (e.g. brute force, dictionary attacks)
  - Backdoors
  - Social engineering

# Application layer Mitigation

Mitigations include:

1. **Input Validation:** ensuring that user inputs do not include special characters or patterns that could be used to inject malicious code
2. **Address space layout randomization (ASLR):** randomize the location of program code and data in memory in the OS-level
3. **Run-time protection mechanism:** Using facilities such as Memory Protection Extensions (MPE) such the set of architectures in Intel CPUs, named **Intel MPX** (Hardware-level)
4. **Compiler-level mitigation:** Advanced compilers can employ techniques such as Bounds checking to prevent memory-related vulnerabilities

# Content

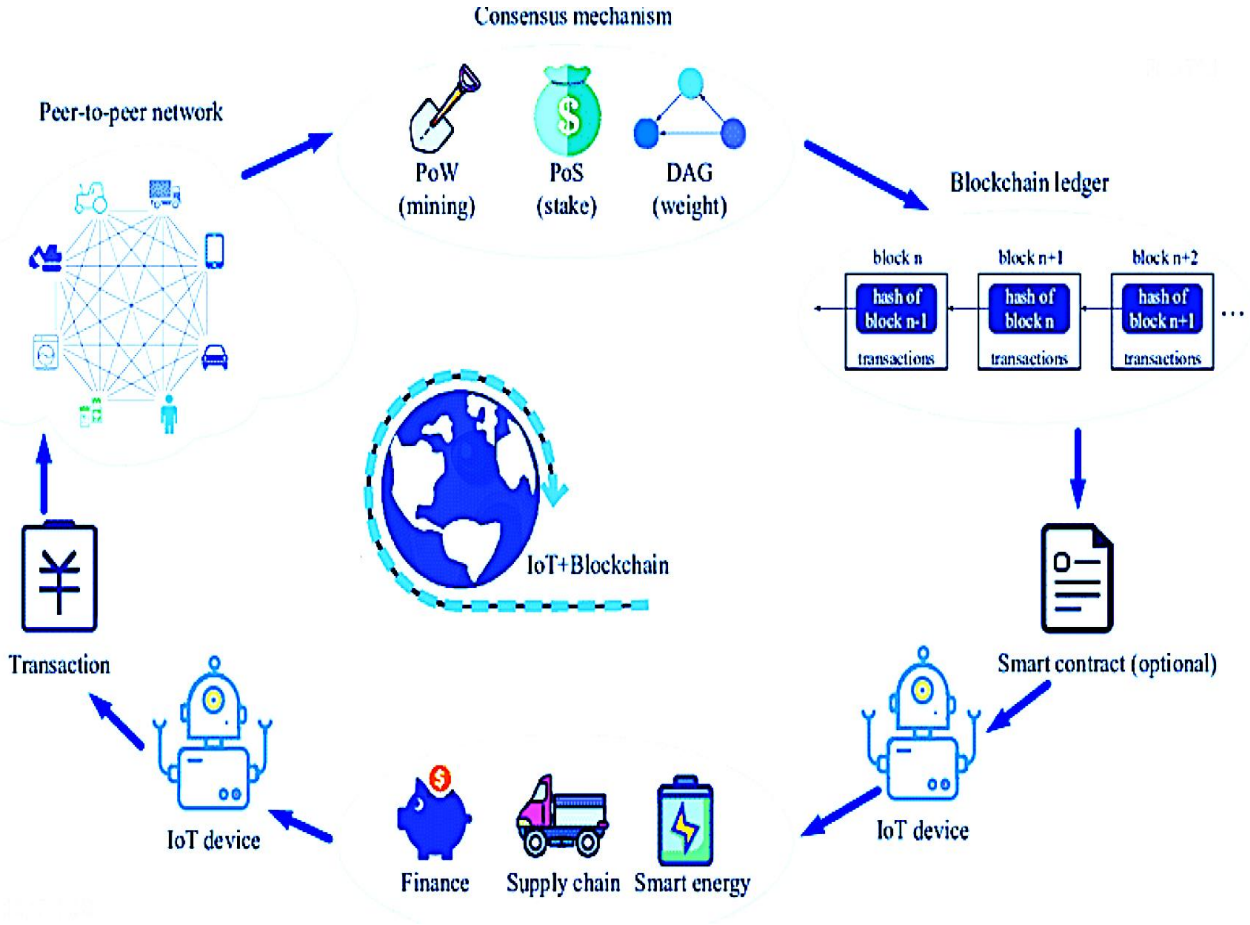
- Introduction
- IoT Security landscape
- IoT Layers attacks and their mitigations
- IoT Security Solutions using Blockchain and Edge computing
- Real life case studies for IoT attacks
- Conclusion
- References

