**Cryptographic Methods for Sensitive Data Protection in a Simulated IoT Network**

Project 2

Aniyah Hall & Sanchez Salvador

**BOWIE STATE UNIVERSITY**

CTEC445.101

Fall 2024

**Table of Contents**

**1. Introduction Page 3**

**2. Problem Statement Page 3**

**3. The Broader Impacts Page 4**

**4. Purpose of the Research Page 4**

**5. Case Study Page 5**

**6.Methogloies Page 5**

**6. Summary Page 14**

**References**

**Introduction**

The Internet of Things (IoT) is a rapidly expanding technology with a wide range of healthcare applications. It refers to a network of connected vehicles, physical devices, software, and electronic items that enable data exchange. IoT provides the IT infrastructure for the secure and reliable exchange of data. Implementations of IoT present new and unique security challenges. The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. [1]A cohesive environment of proprietary IoT technical implementations will ensure user and industry value. This project will explore cryptography methods to ensure sensitive data's privacy, integrity, and confidentiality in a simulated network. [1]With educational articles and testing software and tools, we will research cryptographic techniques. This will offer valuable insights into the strengths and limitations of diverse methods, meeting the rising demand for robust security solutions in an interconnected world.[2]

ChatGPT

In the era of smart devices and interconnected systems, the Internet of Things (IoT) has become a cornerstone of modern technology, revolutionizing industries, especially healthcare, transportation, and home automation. However, the rapid growth of IoT has also introduced significant security challenges, particularly in safeguarding sensitive data transmitted across these networks. Given the vast amounts of personal and business-critical data shared between devices, protecting this data from unauthorized access and breaches is paramount.

This research project focuses on applying cryptographic methods to ensure sensitive data's confidentiality, integrity, and availability in a simulated IoT network. Through theoretical research and practical implementation, this project will explore various cryptographic techniques, testing their effectiveness in real-world IoT environments. This will provide valuable insights into the strengths and limitations of different methods, contributing to the growing need for robust security solutions in an increasingly interconnected world.

**Problem Statement**

The rapid increase in IoT devices has raised concerns about data security and privacy. Current cryptographic methods are not enough to protect against cyber-attacks, leaving networks vulnerable. Failing to secure IoT networks can lead to serious privacy breaches and financial losses. Addressing this issue will improve the reliability of IoT networks and encourage wider adoption of IoT technology in critical sectors. This research aims to investigate advanced cryptographic techniques for safeguarding sensitive IoT data. The primary question is: Which cryptographic methods offer the most robust protection against data breaches in IoT environments? The study will focus on encryption methods applicable to small-scale IoT networks and will not cover large-scale industrial IoT applications.

ChatGPT

As IoT devices become more pervasive, they transmit sensitive data across vast networks, often without adequate security measures. The decentralized nature of IoT, combined with its resource-constrained devices, makes these networks particularly vulnerable to cyberattacks such as data breaches, eavesdropping, and unauthorized access. Traditional security mechanisms are not always effective in securing IoT environments, which demand lightweight yet robust solutions.

The challenge lies in identifying and implementing cryptographic methods that can secure sensitive data without overburdening the limited computational and energy resources of IoT devices. This project addresses this issue by testing various cryptographic techniques in a simulated IoT network to determine the most effective method for protecting sensitive data while ensuring system performance and reliability.

**The Broader Impacts**

This research on secure IoT networks could lead to improved privacy protections for personal health data, enhancing patient trust in digital healthcare solutions. The proposed cryptographic methods could also result in more secure communication protocols for IoT devices, making smart home and industrial applications safer. Enhancing data security in IoT networks could reduce the risk of costly data breaches, potentially saving companies millions.

ChatGPT

The broader impacts of this research extend beyond the technical field of cryptography and IoT security. By identifying effective cryptographic methods for securing sensitive data in IoT networks, this project contributes to the development of safer, more reliable systems in various industries, including healthcare, finance, and smart cities. Enhanced IoT security can lead to improved privacy protections for individuals, safeguarding personal data from breaches and misuse.

Additionally, this research supports societal advancements by fostering trust in IoT technologies, encouraging further innovation and adoption. With more secure IoT infrastructures, businesses and governments can deploy IoT solutions with confidence, driving efficiencies and offering new services that improve quality of life. Ultimately, securing IoT networks not only protects data but also helps address broader concerns of cybersecurity and privacy in an increasingly interconnected world.

