The Future of IoT Security: Integrating Network Protection and Privacy-Enhanced Biometric Systems at Edge

Aminu Bello Usman, PhD, SFHEA
Head of School of Computer Science,
University of Sunderland
Keynote Speech @YISEC2024 conference,
University of Hull, Hull, United Kingdom
Date: 21/06/2024

University of Sunderland

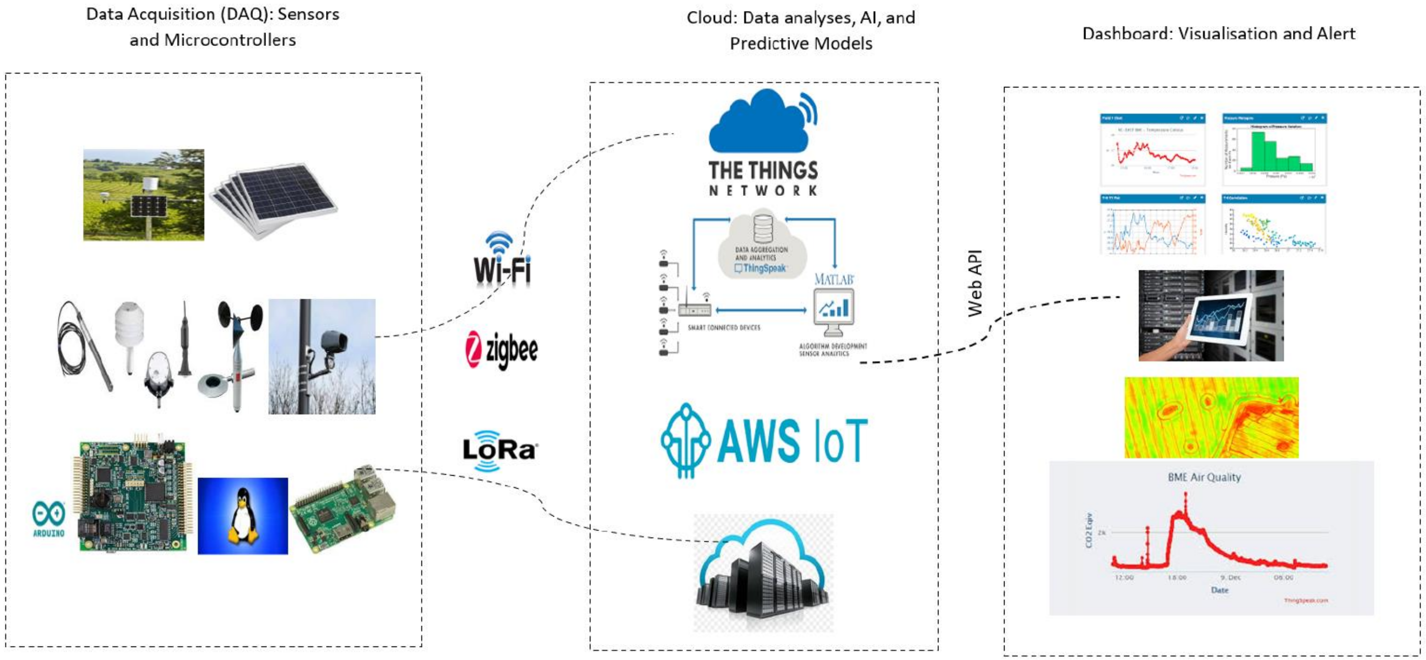
- How can Privacy by Design principles be effectively incorporated into the development of a biometric authentication framework for one-to-many system at edge ?
- Is it possible to **securely** transfer large amounts of **data** over LoRa/LoRaWAN?
- How can we develop a public display architecture that leverages the capabilities of LoRaWAN and Ethereum smart contract technology to ensure tamper-resistant and transparent data integrity through advanced peer-to-peer security measures?

University of Sunderland

IoT

- A network of physical objects, or "things," that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet.

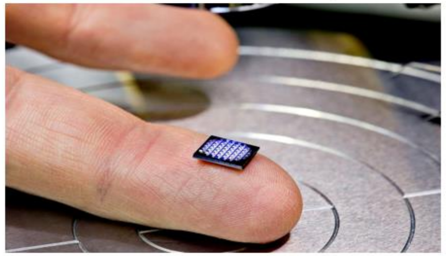
- IoT Connectivity
  - **Device to device (D2D)**
  - **Device to gateway**
  - **Gateway to data systems**
  - **Between data systems**

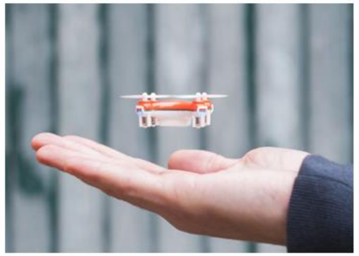


University of Sunderland

Ubiquitous connectivity

Miniaturization—smaller computers and communication chips





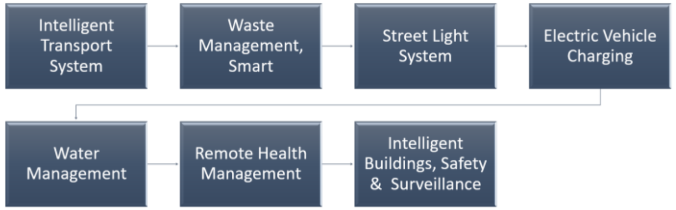
Cloud Computing—cloud computing has become a point with virtually unlimited processing power and storage for IoT data

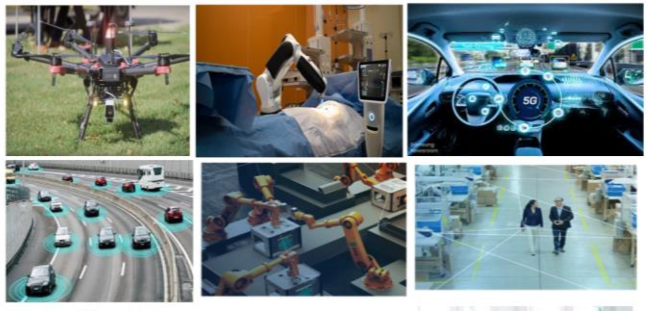
By improving operational efficiency and reducing waste

IoT technology can automate many tasks, freeing up time and resources for more valuable work

IoT has the potential to transform how we live and work, providing new opportunities for innovation, efficiency, and convenience.

IoT Applications for Smart City

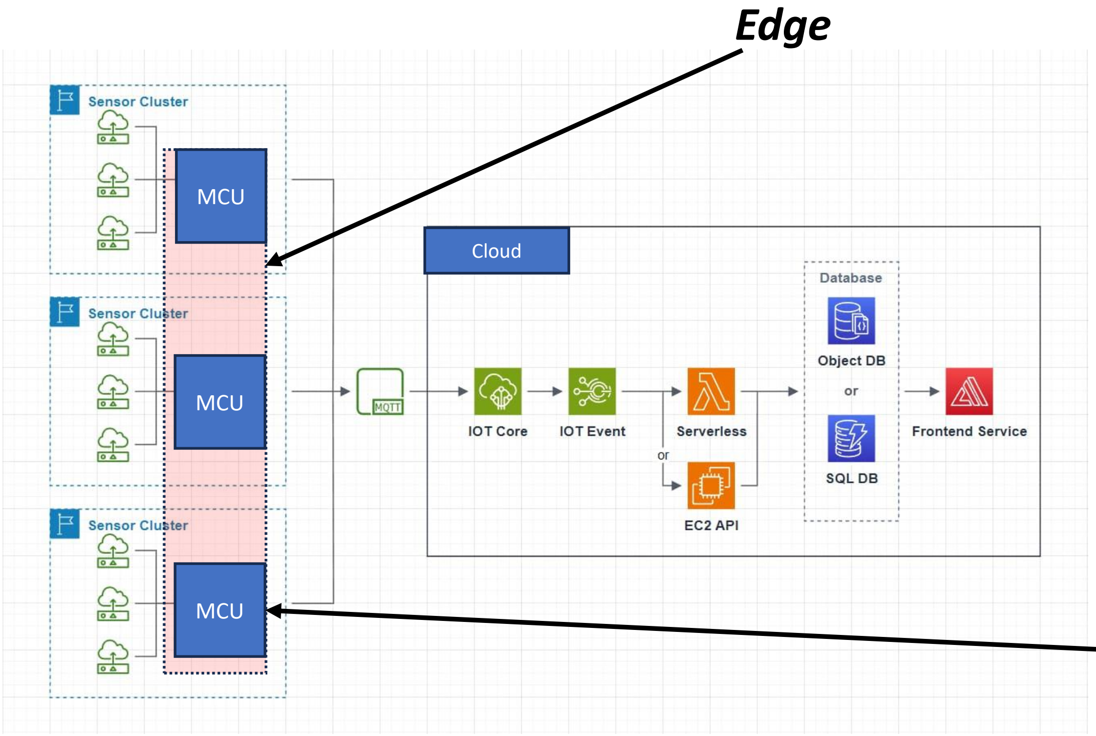




University of Sunderland

Paradigm Shift in IoT: Embracing Edge AI and Federated Learning

- IoT applications



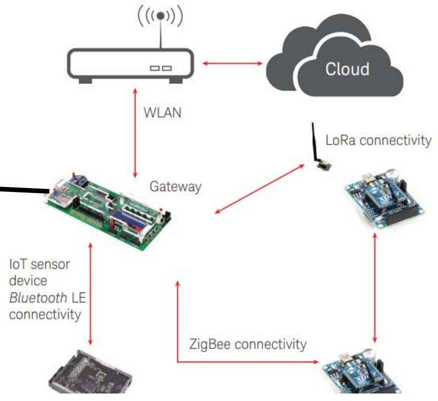
Edge AI *- Deployment of AI algorithms directly on edge devices rather than relying solely on centralised cloud servers.*

- *Reduced Latency*
- *Enhanced Privacy and Security*
- *Scalability*

Federated Learning -
Enables training ML algorithms across multiple decentralised edge devices or holding local data samples, without exchanging their data.

Why Federated learning ?