# IoT Security Solutions

## 1. Blockchain based IoT security solutions

**How blockchain works ?**

1. IoT device broadcasts a transaction
2. The network reaches the agreement of new block creator
3. All IoT devices insert a copy of the new block into their local ledgers.
4. The transaction stored in blockchain triggers smart contract
5. IoT device carries out the task




**Source:** (Bansal and Tomar, 2022)

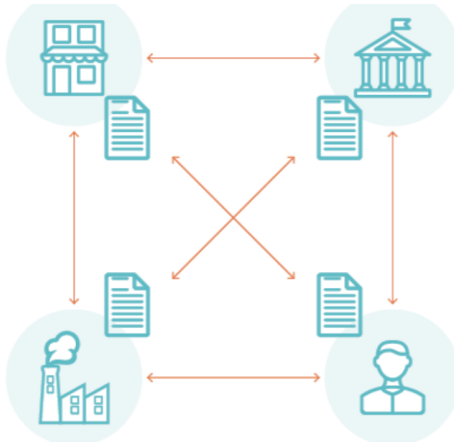
# IoT Security Solutions (con'd)

## 1. Blockchain based IoT security solutions (con'd)

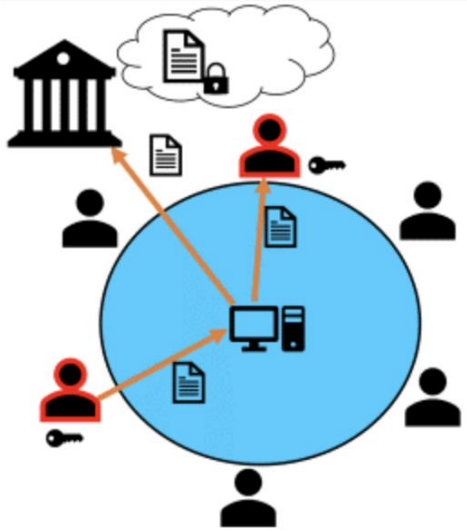
Blockchain technology can enhance the security of IoT devices in the following ways:

- **Distributed Ledger:** The data transferred between devices can be secured. Each transaction is recorded on a distributed ledger, which makes it impossible for any unauthorized party to modify the data.

Centralized ledger



Distributed ledger



Centralized

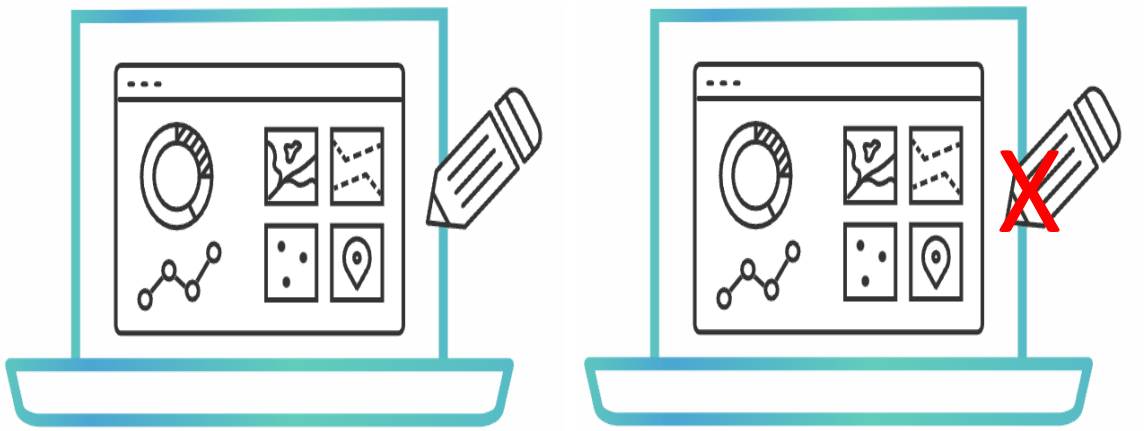
Decentralized

- **Decentralization:** Typically, IoT data are centralized, which makes them vulnerable to attacks. Blockchain-based solution allows IoT devices to be decentralized, allowing for greater security and reducing the risk of a single point of failure.