**Purpose of Research**

This research explores cryptographic methods for protecting sensitive data in IoT networks and maintaining system efficiency. IoT Systems are very vulnerable and require the best methods to ensure security. This research seeks to provide solutions for real-world IoT applications.

ChatGPT

The purpose of this research is to explore and evaluate cryptographic methods that can effectively protect sensitive data in IoT networks while maintaining system efficiency. Given the vulnerabilities inherent in IoT systems due to their decentralized nature and limited computational resources, this study aims to identify cryptographic techniques that offer a balance between security and performance. By simulating IoT environments and testing various cryptographic methods, the research seeks to provide practical solutions for enhancing data security in real-world IoT applications, ensuring confidentiality, integrity, and availability of critical information

**Case Study**

In 2013, Target experienced a significant data breach that affected over 40 million customers, with hackers gaining access to sensitive data such as credit card information. The attackers exploited a third-party vendor to infiltrate Target’s network, installing malware on the point-of-sale systems. In response to the breach, Target faced multiple challenges, including the need to secure customer data and prevent future unauthorized access, especially as IoT devices began playing a larger role in their operations. These challenges highlighted the importance of strengthening security protocols and adopting cryptographic methods for data protection.

Following the breach, Target implemented several cryptographic techniques to safeguard sensitive data within a simulated IoT environment. These methods included encrypting data both in transit and at rest using AES-256, ensuring end-to-end encryption via SSL/TLS, and leveraging Public Key Infrastructure (PKI) to authenticate devices and prevent unauthorized network access. Blockchain technology was also explored to secure and track transactions, while multi-factor authentication (MFA) and network segmentation were introduced to enhance security across the IoT network. As a result, Target invested over $100 million in upgrading its security systems, adopting a Zero Trust model that emphasized encryption, authentication, and continuous monitoring to prevent future breaches.

ChatGPT

In healthcare, the protection of sensitive data such as patient health records is critical, especially in the context of IoT devices like wearable sensors and medical monitoring systems.

This case study demonstrates the use of Advanced Encryption Standard (AES) for securing communication between IoT devices and central healthcare servers. The study evaluated the performance of AES encryption on lightweight IoT devices, focusing on achieving a balance between security and the limited computational resources of such devices. By implementing AES with a 128-bit key, the research successfully secured data transmission while keeping the computational overhead low, making it feasible for real-time health monitoring applications.

The research also explored the use of Blockchain technology to enhance data integrity and security in H-IoT networks. Blockchain, acting as a decentralized ledger, was used to verify and securely store IoT data, preventing tampering and unauthorized access. This approach not only enhanced security but also provided a transparent mechanism for tracking and auditing sensitive healthcare data.

This case study illustrates the real-world application of cryptographic methods in IoT networks, specifically within critical sectors like healthcare, offering valuable insights for your project on IoT data protection​(SpringerOpen)​(MDPI).

**Methodologies**

**Method 1(article) – Formal Verification**

Formal verification is a rigorous technique used to detect unexpected behaviors and security flaws in complex systems like IoT networks. Specifically, model checking is employed, which involves verifying where a system meets predefined security properties, such as resisting cyber-attacks like brute-force attempts.

Probabilistic behaviors can complicate security analysis in cryptographic schemes, such as encryption and watermarking in IoT networks. A model checker like PRISM is used to ensure robustness against privacy attacks. PRISM can evaluate whether the system’s probabilistic behavior satisfies security requirements.[3]

Formal Verification works by:

1. Model Definition: A system model is defined using continuous-time Markov chains (CTMCs), which capture the probabilistic states and transitions within the IoT network. Each device in the IoT network is modeled as an independent module, and the modules interact according to defined security protocols.
2. Logic Properties: Logic properties represent the desired security goals, such as ensuring that an attacker cannot capture encrypted data. The success of an attack is defined by specific conditions, like whether an attacker can remove watermarks from packets or decrypt messages.
3. Adversary Model: Non-parametric Adversary uses techniques like maximum likelihood to analyze captured data packets. The parametric adversary uses advanced statistical methods like ARMAX algorithms to extract information by attempting to guess encryption keys.
4. Attack Evaluations: The system’s resilience is tested under varying conditions. Including different attack durations and the number of captured packets. PRISM calculated the probability of a successful attack based on these conditions.