- Privacy and Security
- Reduced Latency
- Scalability



Multi protocol gateway

University of Sunderland

Paradigm shift Implementing Privacy by Design Principles

What is Privacy by design ?

Privacy by Design (PbD) is a framework aimed at integrating privacy into the design and operation of technologies from the outset.

The 7 Foundation Principles of privacy by design are as follows (Cavoukian 2009):

1. **Proactive not Reactive; Preventative not Remedial** - It is important that applications that use privacy by design are proactive rather than reactive and try to anticipate and prevent potential breaches before they happen.
2. **Privacy as the Default Setting** - Settings that keep data private should be automatically on, meaning the user needs to take no action to protect their data.
3. **Privacy Embedded into Design** - Privacy features should not be bolted on to the application or architecture and should be an essential component of the system, without hurting the functionality.
4. **Full Functionality – Positive-Sum not Zero-Sum** - No negative trade-offs should be taken, and it is desirable to have both privacy and security in a 'win-win' scenario.
5. **End-to-End Security – Full Lifecycle Protection** - Data should be protected throughout its entire usage from when it was conceptualised to its deletion.
6. **Visibility and Transparency – Keep it Open** - The parts and operation of the application or architecture must remain visible and transparent to verified users and providers.
7. **Respect for User Privacy – Keep it User-Centric** - The individuals' interests should be of the upmost importance, hence should have privacy defaults and remain user-friendly.

Why Privacy in Biometric Authentication

- **Sensitive Personal Information**
  - Biometric data, such as fingerprints, facial recognition, iris scans, and voice patterns, is inherently sensitive.
- **Risk of Misuse and Identity Theft**
  - In one-to-many biometric systems, where an individual's biometric data is compared against a large database, the risk of misuse increases.
- **Discrimination and Profiling**
  - Biometric systems, if not properly regulated, could be used to discriminate against individuals based on their physical or behavioral traits.
- **Public Trust and Acceptance**
  - For biometric authentication technologies to be widely accepted, there must be a high level of public trust.

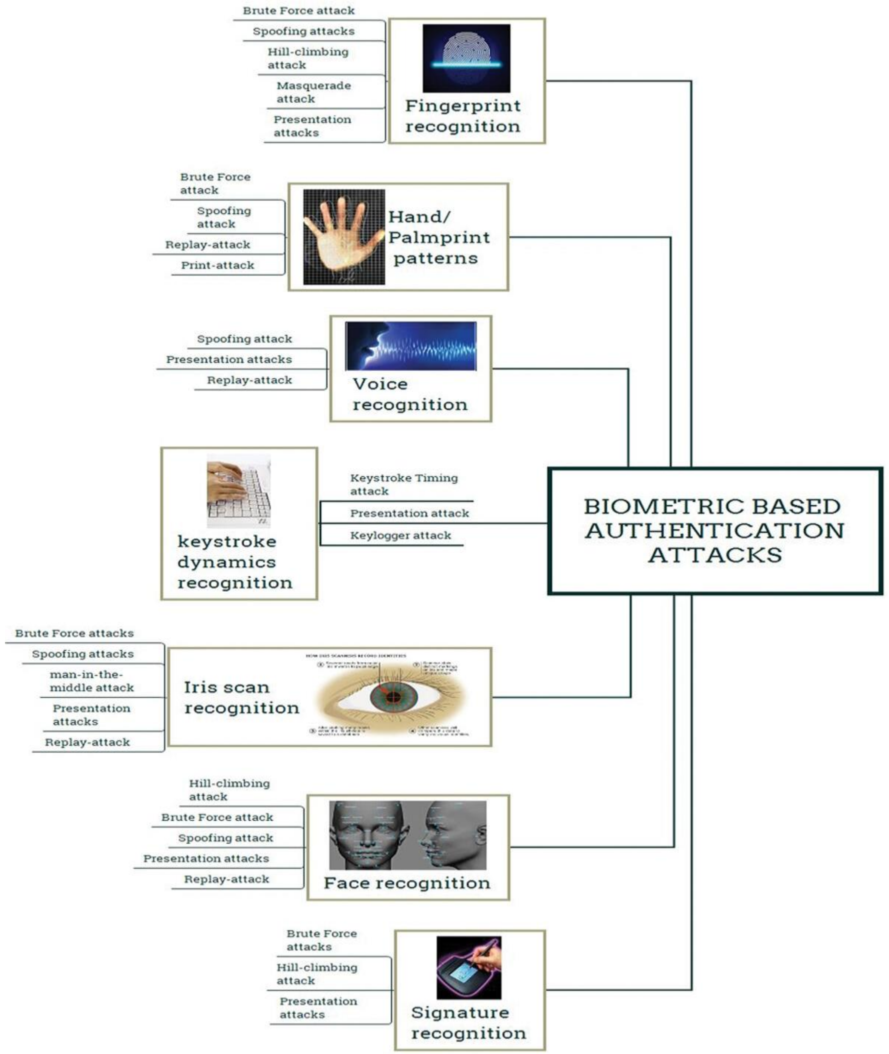

Review Article

Privacy and biometrics for smart healthcare systems: attacks, and techniques

Alec Wells & Aminu Bello Usman

Pages 307-331 | Published online: 03 Oct 2023

Cite this article https://doi.org/10.1080/19393555.2023.2260818 Check for updates



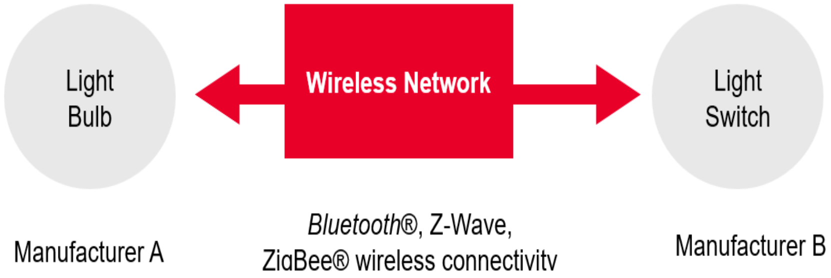
University of Sunderland

- With the paradigm shift in IoT towards embracing Edge AI and Federated Learning, we are interested in underlying security issues associated with IoT communication protocols.
- Additionally, integrating Privacy by Design principles is essential to ensure robust security and privacy in IoT ecosystems.

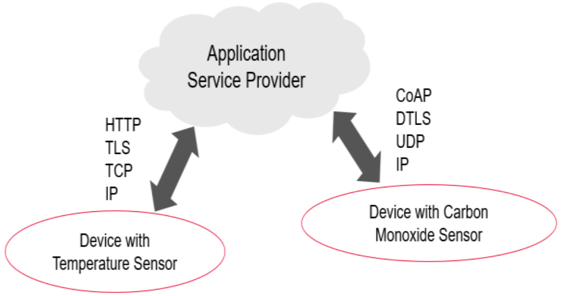
University of Sunderland

IoT Communication

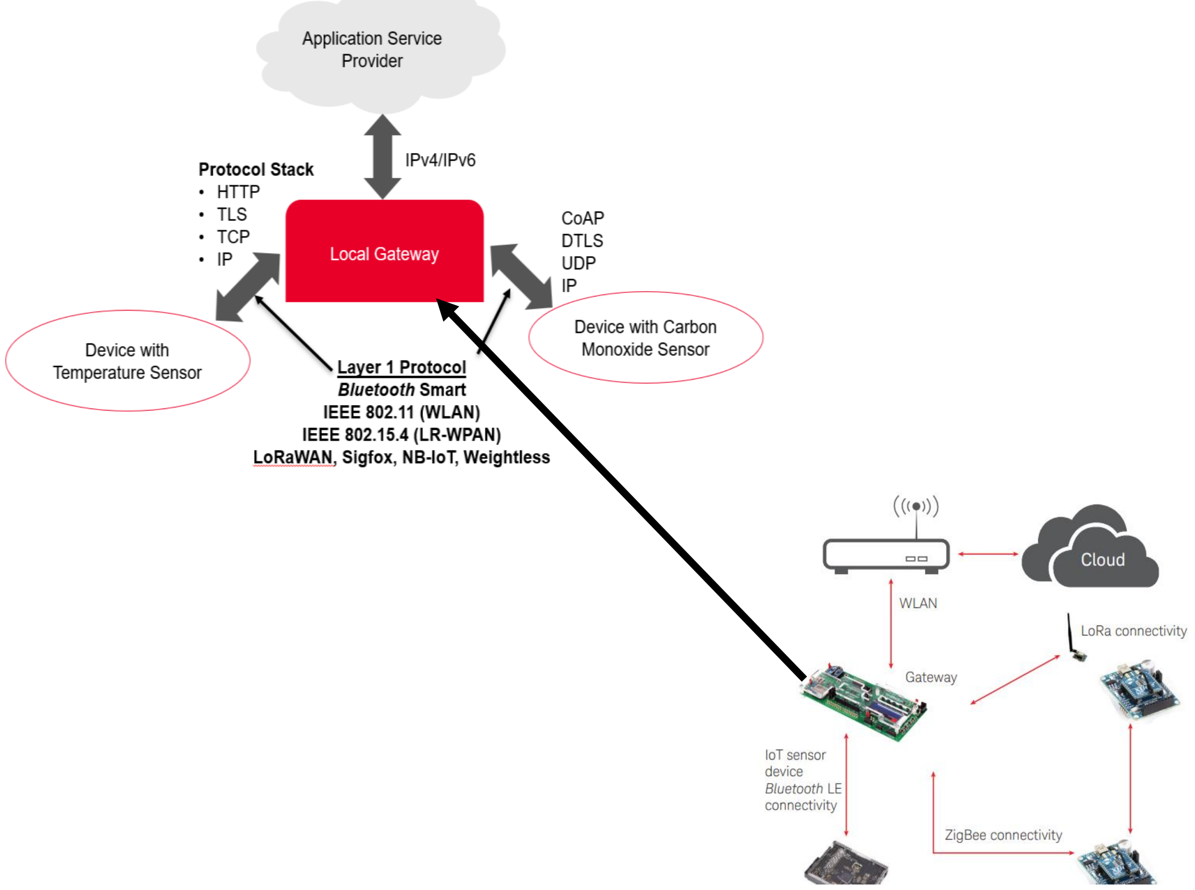
Device to device (M2M)