# IoT Security Solutions (con'd)

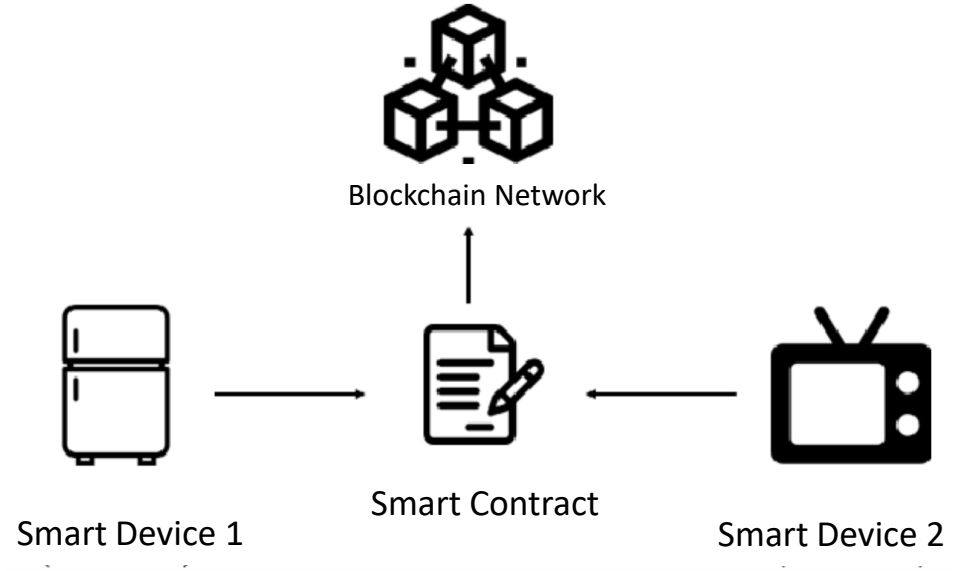
## 1. Blockchain based IoT security solutions (con'd)

- **Immutable Records:** Blockchain's immutable records ensure that once data is stored on the blockchain, it cannot be modified. This ensures that the firmware of IoT devices remains unchanged and secure.