This method allows researchers to prove whether the cryptographic methods in place can prevent even advanced attackers from gaining access to sensitive data in an IoT network simulation. This is particularly important in environments where IoT devices may transmit critical data, such as healthcare or financial systems.

Using formal verification through model checking, researchers can validate that the system meets the highest security standards, ensuring data protection even against sophisticated privacy adversaries.[3] This method is beneficial for detecting flaws that might not be apparent through traditional testing approaches.

Table 3- 
Results From the Formal Verification Experiments

The results show a meager chance (0.05%) for a privacy adversary to break the system's security, even when capturing many packets. This applies to both types of adversaries due to strong encryption and watermarking. Parametric adversaries present a slightly higher risk, but the system remains highly resilient, with a nearly negligible risk of compromise, even under advanced attack scenarios.

ChatGPT

Formal verification is a mathematical approach used to verify that systems behave as intended and meet defined security properties. In a simulated IoT network, it ensures that cryptographic methods and security protocols are correctly implemented and free from vulnerabilities. The process involves creating a mathematical model of the system using tools like PRISM and defining security properties such as data confidentiality and integrity. Adversary models are then used to simulate potential attacks, and the system is tested against these scenarios to check for vulnerabilities.

In the context of an IoT network, formal verification can model each device and its interactions, ensuring that communication protocols like MQTT or CoAP securely transmit data and prevent unauthorized access. By simulating various attack scenarios, such as man-in-the-middle or replay attacks, formal verification provides a quantitative measure of the system's resilience.

This method is beneficial for detecting hidden flaws that might not be apparent through traditional testing. It allows for early identification and correction of security issues, improving system design and ensuring data protection. For your project, using formal verification can validate that the cryptographic methods implemented are robust enough to protect sensitive data in the IoT network, making it a critical tool for achieving high security standards.

**Method 2 (article) – Data Masking using steganography**

The research on hiding data started with steganography, the science and art of concealing information within an image. This method can be used to transmit classified messages without detection, making it difficult to find the hidden information.

The article discusses four processes: Data encryption uses encryption methods to secure messages, with encryption and decryption processes. It involves dividing the plaintext message, encrypting using AES and RSA methods, and sending the private key for added security.[4] The embedding process uses the Haar Discrete Wavelet Transform to break down the image and embed a secret message within it, using odd and even values in specific image coefficients. The extraction process aims to recover the hidden secret message and the original cover image after embedding using the 2D-DWT-2L technique. [4] Decryption is converting encrypted data back into a readable format by reversing the encryption process, using the same key used for encryption. This ensures that the encrypted data can be securely transformed into its original form using the correct keys.

**SSIM (Structural Similarity Index) Values:**

* + The SSIM values for all techniques (both 2D-DWT-1L and 2D-DWT-2L) and image types (color and gray-scale) are very close to 1. This indicates that the structural similarity between the original and stego images is almost perfect.
  + A value close to 1 means that the quality of the stego image is nearly identical to the original image, which is desirable for a steganographic model as it ensures the hidden message does not significantly distort the cover image.

**SC (Structural Content) Values:**

* + The SC values for all techniques and image types are exactly 1. This suggests that the overall content structure of the original and stego images is perfectly preserved.
  + High SC values (close to 1) imply that the image content remains unchanged, which is essential for maintaining the visual integrity of the image after embedding the hidden message.

**Correlation Values:**

* + The Correlation values are also 1 for all cases, indicating a perfect linear relationship between the original and stego images.
  + This means that the stego images are almost identical to the original images in terms of pixel intensity and distribution, which is a critical attribute for a robust steganographic method as it reduces the chance of detection.

**Summary:**

The results demonstrate that the proposed steganographic model using 2D-DWT-1L and 2D-DWT-2L techniques is highly effective in maintaining the structural and statistical properties of the original image while concealing the hidden message. Both techniques show negligible differences between the original and stego images, indicating high imperceptibility and robust security for the hidden data.