Device-to-cloud



Device to gateway/Gateway to data systems



IoT Communication Protocols

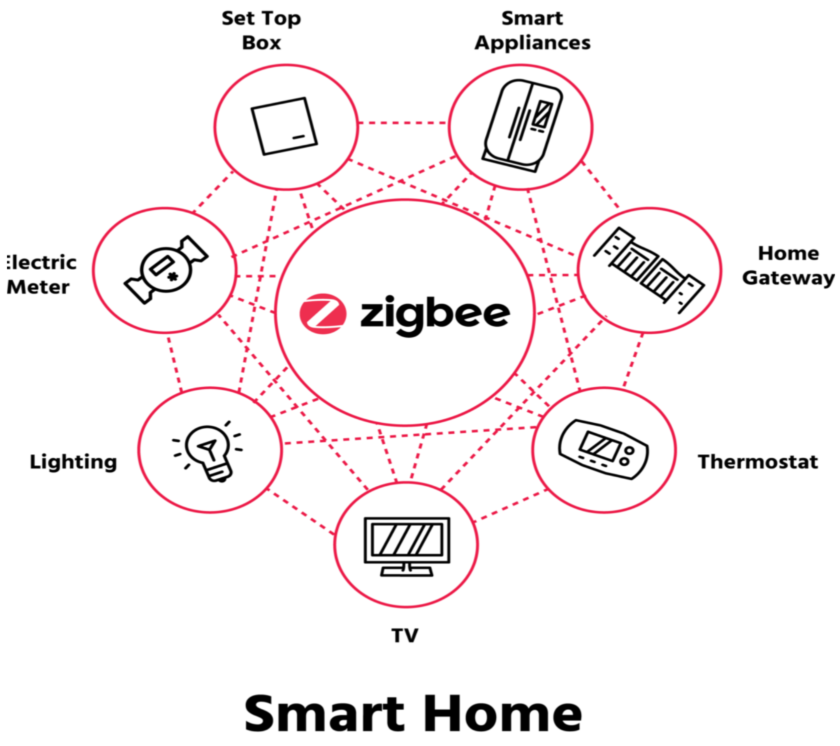
- Two main categories of IoT Communication Protocols
- 2.4GHz IoT protocols.
  - **Wi-Fi**
  - **Bluetooth Low Energy (BLE)**
  - **Zigbee**
  - **Thread**
- Sub-GHz IoT protocols
  - LPWAN - long-range, low-power connectivity and are suitable for a wide range of IoT applications,
    - **LoRaWAN**
    - **Sigfox**
    - **NB-IoT**
    - **Weightless**

Protocol	Range	Data Rate	Multimedia Support
WiFi	30-100 meters	11 Mbps - 10 Gbps	Yes
Zigbee	10-100 meters	20-250 kbps	No
Bluetooth	10 meters	1-3 Mbps	Yes
LoraWAN	Up to 10 km	0.3-50 kbps	No
NB-IoT	Up to 10 km	50-250 kbps	No
Sigfox	Up to 40 km	100 bps - 1 kbps	No
Z-Wave	Up to 100 meters	9.6-100 kbps	No
Thread	Up to 700 meters	250 kbps	Yes
6LoWPAN	Up to 100 meters	250 kbps	Yes
MQTT-SN	Up to several kilometers	10-250 kbps	No
CoAP	Up to several kilometers	10-250 kbps	Yes
LoRa	Up to 10 km	0.3-50 kbps	No
NB-Fi	Up to 5 km	100-250 kbps	No

University of Sunderland

What is Zigbee ?

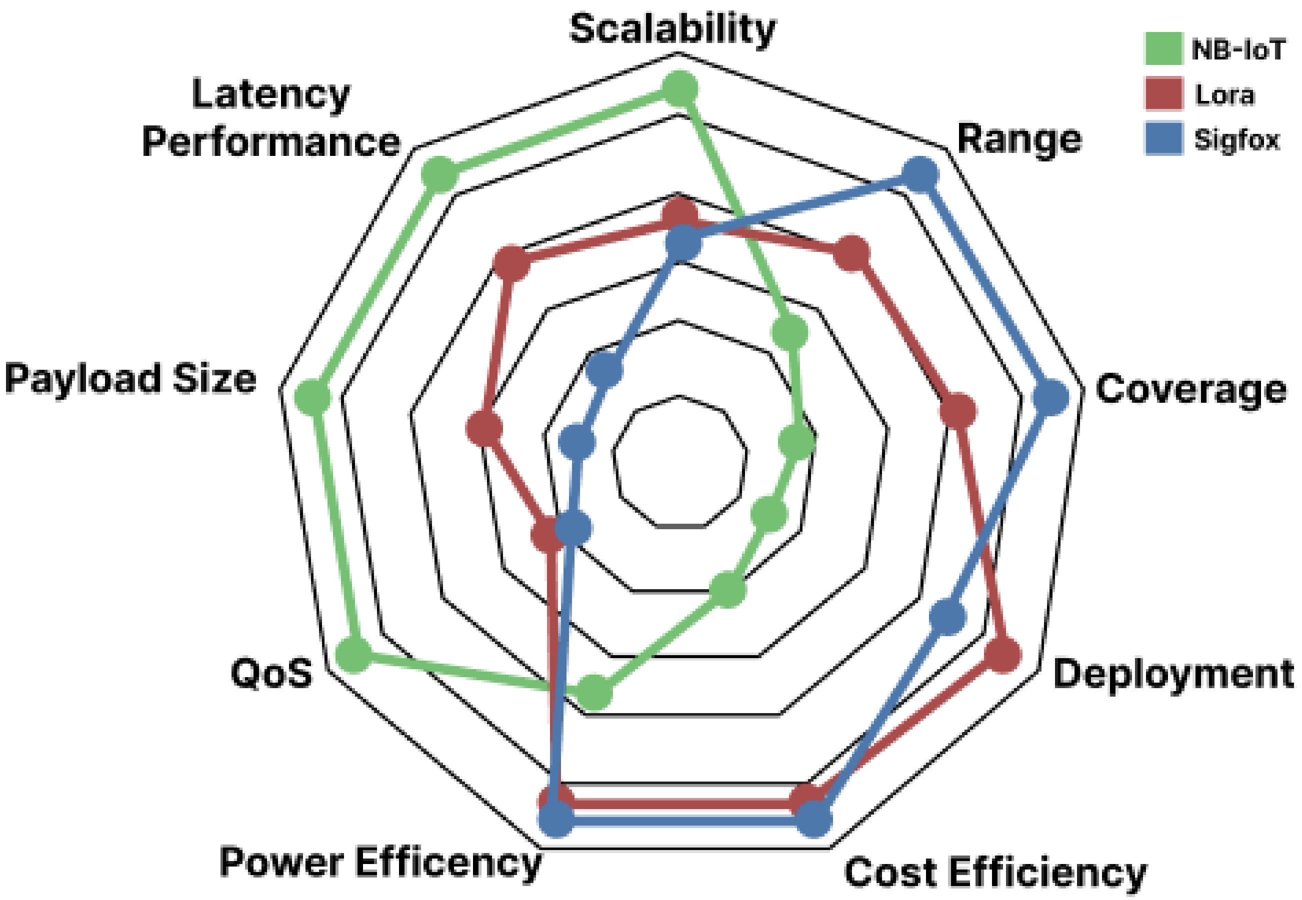
- Zigbee is a wireless communication protocol designed for low-power, low-data rate, and close-proximity applications. It is based on the IEEE 802.15.4 standard
- Applications: Home automation, Health care, Energy management
- **Why Zigbee Protocol ?**
  - **Low Power Consumption**
    - **Efficiency**: Zigbee devices are designed to be energy-efficient, which is crucial for battery-powered devices.
    - **Battery Life**: The protocol allows devices to have long battery life, often lasting several years on a single set of batteries.
  - **Mesh Networking**
  - **Range and Coverage**: Zigbee supports mesh networking, where each device (or node) can act as a repeater,
  - **Scalability**
    - **Large Networks**: Zigbee can support large networks with up to 65,000 nodes



University of Sunderland

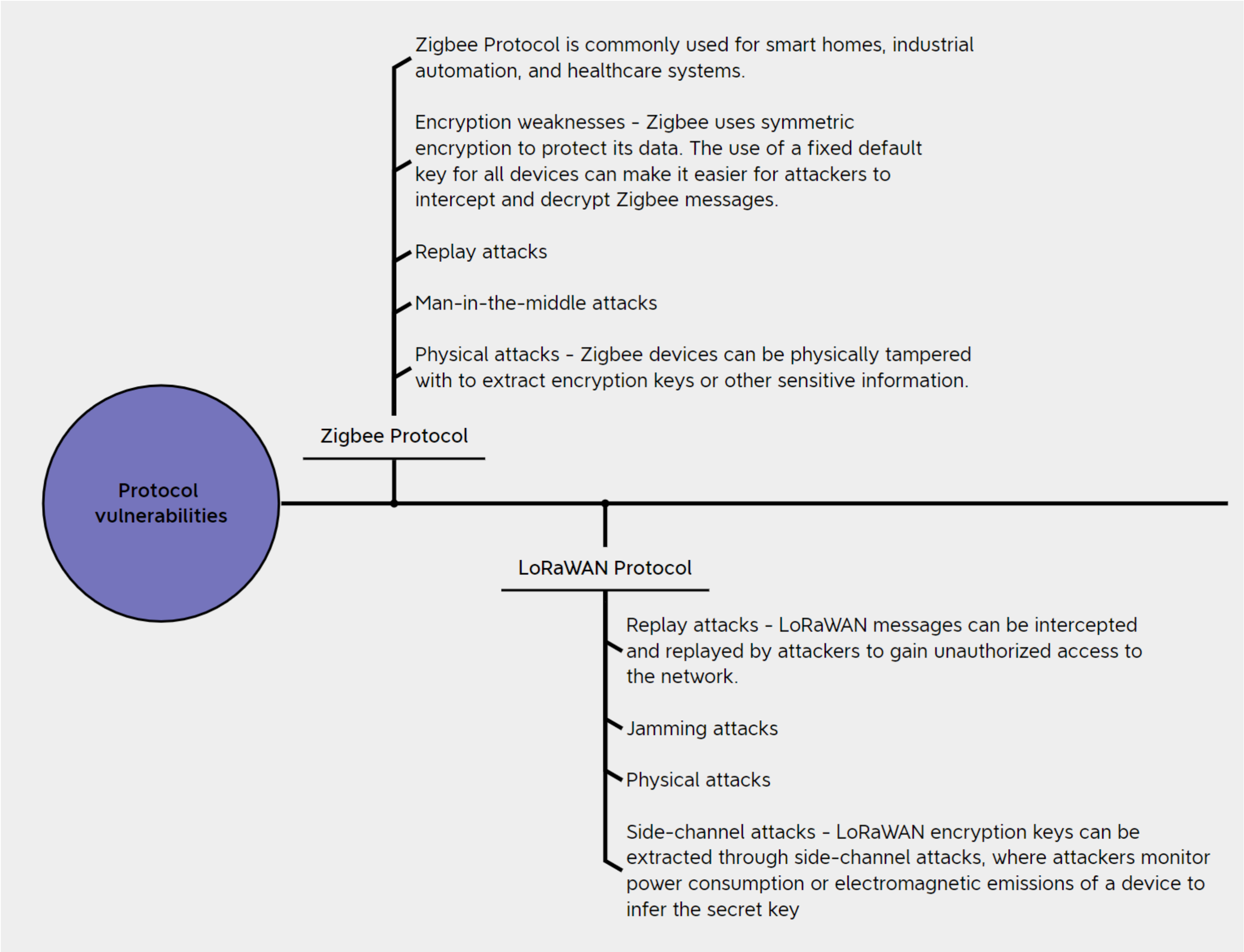
What is LoRaWAN?