Mutable records

Immutable records

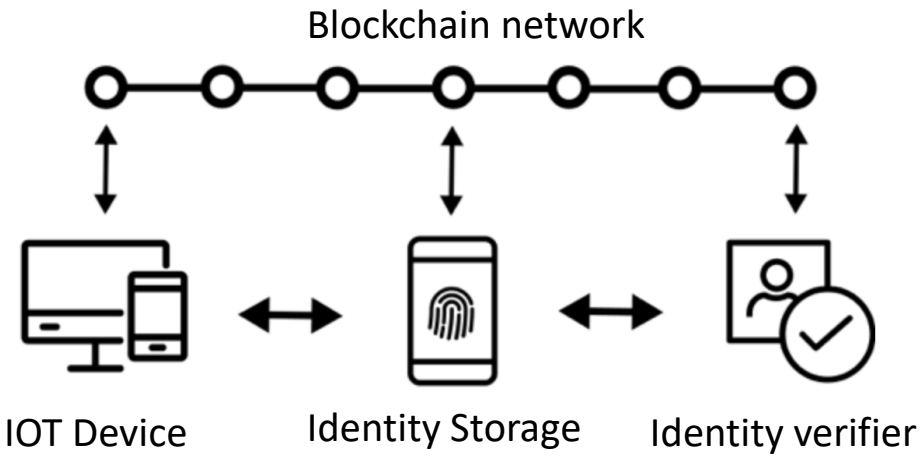


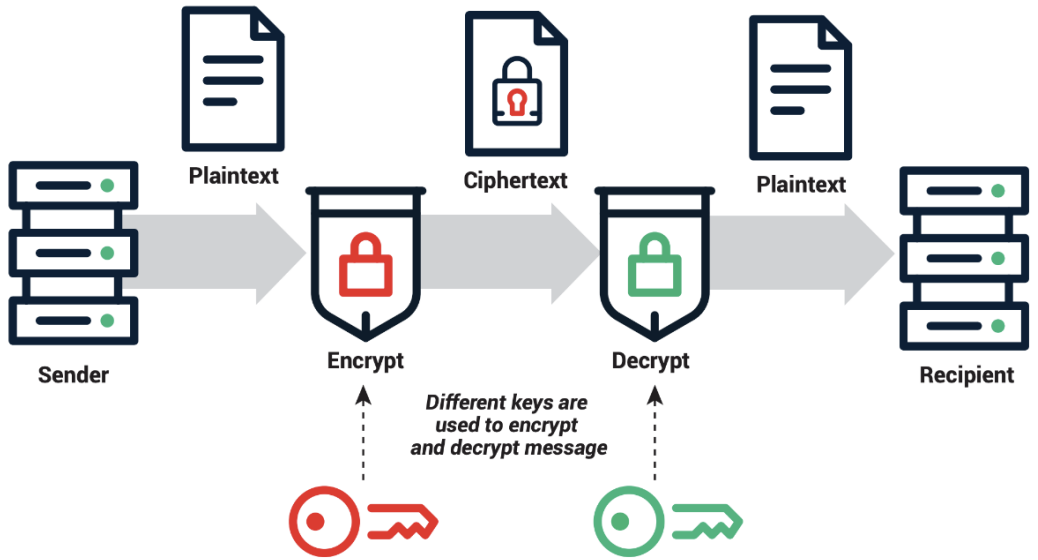

- **Smart Contracts:** This can automate the process of updating IoT device firmware and ensuring that it is done securely.

# IoT Security Solutions (con'd)

## 1. Blockchain based IoT security solutions (con'd)

- **Identity Management:** Blockchain-based identity management solutions can be used to authenticate IoT devices and ensure that only authorized devices are allowed to access the network. This can be done by assigning a unique digital identity to each IoT device, which can be verified by the blockchain network.