ChatGPT:

A graph with blue squares

Description automatically generated

**Method 3 (article) – Blockchain-based distributed access control system**

Blockchain is a unique data structure formed by combining data blocks in a chain of chronological order along with a protocol that guarantees its cryptographic properties like tamper-proof data. It is composed of a data layer, a network layer, a consensus layer, and an application layer. Blockchain technology utilizes an encrypted chain of blocks structure to verify and store data.[6]

The blockchain-based distributed access control system protects IoT data by using a combination of blockchain for secure data storage and chaotic encryption for data privacy. Key elements include:

1. **Decentralized Access Control**: IoT devices upload data to edge nodes, which serve as blockchain nodes. Access control policies are stored on the blockchain.
2. **Encryption**: The chaotic sequence and MLNCML series provide strong encryption for the data before uploading it to cloud storage.
3. **Tamper-Resistance**: Blockchain’s decentralized structure ensures data integrity, prevents unauthorized tampering, and provides secure, fine-grained access control.

These elements ensure privacy and security for sensitive data in simulated IoT networks.

Blockchain technology combined with access control to protect privacy can also be used to protect medical information, IoT, and cloud data.

The security analysis of the proposed blockchain-based system covers four key areas:

1. **File Storage Security**: Files are encrypted before upload, ensuring they can't be decrypted without the chaos code.
2. **Anti-Tampering**: Encryption and chaos coding prevent tampering without proper decryption keys.
3. **Theft Prevention**: Hash checks validate the authenticity of files, preventing unauthorized file replacements.
4. **Data Privacy**: Fine-grained access control via blockchain ensures only authorized users access encrypted files, enhancing privacy and data security.

Together, these measures ensure robust protection for IoT data.

ChatGPT

A screenshot of a computer

Description automatically generated

The results in Table 3 compare various systems based on security performance, focusing on dynamic access control, the number of nodes, voting weight setting, and payment requirements:

* **MDSM** has no dynamic access control, 121 nodes, and voting weight setting, but no payment.
* **BACC** and several other works (such as [40] and [41]) have many nodes but lack dynamic access control.
* **Our work** offers dynamic access control with fewer nodes (at least three), no voting weight setting, and no payment requirement, showcasing a lightweight, secure system.

**Method 4 (article) – ECC**

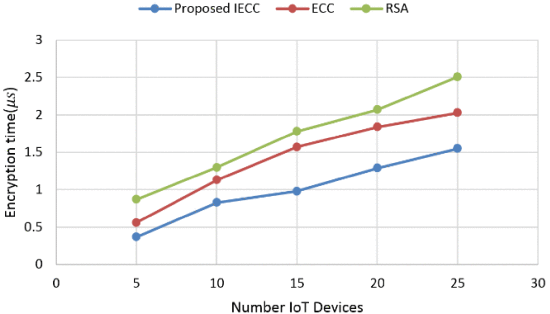
The Internet of Things (IoT) is a rapidly growing technology that is expected to have a wide range of applications in healthcare. The proposed method demonstrates how Elliptic Curve Cryptography (ECC) can protect sensitive data in a simulated IoT network by integrating authentication, encryption, and decryption mechanisms. Data from IoT sensor devices is initially encrypted using a Caesar cipher and then further encrypted by the ECC algorithm. ECC secures data using a combination of public, private, and secret keys, adding complexity to encryption and decryption, making it highly resistant to brute-force attacks.[7] This layered encryption ensures data privacy and security throughout the network. The proposed technique to protect sensitive data in a simulated IoT network uses a multi-layered encryption process combining a substitution Caesar cipher with Improved Elliptic Curve Cryptography (IECC).

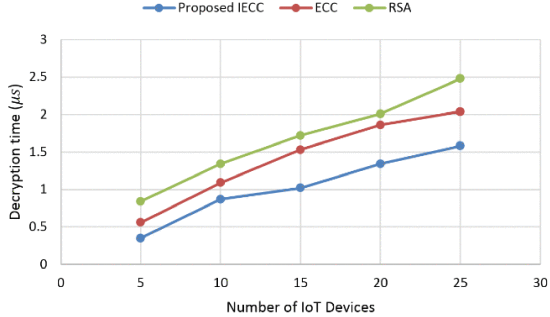
Authentication Phase: It starts with patient registration, using the SHA-512 algorithm to generate hash codes that verify user identity. This ensures that only authorized individuals can access the system. Data Encryption: After authentication, sensor data is encrypted using a simple Caesar cipher and passed through the IECC for enhanced security.[7] The IECC has improved over the regular ECC by introducing a secret key, in addition to public and private keys, making the encryption process more complex and secure. Key Generation: IECC generates three keys: a public key for encryption, a private key for decryption, and a secret key for additional complexity. The secret key is derived from elliptic curve points, adding a layer of mathematical difficulty that protects against brute force attacks. Secure Data Transmission: The encrypted data is transmitted to the cloud server and decrypted using the reverse ECC. The system ensures only authorized users can decrypt and access sensitive healthcare data.