- LoRaWAN is a low-power, wide-area network protocol designed for IoT applications.
- It enables long-range communication (Up to 10 km) with minimal power consumption.
- Key Features:
  - Long-range communication
  - Low power usage
  - Supports a large number of devices



[3]

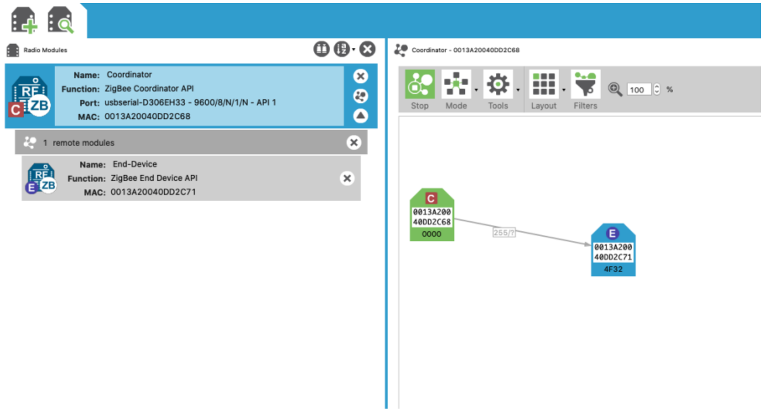
University of Sunderland



University of Sunderland

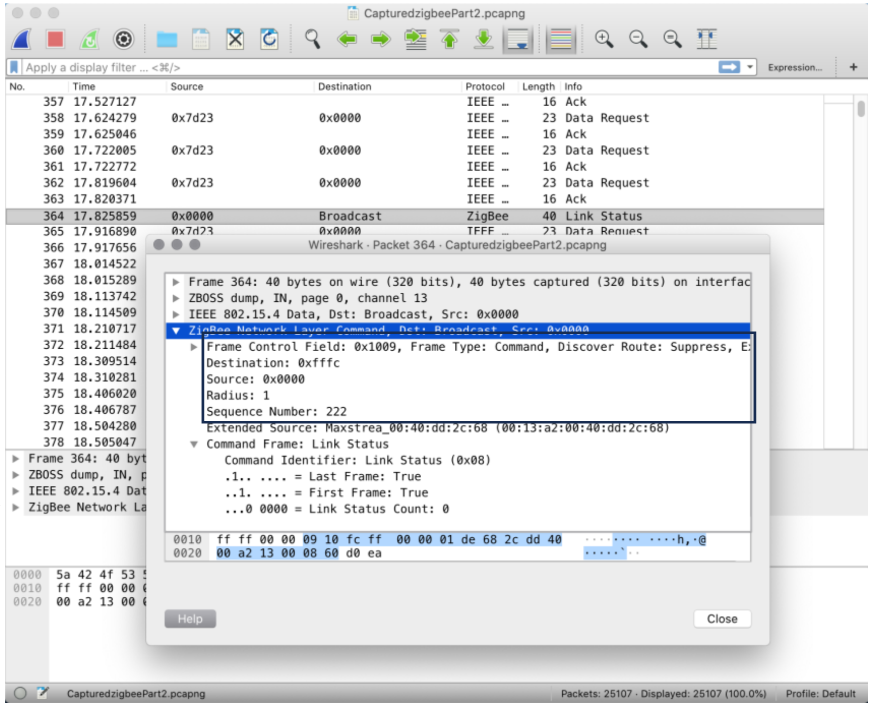
Zigbee Vulnerabilities – Replay attacks

CC2351 Sniffer



- **How a Zigbee Replay Attack Works:**
  1. Captures a legitimate data packet transmitted between Zigbee devices.
  2. The captured packet is analysed to understand its structure and the commands it contains.
  3. Retransmits the intercepted packet at a later time to the Zigbee network.
  4. The network accepts the replayed packet as a legitimate command, causing devices to execute the actions specified in the packet.

- **Tools and Equipment**
- **Hardware:**
  - Zigbee Sniffer (e.g., TI CC2531 USB dongle)
  - Zigbee Transmitter (e.g., XBee modules)
- **Software:**
  - Wireshark
  - Scapy
  - KillerBee framework

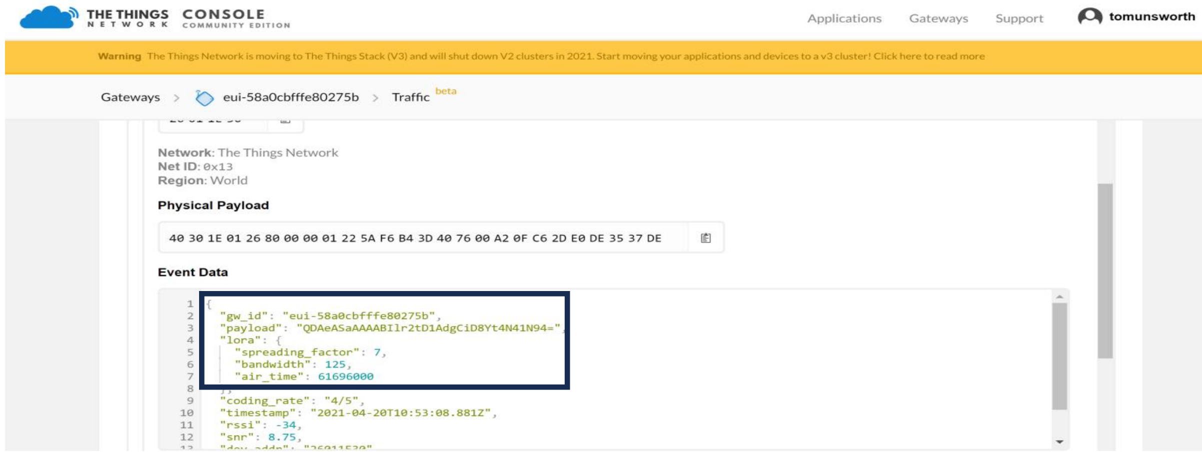


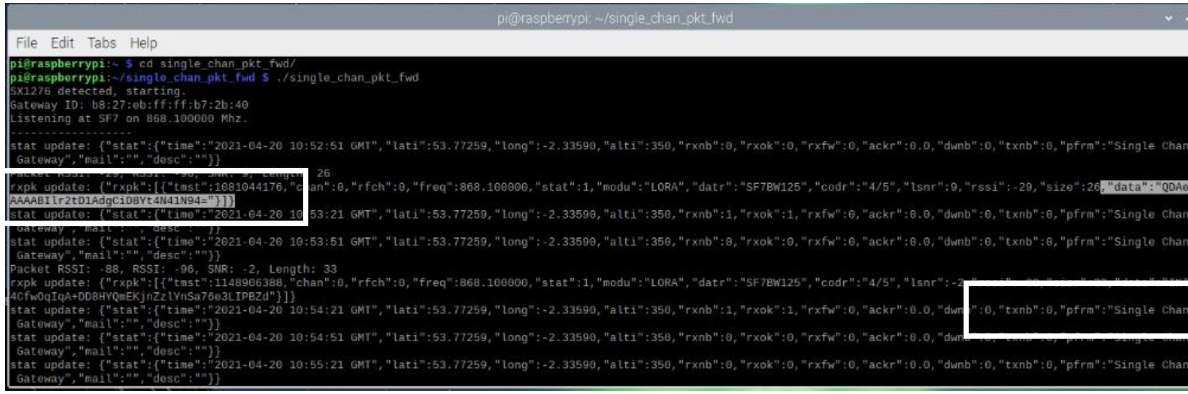
University of Sunderland

LoRaWAN Replay Attack

- **Attack Vector:**
  - Capture valid LoRaWAN packets during legitimate communication.
  - Replay the captured packets to achieve unauthorized actions.
- Sniffing LoRaWAN Traffic:
  - LoRaMon to capture LoRaWAN packets.
- Analyzing Captured Packets:
  - Identify packets suitable for replay.
  - Extract necessary data fields (e.g., frame counters, payload).
- Replaying Captured Packets

Capturing OTAA Join Request Packet with Rnode





Malicious Gateway Sniffing OTAA Join Request

University of Sunderland

Summary of the findings Replay attacks on LoRaWan and Zigbee

- Both Zigbee and LoRaWAN use AES-128 encryption and nonces/frame counters to mitigate replay attacks. The effectiveness largely depends on the proper implementation and management of these security features.