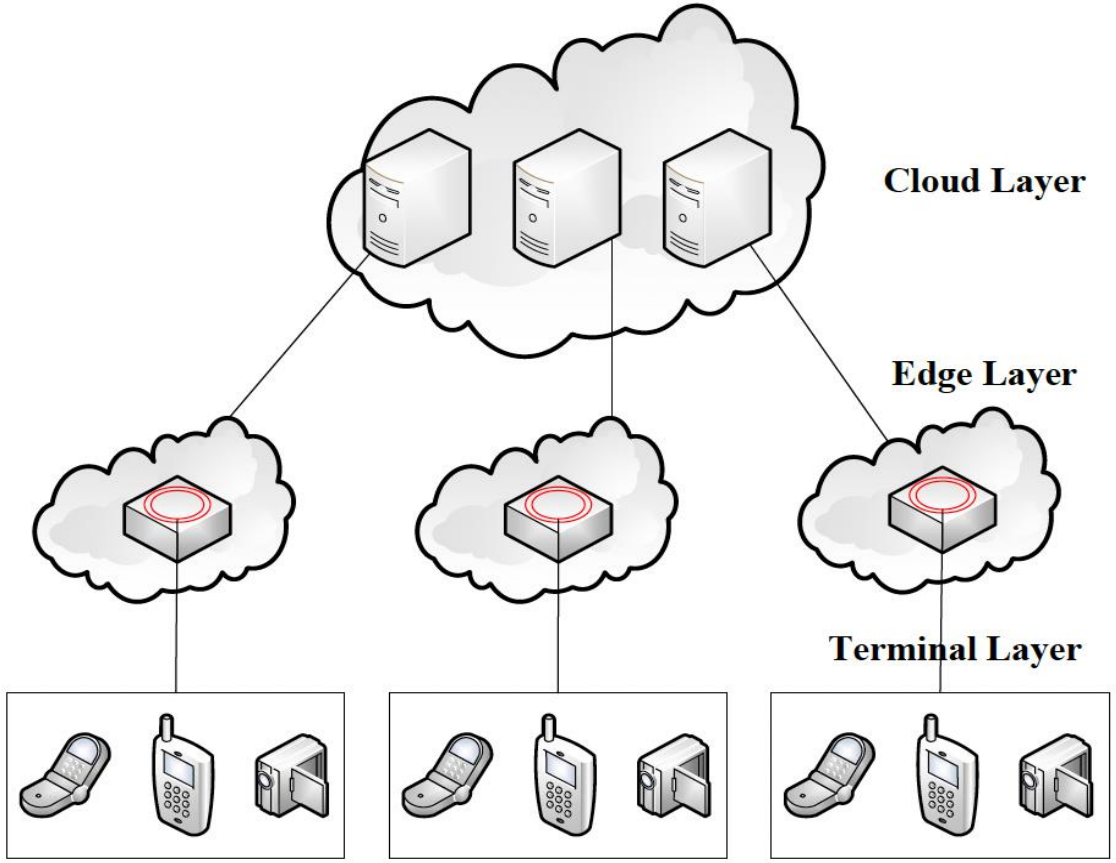




- **Secure Communication:** Secure communication between IoT devices can be done by encrypting data using public key cryptography and using the blockchain network to verify the identity of the devices involved in the communication.

# IoT Security Solutions (con'd)

## 2. Edge Computing based IoT security solutions

- It is a distributed computing model where data processing occurs closer to the edge devices rather than sending them to a centralized location.
- Edge computing architecture of the IoT system is mainly consists of three layers, terminal layer, edge layer and cloud layer.
- No need to send all data collected from terminal nodes up to the cloud platform since distributed local computing and controlling can be conducted in the edge layer.

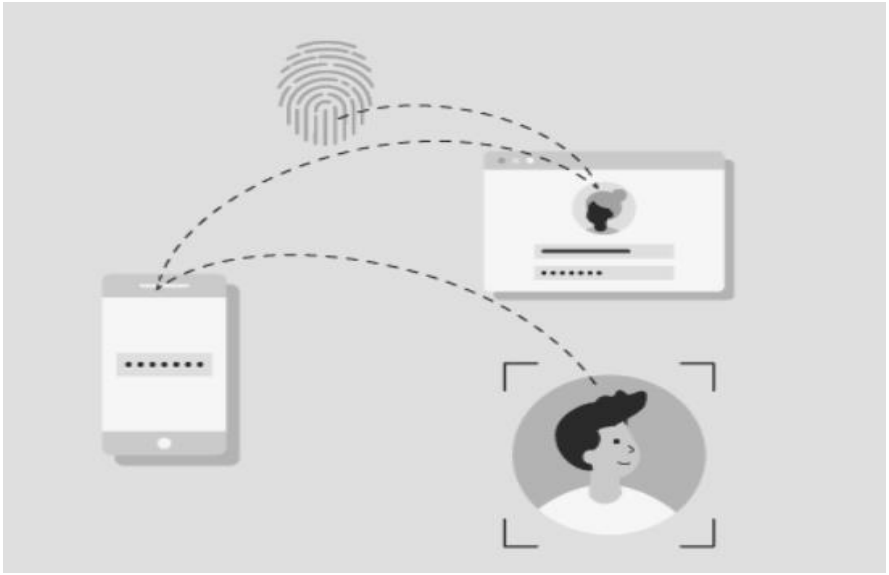



**Source:** (Sha et al., 2020)

# IoT Security Solutions (Con'd)

## 2. Edge Computing based IoT security solutions (con’d)

- **Secure Boot:** This process ensures that only trusted software is executed on an edge device. The device firmware is verified before booting up to prevent any unauthorized access.