ECC and the Caesar cipher combination secure data at multiple stages, ensuring confidentiality, integrity, and resilience against attacks in an IoT-based healthcare network. The simulation results highlight the improved performance of Elliptic Curve Cryptography (IECC) compared to traditional ECC and RSA in an IoT healthcare network. Key findings include Encryption/Decryption Time: IECC shows significantly faster encryption (0.35 μs) and decryption (1.55 μs) times for 25 IoT nodes, outperforming ECC and RSA. Correlation Coefficient: The IECC achieved a correlation coefficient of 0.045, indicating minimal statistical similarity between plaintext and ciphertext, which means more robust security against attacks. Computational Cost: IECC requires fewer hash computations and incurs lower message overhead than other algorithms, optimizing performance for IoT environments.

ChatGPT

Table 5- 
The Comparison of Encryption and Decryption Time (
$\mu s$
)





**Method 5- Testing Encryption Methods**

A key and an Initialization Vector (IV) were generated. The data was padded to fit the required block size, and encryption was performed using AES in CBC mode. This method encrypts sensitive data transmitted between IoT devices and the central server, ensuring confidentiality and integrity. In the case of DES encryption, a random 8-byte key and IV were generated, and data was padded to match DES's block size. The encryption was carried out using DES in CBC mode, primarily for backward compatibility with older IoT devices or systems that may still use this outdated encryption method. RSA encryption involves the generation of a 2048-bit RSA key pair (public and private keys). The public key was used to encrypt a message for secure data transmission, and the private key was used for decryption. RSA was utilized to securely exchange encryption keys between the central server and IoT devices before starting data communication using AES, ensuring a secure essential exchange process protected from eavesdropping or man-in-the-middle attacks. AES is used to encrypt data between IoT devices and the central server due to its high security and fast performance, making it ideal for real-time data protection. DES was demonstrated for comparison purposes, highlighting its inadequacies in securing modern IoT systems and its suitability only for backward compatibility. RSA was employed for secure key exchange, ensuring that the keys used for AES encryption are safely shared without interception, making it ideal for establishing secure communication channels.

**A screenshot of a computer program

Description automatically generated**

A graph of a number of encryption method

Description automatically generated

**Method 6- Simulating a Blockchain Network**

The blockchain simulation code showcases the fundamental principles of blockchain technology and its potential applications in your project. It consists of core components such as the Block class, which represents each block containing transactions, and the Blockchain class, which manages the chain of blocks and validates their integrity using cryptographic hashing and a Proof of Work (PoW) mechanism. The Transaction and Wallet classes simulate secure transaction handling through digital signatures, ensuring only authorized users can create valid transactions. This code is essential for demonstrating how blockchain can secure sensitive data, particularly in environments like IoT networks where data integrity and security are critical. The project highlights how blockchain can protect data against unauthorized modifications and improve trust in distributed systems by simulating a decentralized, tamper-proof ledger. Including consensus mechanisms, like PoW, adds a layer of security, making it difficult for malicious actors to alter the blockchain. This simulation is a prototype for integrating blockchain into real-world systems, showcasing its potential to enhance data security and operational efficiency in various applications.

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Method 7- Implementing IDS**

Implementing an Intrusion Detection System (IDS) like Snort is a highly effective approach for enhancing the protection of sensitive data in network environments, especially when used alongside cryptographic methods. While encryption and other cryptographic techniques ensure data confidentiality and integrity by making it unreadable to unauthorized users, they do not inherently provide real-time monitoring or alerts for suspicious activities. Snort addresses this gap by offering comprehensive network traffic analysis and threat detection, which is crucial for early identification and mitigation of security incidents.

Snort functions by monitoring both inbound and outbound network traffic, detecting known attack patterns such as brute-force attempts, SQL injections, and data exfiltration activities. It alerts administrators to potential threats, even when encrypted channels are used, and can be configured to respond to threats in real time by blocking malicious traffic or isolating compromised devices. This proactive approach is essential for preventing unauthorized access and data breaches.