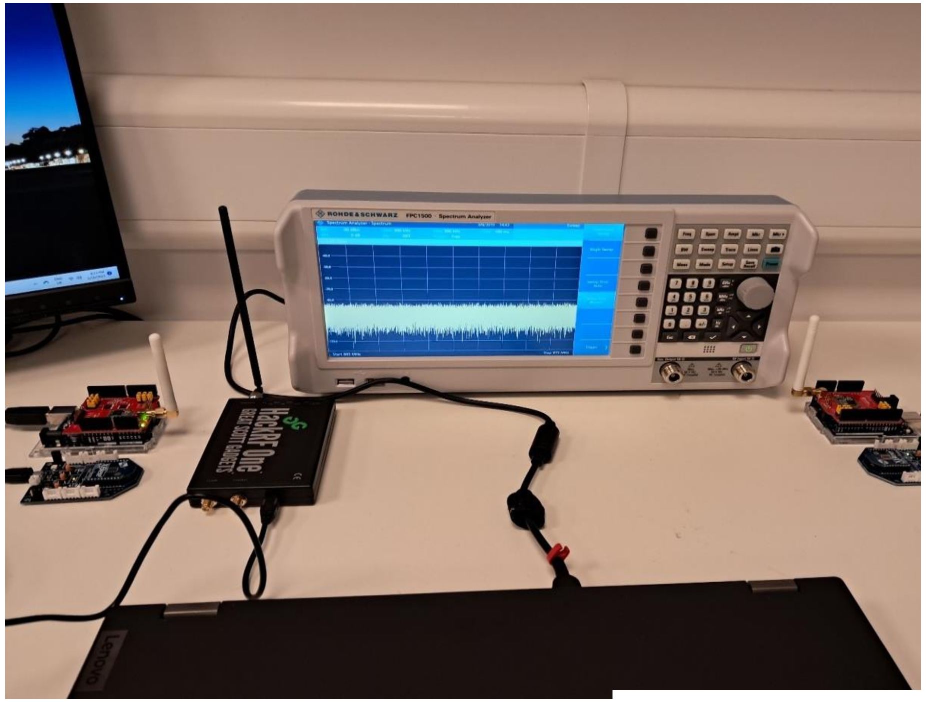
- LoRaWAN's long-range and wide-area applications introduce different attack vectors, but the strict counter management typically offers robust protection against replay attacks.

University of Sunderland

Signal Jamming Against LoRaWAN and Zigbee

- **Details of the Attack**

1. **Identification of Target Devices**:
    1. We used a spectrum analyzer to identify the frequency bands used by the Zigbee devices (2.4 GHz) and for LoRaWAN (868MHZ).
2. **Jamming Equipment**:
    1. Spectrum analyzer
    2. HackRF One
    3. Two Xbee modules configured using XTU
    4. Two Lora shield modules, two MCUs, and two Air quality sensors
3. **Execution**:
    1. The jamming device was placed within range of the Xbee modules and LoRa shields, broadcasting continuous noise or random data at the 2.4 GHz frequency, effectively drowning out the Zigbee signals.
    2. This prevented Zigbee devices from communicating with each other, causing the network degradation.

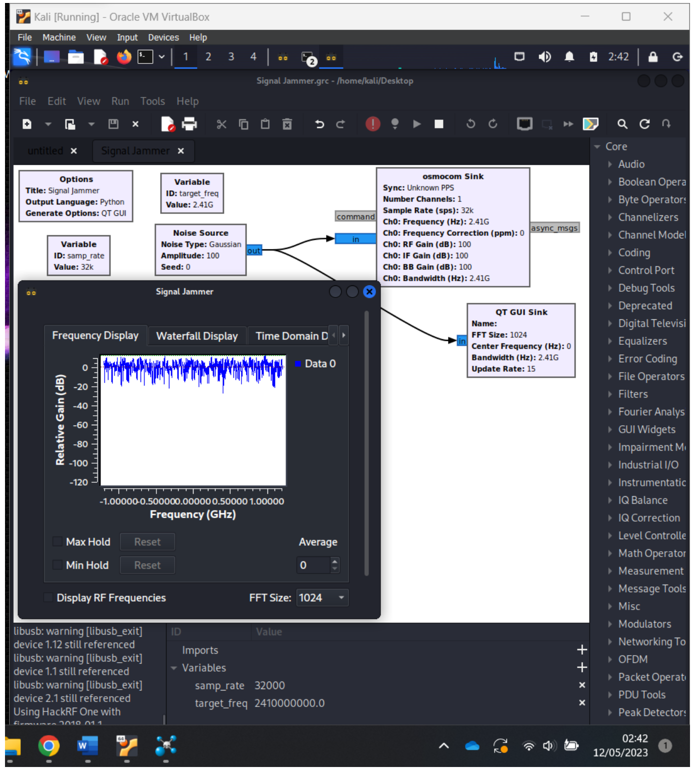


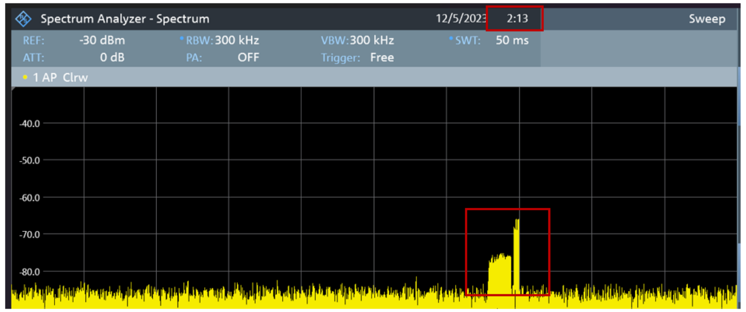
University of Sunderland

Experiment set-up

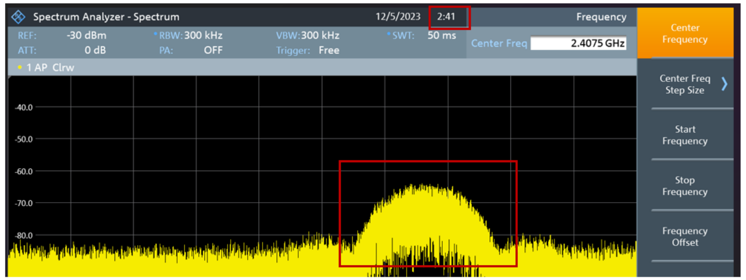
Impact of the attacks on Zigbee networks

- We applied Gaussian noise.
- $N(t) = A * N\ (0, \delta^2)$
- Where:
- $N(t)$ represents the Gaussian noise signal as a function of time.
- A is the amplitude of the noise signal.
- N (0, σ2) denotes a Gaussian (normal) distribution with mean 0 and variance δ^2.

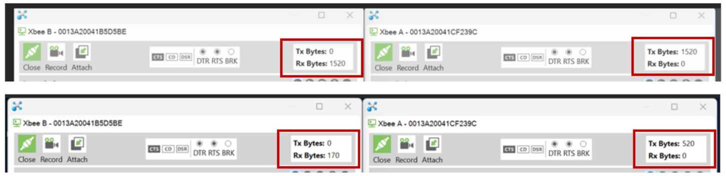




ZigBee Transmission Signal Trace Before Attack



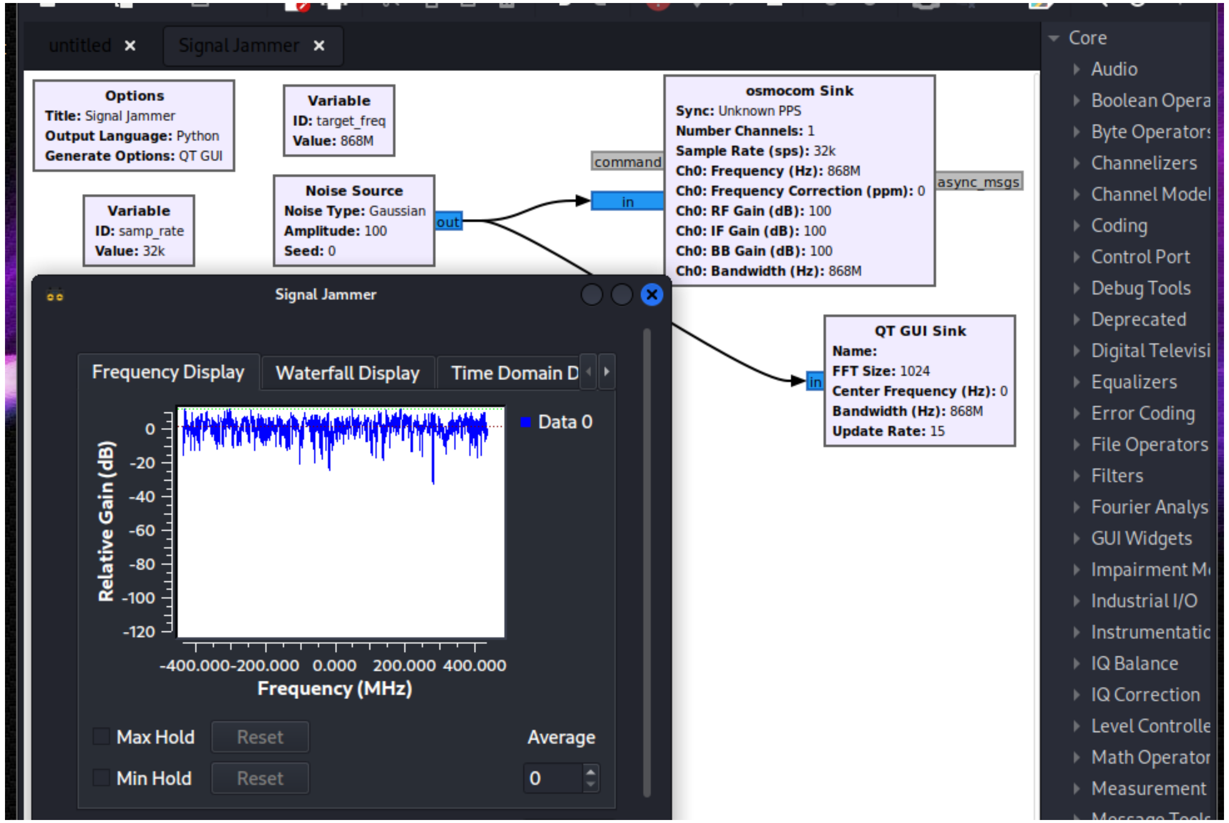
ZigBee Transmission Signal Trace During the Attack