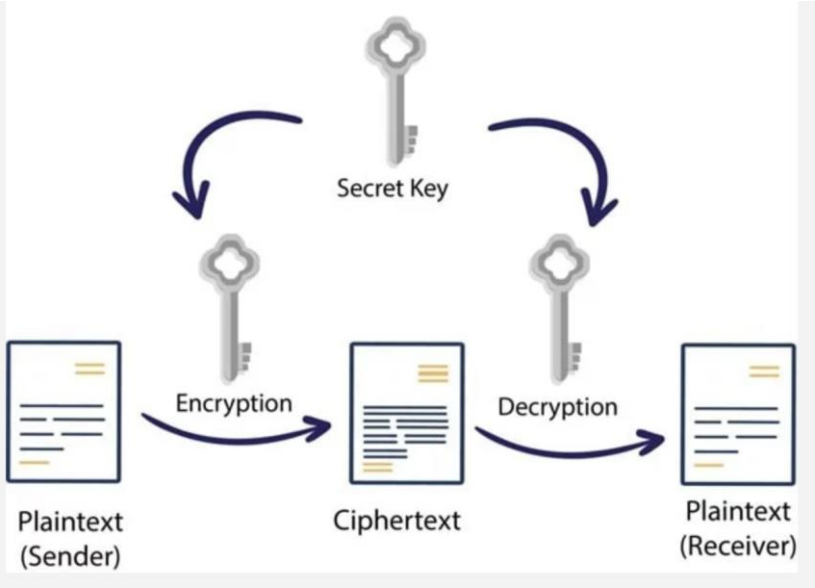


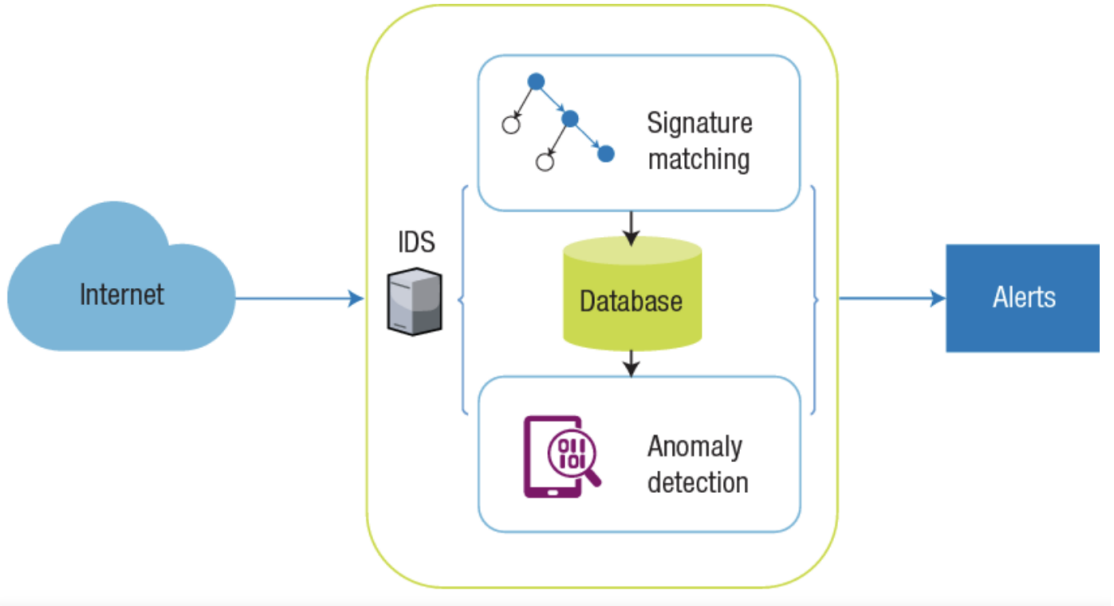
- **Identity and Access Management:** It can be used to authenticate and authorize access to edge devices. This ensures that only authorized users or devices can access the data or control the edge devices.

# IoT Security Solutions (Con'd)

## 2. Edge Computing based IoT security solutions (con'd)

- **Data Encryption:** Data encryption can be used to secure data at rest and in transit between edge devices and the cloud. Encryption keys can be stored on the edge device to ensure that data is encrypted at the source and remains encrypted even when transmitted to the cloud.