Moreover, Snort's ability to integrate with other security tools and its cost-effectiveness as an open-source solution make it a versatile and powerful addition to any security strategy. By complementing cryptographic methods with Snort’s real-time monitoring and active response capabilities, organizations can achieve a robust, multi-layered defense system that ensures sensitive data remains secure from a wide range of threats.

**Method 8- Assessing Multifactor Authentication**

Google Authenticator is a tool that generates time-based one-time passwords (TOTPs) for multi-factor authentication (MFA), providing an additional layer of security for IoT networks. Focusing on securing sensitive data within an IoT network using cryptographic methods, implementing MFA, particularly with tools like Google Authenticator, ensures that even if an attacker gains access to a device or password, they would still need the dynamic TOTP to authenticate successfully. Each IoT device or user is registered with a secret key, used to generate TOTPs in conjunction with Google Authenticator. The TOTP changes every 30 seconds based on the current time and the secret key. By implementing MFA with Google Authenticator, each device or service in the IoT network can be protected against unauthorized access, reducing the risk of attacks.

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a phone

Description automatically generated**

**A qr code with black squares

Description automatically generated**

**Summary**

This project explores using cryptographic methods to secure sensitive data in a simulated IoT network, focusing on privacy, integrity, and confidentiality. The findings indicate that advanced cryptographic methods, like Elliptic Curve Cryptography (ECC) and blockchain technology, offer robust security for IoT networks, especially in critical sectors like healthcare. It is recommended to implement a multi-layered security approach in IoT networks, combining lightweight cryptographic methods such as ECC with blockchain technology for secure data storage and access control. These findings support the development of secure IoT solutions across various industries, contributing to the broader goal of protecting critical information in an increasingly interconnected world.

REFERENCES

[1] Author Unknown. (n.d.). **Cryptographic methods for sensitive data protection in a simulated IoT network**. IEEE. Retrieved from <https://ieeexplore.ieee.org/abstract/document/8675777>

[2] Internet Society. (2015). **The Internet of Things: An Overview**. Retrieved from [https://d1wqtxts1xzle7.cloudfront.net/48790442/ISOC-IoT-Overview-20151014\_0-libre.pdf](https://d1wqtxts1xzle7.cloudfront.net/48790442/ISOC-IoT-Overview-20151014_0-libre.pdf?1473746977=&response-content-disposition=inline%3B+filename%3DThe_Internet_of_Things_An_Overview_Under.pdf&Expires=1727327215&Signature=I1tv6-9aokbCbvbP5zuGL120VX6nz3X~oyhSESN4UQWlXoY5yWR6c-A8IqbSeStEM3splbY5dRObf5dhJd~TMX4MBgXPgLY5NkYIP99iEhqIDTzCrv49fcKbaKpUz5y-optTg3aphBeZ3RHAPJwZfTbZ0F0QyoMgZc1ews1cO1ECBShxzGphh4zXjPaEic036FDM9xVYYY2JbDoHGxpCnkFDGVWoTd0Kfdw1dbgDmKTRmF2rHuFm0yOzQI7~DpGye8dKUndRKou4wpN2klgytw3OCqLgwPF9wLrw8TyhRdRlWpfxUF1dWFbkvnRW6~wO8nzRDAIAyLHhCH6jNS9gsQ__)

[3] Author Unknown. (2023). **Security analysis of IoT systems using formal verification**. IEEE. Retrieved from [https://ieeexplore.ieee.org/abstract/document/9343245](https://ieeexplore.ieee.org/abstract/document/9343245/figures#figures)

[4] Author Unknown. (2018). **Data masking using steganography in IoT networks**. IEEE. Retrieved from <https://ieeexplore.ieee.org/abstract/document/8320774>

[5] Wang, G., Zhang, H., & Li, J. (2020). **Blockchain-based distributed access control for IoT data protection**. Journal of Supercomputing. Springer. Retrieved from <https://link.springer.com/article/10.1007/s10586-020-03190-3>

[6] Author Unknown. (2019). **Elliptic Curve Cryptography for secure IoT data transmission**. IEEE. Retrieved from <https://ieeexplore.ieee.org/abstract/document/9035402>

[7[ Author Unknown. (2023). **IoT case study and security analysis**. MDPI. Retrieved from <https://www.mdpi.com/2624-831X/5/1/2>