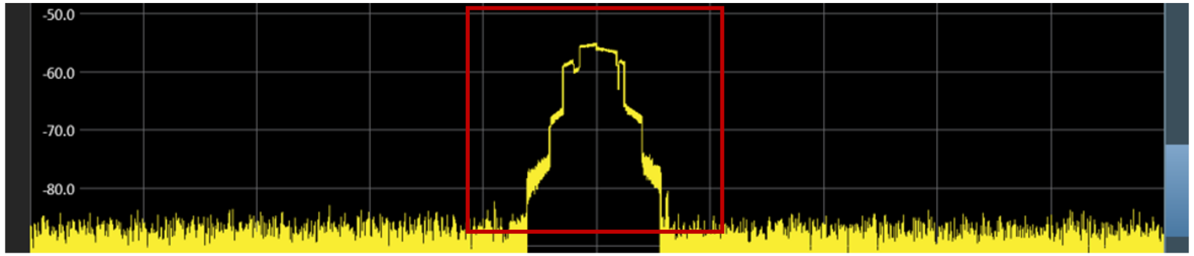


ZigBee Data Transmission Before and During the Attack

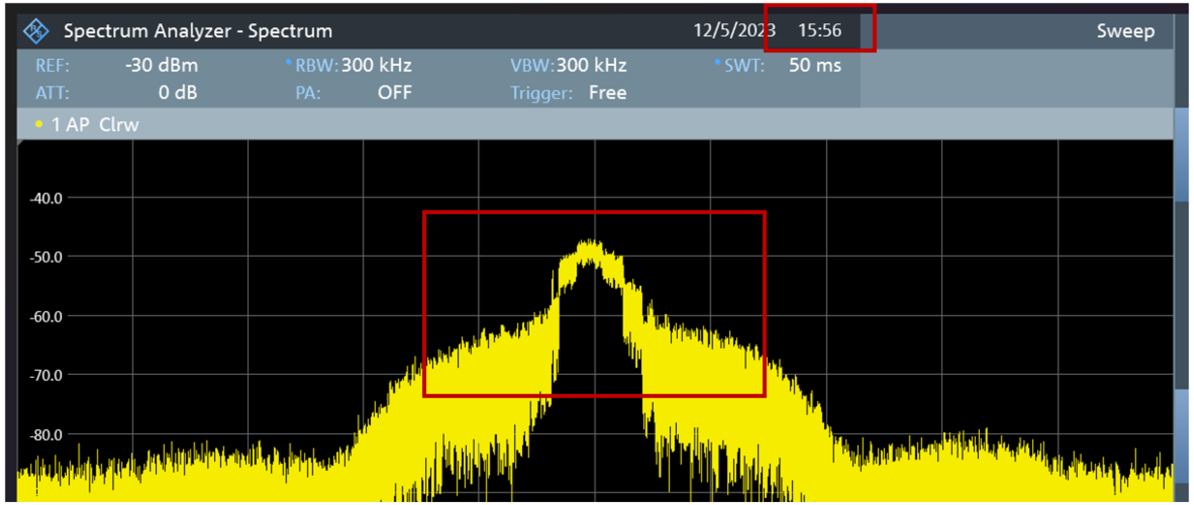
University of Sunderland

Impact of the attacks LoRaWAN networks





LoRa Transmission Signal Trace Before Attack



Summary of the findings: Signal Jamming on LoRaWan and Zigbee

- We were able to establish that the ZigBee network was more vulnerable to signal jamming attacks than the LoRa network.
- **The ZigBee network completely stopped transmitting data in the presence of a signal jamming attack.**
- In contrast, the LoRa network was able to transmit data even in the presence of the same intensity of signal jamming.
- The LoRa network's ability to transmit data in the presence of signal jamming is due to its use of a spread-spectrum technique that distributes the signal over a wide range of frequencies, making it difficult for an attacker to jam the entire signal.

1. Is it possible to **securely** transfer large amounts of **data** over LoRa?

2. How can we develop a public display architecture that leverages the capabilities of LoRaWAN and Ethereum smart contract technology to ensure tamper-resistant and transparent data integrity through advanced peer-to-peer security measures?

University of Sunderland

Q1 - Is it possible to securely transfer large amounts of data over LoRa?

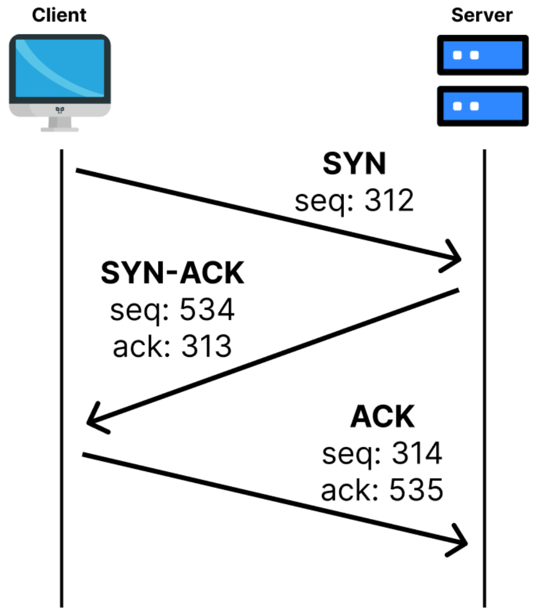
- [1] A study by Kirichek et al. (2017) demonstrated that it is possible to transfer large amounts of data over LoRa by dividing the data into sections and transmitting each section individually. However, the results indicated that when transferring images, there was a packet loss ranging from a minimum of **9.86%** to a maximum of **18.29%.**

- [2] Jebril et al. (2018) employed similar methods to develop a new approach. The study successfully transmitted images over distances of up to 6 km, with no packet loss observed between 1 and 4 km. However, of the 21 images sent, only 12 were successfully transferred due to packet loss beyond the 4 km range. The data was encrypted using hexadecimal encryption, which the authors considered not very secure and suggested could be improved.

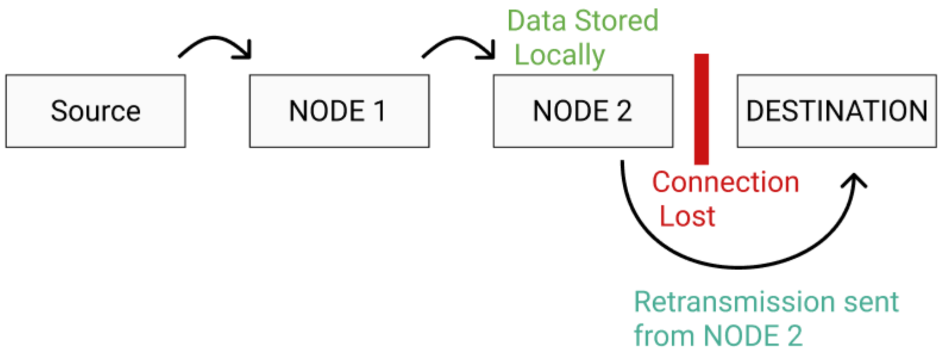
University of Sunderland

TCP and DTN

- Transmission Control Protocol



Delay Tolerant Networking (DTN)



Store-and-Forward

Application Areas: Space communications, remote or rural area networking, disaster recovery, military communications, and undersea exploration.

Enhancing the LoRa Physical Layer for Efficient Large-Scale Data Transmission

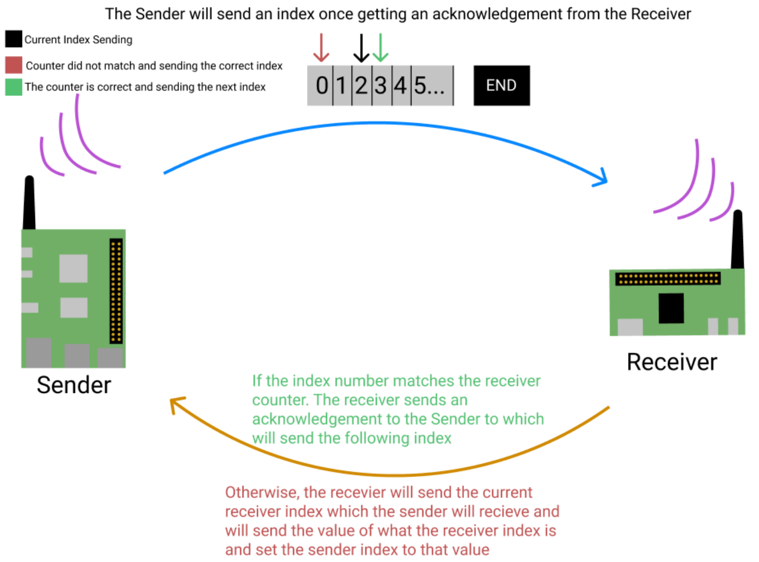
- We used **Brotli Compression and AES encryption**

- Preliminary results
  - Acknowledgement testing had a 100% pass rate out of the 240 tests.
  - No Acknowledgement testing had an overall pass rate of 70%.
  - 0% packet loss using the acknowledgement method and use AES encryption while sending the device up to 8km.