- **Intrusion Detection Systems:** This can be deployed at the edge to detect and prevent unauthorized access or data breaches. These systems can monitor network traffic and identify any suspicious activity.

# IoT Security Solutions (Con'd)

## 2. Edge Computing based IoT security solutions

- **Threat Intelligence:** Edge devices can be protected by regularly updating threat intelligence feeds to identify and prevent new threats. This can help to detect and mitigate potential attacks before they can cause damage.

- **Physical Security:** Physical security measures can be used to protect edge devices from physical tampering or theft. This can include using security cameras, access control systems, and alarm systems.

# Content

- Introduction
- IoT Security landscape
- IoT Layers attacks and their mitigations
- IoT Security Solutions using Blockchain and Edge computing
- Real life case studies for IoT attacks
- Conclusion
- References

# Case Studies

1. The Mirai botnet

The Mirai botnet was malware that targeted IoT devices and launched DDoS attacks

- It scanned for victims using pseudorandom IPv4 network addresses and preconfigured credentials
- It installed undetected malware and remotely managed infected devices, allowing attackers to launch DDoS attacks
- It infected 600,000 devices and caused significant damage to enterprise networks, resulting in unresponsive networks and network bandwidth saturation
- Countries impacted include the US, UK, Germany, France, Italy, Brazil, Australia, Japan, and China

# Case Studies (Con'd)

- Estimated cost of around $4,207.03 per hour of network bandwidth overflow

**Solutions:**

- To avoid botnet attacks, randomized passwords, avoiding default network configurations, applying ASLR, automatic updates, and notification alerts when suspicious behavior is detected are encouraged.
- Adoption of immune-to-fragmentation attacks operating systems and the withdrawal and upgrade of outdated systems can also impede botnet attacks.

# Case Studies (Con'd)

2. Healthcare devices

During the COVID-19 crisis, the U.S. Department of health and human services (HHSs) reported the increase of 50% in cyberattack incidents targeting the healthcare industry

- **Key factor for security breaches in the US health sector?** Research found that more than 80% of the 1.2 million IoT devices located in U.S. healthcare organizations were operating using outdated OS, and do not support security updates
- In another example, an incident in 2020 occurred in Germany caused a life of a patient, which was caused by the flaw in the outdated VPN server of the hospital

# Case Studies (Con'd)

## Damages:

- Disclosure of user medical records
- Harm to patients' well-being
- Inability to admit patients due to system access unavailability
- Patient deaths due to system unavailability and lack of access to healthcare services

# Case Studies (Con'd)

- In 2015, security researchers utilized honeypots to study security mimicking the existing healthcare architectures
- The honeypots recorded 55,416 successful logins and 24 successful exploitations during their active period
- The most common exploit was **MS08-067** which is a remote execution vulnerability present in Microsoft Windows Server 2003, 2008, XP and Vista
- **Solution:** Incorporating IoT-enabled technologies in an existing healthcare system should be accompanied by redesigning network infrastructure to be preventive against new attacks

# Case Studies (Con'd)

3. Aircraft avionics

- In 2018, an unprotected server was discovered on Boeing's network, which allowed download access to the avionics system provider data and code specifically crafted to run on the company's 737 and 787 passenger jets.

- Vulnerabilities were discovered in some of the obtained .vex files, including stack and buffer overflows, remote code execution, a vulnerable trivial file transfer protocol (TFTP) server, an insecure system-call handler, and return-oriented programming (ROP) exploits.
- The security analysis reveals references to many insecure code functions on the crew information system-maintenance system (CIS/MS) module, such as strcpy, sprintf, and strcat, which can allow buffer overflows and out-of-bound read/write operations.
- Leveraging the vulnerabilities, two communication-based attack scenarios were depicted, targeting the network infrastructure of the 787 aircraft.

# Case Studies (Con'd)

- The discovered vulnerabilities, including zero days, can be exploited leading to destructive attacks.
- The common data network (CDN) could be compromised, providing unauthorized access to systems such as fuel quantity, low pressure, and lightning.