The average, minimum and maximum times for the distances split by encryption and plaintext for Acknowledgements and no acknowledgement tests

Acknowledgements					
Encryption	***Distance(km)***	***Number Of Tests Passed***	***Minimum Time***	***Maximum Time***	***Total retransmission***
Plaintext	0.5	15	0:02:17.00	0:02:35.00	2
	1.0	15	0:02:13.00	0:02:23.00	0
	1.5	15	0:02:16.00	0:02:21.00	0
	2.0	15	0:02:15.00	0:02:33.00	0
	3.0	15	0:02:16.00	0:02:32.00	1
	4.0	15	0:02:18.00	0:02:33.00	4
	6.0	15	0:02:12.00	0:02:36.00	0
	8.0	15	0:02:30.00	0:03:44.00	4
Encrypted	0.5	15	0:03:16.00	0:03:30.00	0
	1.0	15	0:03:18.00	0:03:38.00	2
	1.5	15	0:03:19.00	0:03:31.00	1
	2.0	15	0:03:19.00	0:03:37.00	4
	3.0	15	0:03:16.00	0:03:32.00	2
	4.0	15	0:03:22.00	0:03:34.00	1
	6.0	15	0:03:20.00	0:03:49.00	0
	8.0	15	0:04:09.00	0:22:35.00	64
No Acknowledgements					
Encryption	***Distance(km)***	***Number Of Tests Passed***	***Minimum Time***	***Maximum Time***	***Mean (Time)***
Plaintext	0.5	14	0:00:15.00	0:00:27.00	0:00:15.86
	1.0	15	0:00:14.00	0:00:15.00	0:00:14.93
	1.5	13	0:00:15.00	0:00:16.00	0:00:15.15
	2.0	14	0:00:15.00	0:00:17.00	0:00:15.14
	3.0	15	0:00:15.00	0:00:15.00	0:00:15.00
	4.0	13	0:00:15.00	0:00:15.00	0:00:15.00
	6.0	3	0:00:15.00	0:00:15.00	0:00:15.00

File	Raw Data Size (Kilobytes) (RDS)	Compressed Data Size (Kilobytes) (CDS)	Encrypted and Compressed Data Size (Kilobytes) (ECDS)	Percentage Change Of The Decrease File Size (RDS vs CDS)	Percentage Change Of The Decrease File Size (RDS vs ECDS)
Index.html	2.838	1.056	1.477	62.79%	47.95%
Update.js	8.487	2.451	3.353	71.12%	60.49%



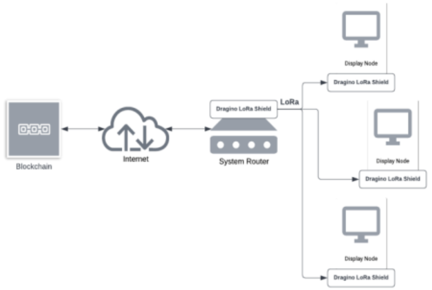
University of Sunderland

How can we develop a public display architecture that leverages the capabilities of **LoRaWAN** and **Ethereum smart contract** technology to ensure tamper-resistant and transparent data integrity through advanced peer-to-peer security measures?

- **Why Ethereum Smart contract ?**
- **Encryption**
  - Sensitive data can be encrypted before being stored on the blockchain, ensuring that even if the data is public, its contents remain confidential unless decrypted by an authorized party.
- **Access Control**
  - Smart contracts can implement access controls to restrict who can read or modify certain data.
- **Zero-Knowledge Proofs**
  - **Privacy-Preserving Transactions**: Utilising cryptographic techniques such as zero-knowledge proofs (ZKPs), smart contracts can prove the validity of transactions without revealing the underlying data, thus maintaining privacy while ensuring correctness.

University of Sunderland

Blockchain-Enabled Security Augmentation and LoRaWAN Integration for Resilient Public Display Networks

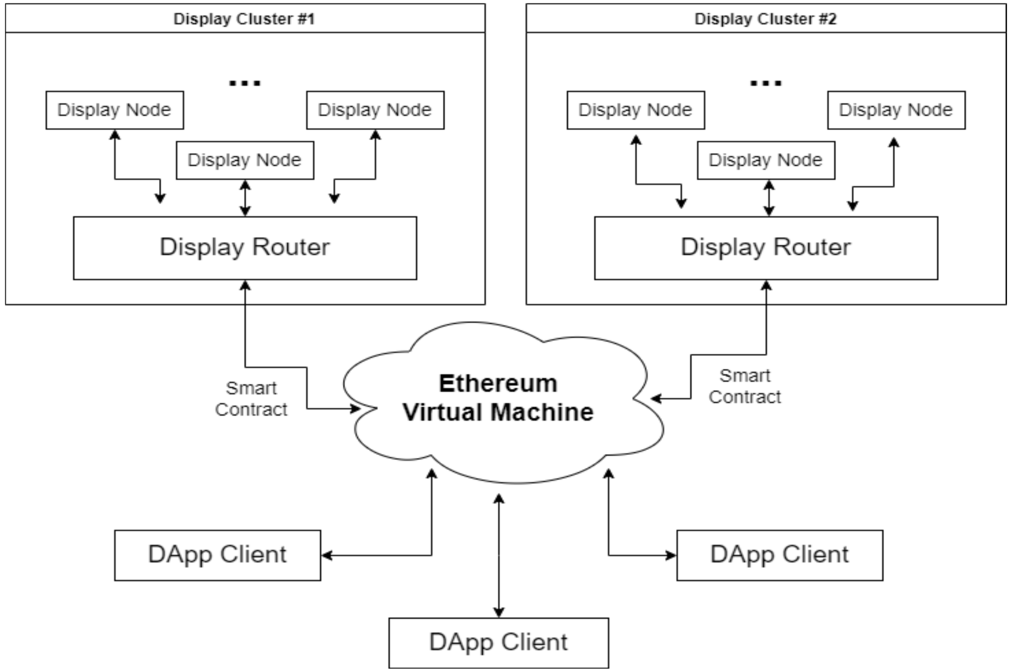


LoRa (long range) Implementation of the display networks


Piccadilly Circus in London/UK


Data Visualization Lab at University of Sunderland Utilizing Public Display Systems

- System Architecture
  - the DApp client represents a user connected to the system through the web application end, communicating through our Ethereum blockchain to interact with the displays.
  - the display router of the system is focused on handling a cluster of displays in multiple remote areas and maintaining communication with the blockchain.
  - any interaction in the system between a device and the blockchain utilises a smart contract
  - the display nodes are isolated in a private LoRa network with the only internet access device being the display router.
  - API communication and SQL queries responsible for data handling have been replaced with smart contracts through the use of Solidity code.



System Architecture

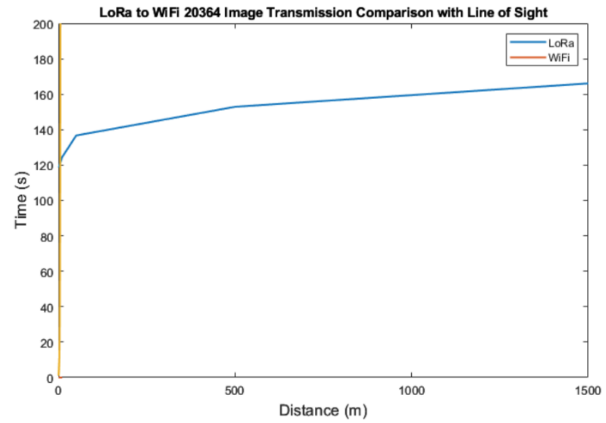
Blockchain-Enabled Security Augmentation and LoRaWAN Integration for Resilient Public Display Networks

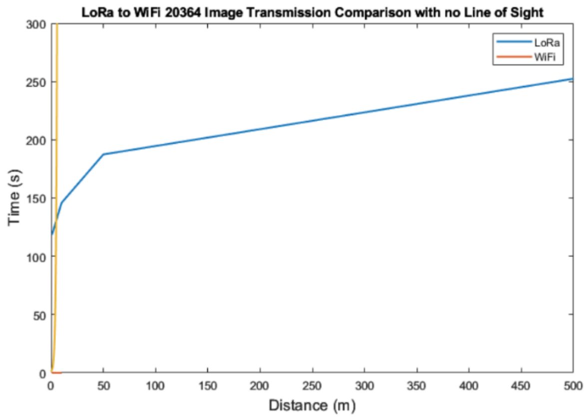
Blockchain-Enabled Security Augmentation and LoRaWAN Integration for Resilient Public Display Networks

Norbert Dajnowski[1,] and Aminu Bello Usman[2], and John Murray[2]

Summary of Functionality Requirement Tests

Test ID	Test type	Test description	Results of the test
1	Functionality test	On Client's web application connection, are they assigned an existing and exclusive wallet address?	User was able to see their unique wallet address on the top of the main web page
2	Functionality test	Does minting a new custom token work through the web application?	User was able to upload an image and generate an ERC-721 token into their wallet using the web application.
3	Functionality test.	Are all the user's ERC-721 tokens and available display devices listed on the main web page?	User able to see all his owned nonfungible tokens and the available display devices.
4	Functionality test.	Does deploying a token to an available display device work?	User is able to display his ERC-721 token on one of the





- This study introduces a decentralised public display method, replacing traditional centralised server architectures with a blockchain operating at edge level.
- The proposed architecture offers tamper-resistant data integrity, decentralised data storage, and contributing to the evolution of public display networks.

University of Sunderland

- How can Privacy by Design principles be effectively incorporated into the development of a comprehensive biometric authentication framework for one-to-many system at edge ?

Privacy-Enhanced One-to-Many Biometric System Using Smart Contracts: A New Framework

- What approaches can be developed to harness the potential of LPWAN and blockchain technology for the purpose of optimizing both privacy and transparency in the realm of biometric authentication within one-to-many systems?

Privacy-Enhanced One-to-Many Biometric System Using Smart Contracts: A New Framework

1st Alec Wells
School of Computer Science
University of Sunderland
Sunderland,United Kingdom
alec.wells@research.sunderland.ac.uk

2nd Norbert Dajnowski
Department of Computer Science
York St John University
York, United Kingdom
norbertdajnowski@gmail.com

3rd Aminu Bello Usman
School of Computer Science
University of Sunderland
Sunderland, United Kingdom
aminu.usman@sundeland.ac.uk

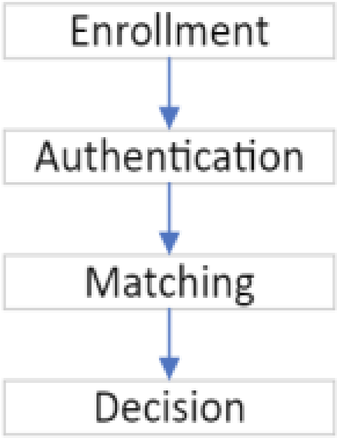
4th John Murray
Faculty of Technology
University of Sunderland
Sunderland, United Kingdom
john.murray@sunderland.ac.uk

5th Bassel Barakat
School of Computer Science
University of Sunderland
Sunderland, United Kingdom
basel.barakat@sunderland.ac.uk

University of Sunderland

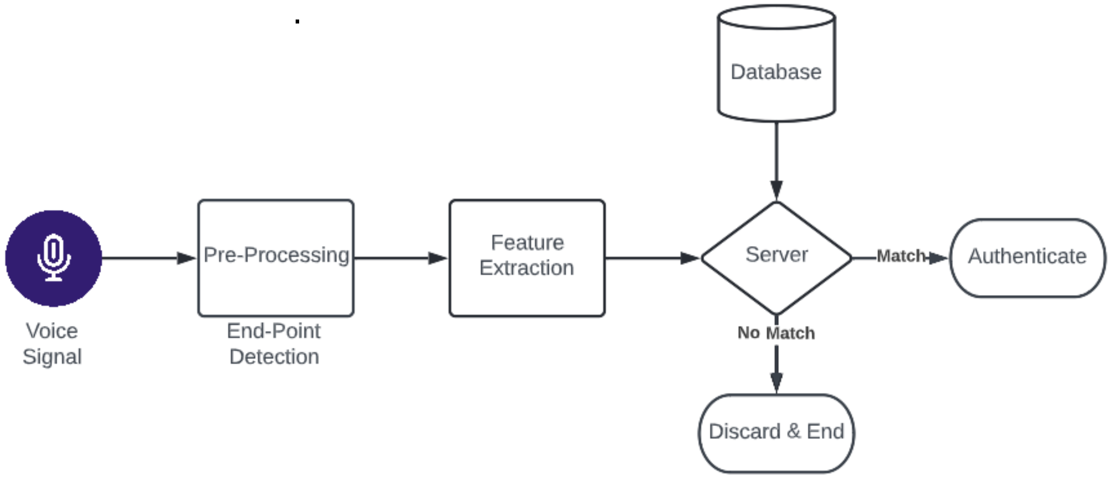
One-to-one biometric system

One-to-one biometric systems are designed for authentication purposes, where the primary goal is to confirm a claimed identity



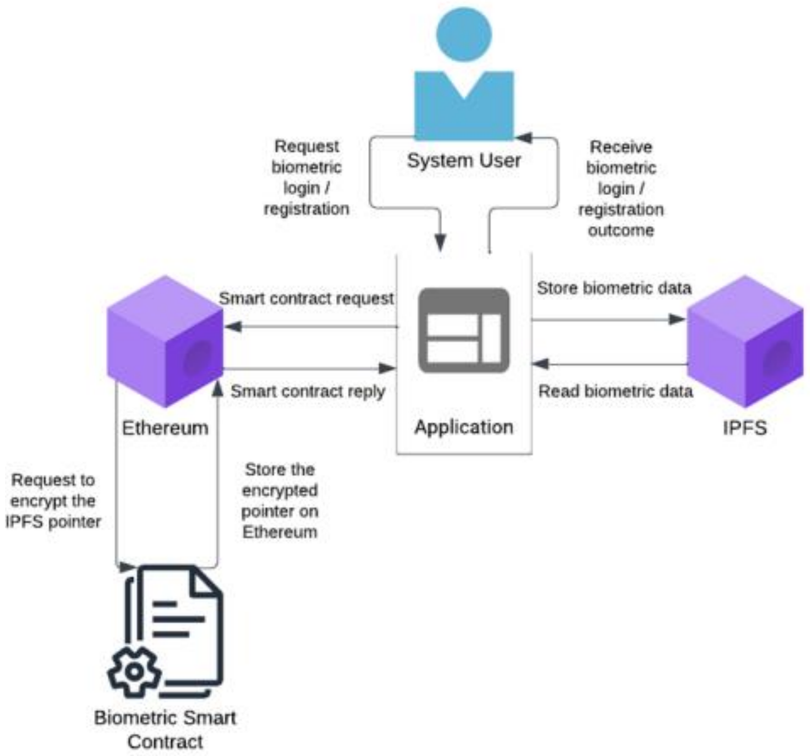
One-to-many biometric system

One-to-many biometric systems are designed for identification purposes, where the goal is to determine an individual's identity from a large database of stored templates without prior knowledge of their claimed identity.



University of Sunderland

Privacy-Enhanced One-to-Many Biometric System Using Smart Contracts: A New Framework

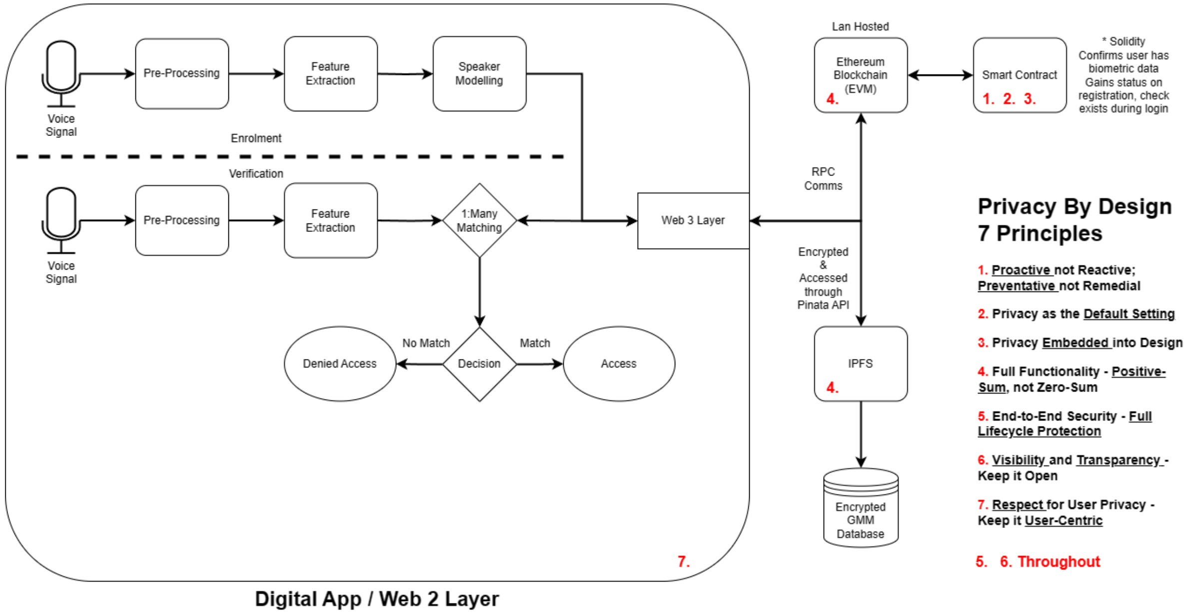


- User's biometric data will be split into blocks of 256 kilobytes and assigned unique identifiers
- The data will then be encrypted and stored across the blockchain
- The InterPlanetary File System (IPFS) decentrally hosts the system's sensitive data
    - Why IPS?
    - IPS is a peer-to-peer distributed file system that aims to connect all computing devices with the same system of files.
    - Improved Speed and Efficiency
    - To reduce gas fees
    - **Data Integrity and Security**:

- The Ethereum smart contract serve as a repository for storing pointers and encryption keys that grant access to biometric data on the IPFS blockchain
- The smart contract assumes the responsibility of safeguarding the privacy and tracking the IPFS biometric data pointers

Security features of the Framework

- **Single point of failure** - In contrast to centralised systems, this framework eliminates single point of failure, providing enhanced robustness and reliability.
- **Data integrity** - Improved data integrity is introduced, since all blockchain transactions must be publicly validated on the network.
- **Encryption** - All data stored on the blockchain is encrypted to ensure user's privacy is maintained, and their credentials are inaccessible to other network users.
- **Transparency** - Blockchain's transparent nature provides a verifiable history of immutable transactions, and com-prehensive audit trails.
- **Insider threat** - Prevents scenarios in which a system administrator or insider could maliciously tamper with user data.



Conclusion

Embracing the future of IoT security requires a dual focus on robust network protection and innovative privacy-enhanced biometric systems at the edge.

- Scalability of Biometric Systems: Developing scalable biometric authentication systems that can efficiently handle large numbers of IoT devices without compromising security or performance at edge.

- Addressing security challenges specific to edge computing environments, such as limited computational resources, heterogeneous devices, and distributed processing.

- Privacy-Preserving Biometric Data Handling: Designing techniques to securely collect, store, and process biometric data at the edge while preserving user privacy and complying with regulations like GDPR.

University of Sunderland

References

- [1] Kirichek, R., Pham, V.D., Kolechkin, A., Al-Bahri, M. and Paramonov, A., 2017. Transfer of multimedia data via LoRa. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 17th International Conference, NEW2AN 2017, 10th Conference, ruSMART 2017, Third Workshop NsCC 2017, St. Petersburg, Russia, August 28–30, 2017, Proceedings 17 (pp. 708-720). Springer International Publishing.
- [2] Jebril, A.H., Sali, A., Ismail, A. and Rasid, M.F.A., 2018. Overcoming limitations of LoRa physical layer in image transmission. Sensors, 18(10), p.3257.
- [3] Mekki, K., Bajic, E., Chaxel, F. and Meyer, F., 2019. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT express, 5(1), pp.1
- [4] Schaar, P., 2010. Privacy by design. Identity in the Information Society, 3(2), pp.267-274.
- [5] Cavoukian, A. and Stoianov, A., 2014. Privacy by design solutions for biometric one-to-many identification systems.
- [6] Tomko, G.J., Mytec Technologies Inc, 1998. Method and apparatus for securely handling data in a database of biometrics and associated data. U.S. Patent 5,790,668.
- [7] Abdullah, M.F.A., Bashier, H.K., Sayeed, S., Yusof, I., Azman, A., Ibrahim, S.Z. and Liew, T.H., 2014.. *Journal* Answering Incoming Call For Implicit Authentication Using Smartphone *of Theoretical & Applied Information Technology*, *61*(1).
- [8] Wells, A. and Usman, A.B., 2024. Privacy and biometrics for smart healthcare systems: attacks, and techniques. Information Security Journal: A Global Perspective, 33(3), pp.307-331.

University of Sunderland