**Solutions:**

- Use of the x86 32-bit CPU No-Execute (NX/XD) hardware mitigation and the adoption of compiler-level mitigation for insecure functions.
- Secure firmware updates are strongly advised for mission-critical subsystems attested by integrity checks and controls to verify the authenticity of the firmware.

# Case Studies (Con'd)

4. Baby Monitors


**Source:** Xenofontos et al. (2021)

- Baby Monitoring Cameras (BMCs) are popular consumer electronic devices.
- A security analysis of a BMC revealed multiple vulnerabilities.
- TCP ports 554 and 5000 can be exploited without authentication from anyone with access to the BMC's local network.
- The default password is neither device specific nor randomly generated.

# Case Studies (Con'd)

- The BMC features two universal asynchronous receiver–transmitter (UART) interfaces, which grant complete administrator control to anyone who can acquire physical access to the device.
- Attackers can exploit the default-enabled peer-to-peer (P2P) cloud feature to compromise the device and violate users' privacy.
- Default credentials can lead to possible attacks targeting the service aspect of the device, locking authorized users out, or providing adversaries with access to customer local networks via compromised devices.

# Case Studies (Con'd)

- The attack compromises users' privacy
- The compromise of a BMC can provide adversaries with access to customer local networks

**Solutions:**

- Researchers, manufacturers, and service providers recommend countermeasures to safeguard customer security, such as changing default credentials, disabling unused features, patching with the latest firmware updates, and enabling encrypted traffic.

# Content

- Introduction
- IoT Security landscape
- IoT Layers attacks and their mitigations
- IoT Security Solutions using Blockchain and Edge computing
- Real life case studies for IoT attacks
- Conclusion
- References

# Conclusion

- IoT landscape was discussed and an analysis of the 4 different layers of IoT was conducted
- Alongside the threat taxonomy, possible mitigations and solutions were mentioned and highlighted the common techniques
- The application of blockchain-based and Edge computing were discussed in the security of IoT
- Various major incidents were studied. We presented their causes, areas affected, damages and the lessons learned.

# Content

- Introduction
- IoT Security landscape
- IoT Layers attacks and their mitigations
- IoT Security Solutions using Blockchain and Edge computing
- Real life case studies for IoT attacks
- Conclusion
- References

# References


1. Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." *IEEE internet of things journal* 4.5 (2017): 1125-1142.

2. Mishra, Nivedita, and Sharnil Pandya. "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review." *IEEE Access* 9 (2021): 59353-59377.

3. Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.

4. Yang, Yuchen, et al. "A survey on security and privacy issues in Internet-of-Things." *IEEE Internet of Things Journal* 4.5 (2017): 1250-1258.

5. N. A. Khan, A. Awang and S. A. A. Karim, "Security in Internet of Things: A Review," in IEEE Access, vol. 10, pp. 104649-104670, 2022, doi: 10.1109/ACCESS.2022.3209355.

6. Bellman, Christopher, and Paul C. van Oorschot. "Analysis, implications, and challenges of an evolving consumer iot security landscape." *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, 2019.

7. Carlini, Nicholas, et al. "Hidden voice commands." *Usenix security symposium*. 2016.

8. Saloni Bansal and V.K Tomar. “Challenges & Security Threats in IoT with Solution Architectures”. 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and Its Control. 2022 IEEE

9. Wenbin Chen, Yuxin Chen, Yishuo Jiao and Quanchun Liu. “Security Awareness Scheme of Edge Computing in IoT Systems”. 2021 IEEE 4th International Conference on Computer and Communication Engineering Technology, doi: 10.1109/CCET52649.2021.9544267.

10. K. Sha, T. A. Yang, W. Wei, and S. Davari, “A survey of edge computing-based designs for IoT security,” Digital Communications and Networks, vol. 6, no. 2, pp. 195–202, 2020, doi: https://doi.org/10.1016/j.dcan.2019.08.006.

11. Rassam, Murad A., et al. "A sinkhole attack detection scheme in mintroute wireless sensor networks." *2012 International Symposium on Telecommunication Technologies*. IEEE, 2012.

12. Sharma, Sparsh, and Ajay Kaul. "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud." *Vehicular communications* 12 (2018): 138-164.

13. C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, Consumer, Commercial and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. 2021.