ENHANCING IOT DATA SECURITY WITH CRYPTOGRAPHY AND STEGANOGRAPHY

Cheruku Ramya
Scholar, Department of MCA
Vaageswari College Of Engineering-Karimnagar

P.Sathish
Assistant Professor, Department Of MCA
Vaageswari College Of Engineering-Karimnagar

Dr. V. Bapuji
Professor and Head, Department Of MCA
Vaageswari College Of Engineering-Karimnagar

ABSTRACT: In the realm of the Internet of Things (IoT), where data transfer occurs incessantly, ensuring the security of this data presents a formidable challenge. However, cryptography and steganography techniques offer promising avenues for mitigating these security challenges, particularly concerning user authentication and data privacy. This paper introduces and discusses the elliptic Galois cryptography (EGC) protocol, which employs cryptographic techniques to encrypt confidential data sourced from diverse medical channels. Subsequently, a Matrix XOR encoding steganography technique is employed to embed the encrypted data into a low-complexity image. Additionally, an optimization algorithm, Adaptive Firefly, is utilized to enhance the selection of cover blocks within the image. Through comprehensive evaluation and comparison of various parameters with existing techniques, the efficacy of the proposed approach is demonstrated. Finally, the concealed data within the image is recovered and decrypted, highlighting the practical applicability of the protocol.

Index Terms: Internet Of Things (Iot), Cryptography, Steganography, Elliptic Galois Cryptography (EGC), Matrix XOR Encoding, Adaptive Firefly Algorithm, Data Security.

1.INTRODUCTION

The Internet of Things (IoT) encompasses a network of interconnected vehicles, physical devices, software, and electronic items, facilitating seamless data exchange [1]. Its primary goal is to establish a robust IT infrastructure ensuring secure and reliable communication among various "Things" [2].

At the heart of IoT lie the integration of sensors/actuators, radio frequency identification (RFID) tags, and communication technologies, enabling diverse physical objects and devices to collaborate and communicate over the Internet towards common objectives. Despite the myriad benefits IoT devices offer in simplifying daily tasks, their security often remains overlooked. Presently, developers prioritize enhancing device capabilities, with scant attention to device security [3]. Consequently, data transmitted over IoT networks becomes vulnerable to attacks, posing risks to user privacy. Unsecured data transmission heightens the possibility of data breaches, thereby exposing personal information to potential hacking incidents. Vital concepts within IoT include identification and authentication, crucial for ensuring secure communication channels. Authentication ensures that information is transmitted to the correct device from a trusted source. Without proper authentication, hackers can exploit vulnerabilities to communicate with any device indiscriminately.

When data is exchanged between IoT devices, especially sensitive and personal data, encryption becomes imperative to safeguard its confidentiality. Cryptography serves as the primary means to encrypt data, converting plaintext into unintelligible ciphertext. The objectives of cryptography encompass ensuring confidentiality, integrity, non-repudiation, and authentication. One prominent cryptographic algorithm employed in IoT security is Elliptic Curve Cryptography (ECC), leveraging the algebraic structure of elliptic curves over finite fields. In addition to cryptographic techniques, steganography emerges as another method enhancing data security. Steganography conceals encrypted messages in a manner that makes their existence virtually undetectable. In modern digital steganography, data encryption precedes insertion into redundant data within a file format, such as a JPEG image [4]. The proposed approach integrates Matrix XOR steganography for added security, optimizing image blocks through the Adaptive Firefly algorithm to hide encrypted data within selected image blocks effectively.

1.1 PROBLEM STATEMENT

The exponential growth of the Internet of Things (IoT) has ushered in a new era of data transfer, yet it has also introduced formidable challenges in ensuring the security of transmitted data. Traditional security measures have proven inadequate to safeguard against the diverse and dynamic threats encountered in IoT ecosystems, leaving sensitive information vulnerable to breaches and unauthorized access. In sectors like healthcare, where the stakes for data privacy are particularly high, the need for robust security solutions is paramount. This research aims to tackle these challenges by proposing an innovative approach that combines elliptic Galois cryptography (EGC) with Matrix XOR encoding steganography and an Adaptive Firefly algorithm for optimization. By integrating these techniques, the objective is to develop a comprehensive solution that not only encrypts data effectively but also minimizes computational overhead and enhances efficiency in IoT networks. Through rigorous evaluation and practical experimentation, this

research seeks to demonstrate the efficacy of the proposed approach in safeguarding IoT data privacy and integrity, ultimately fostering trust and confidence in IoT deployments.

2.LITERATURE SURVEY

R. H. Weber describes the Internet of Things (IoT) as an emerging global Internet-based technical architecture that facilitates the exchange of goods and services in global supply chain networks, impacting the security and privacy of the stakeholders involved. Measures to ensure the architecture's resilience to attacks, data authentication, access control, and client privacy need to be established. An adequate legal framework must consider the underlying technology and would be best established by an international legislator, supplemented by the private sector according to specific needs, making it easily adjustable. The respective legislation must encompass the right to information, provisions prohibiting or restricting the use of IoT mechanisms, rules on IT security, provisions supporting the use of IoT mechanisms, and the establishment of a task force to research the legal challenges of IoT.

Ukil, J. Sen, and S. Koilakonda explain that the Internet of Things (IoT) consists of several tiny devices connected to form a collaborative computing environment. IoT imposes peculiar constraints in terms of connectivity, computational power, and energy budget, making it significantly different from those contemplated by the canonical doctrine of security in distributed systems. To address the problem of security in the IoT domain, networks and devices need to be secured. Their work focuses on embedded device security, assuming that network security is properly in place. They note that the existence of tiny computing devices in the IoT domain makes them vulnerable to various security attacks. The paper provides the requirements of embedded security, solutions to resist different attacks, and technology for resisting tampering of embedded devices using the concept of trusted computing. It attempts to address the issue of security for data at rest, equivalent to addressing the security issue of the hardware platform, and partially helps in securing data in transit.

U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan propose that in the fast-growing world of the Internet of Things (IoT), security has become a major concern. Datagram Transport Layer Security (DTLS) is considered one of the most suited protocols for securing the IoT. However, computation and communication overheads make it very expensive to implement DTLS on resource-constrained IoT sensor nodes. Their work profiles the energy costs of DTLS 1.3 using experimental models for cryptographic computations and radio-frequency (RF) communications. Based on this analysis, they present eeDTLS, a low-energy variant of DTLS that provides the same security strength but with lower energy requirements. By employing a combination of packet size reduction and optimized handshake computations, eeDTLS can provide up to 45% energy savings in a typical IoT use case. eeDTLS can be implemented in conjunction with any low-energy IoT RF protocol, and the proposed energy models and protocol optimizations can also improve the energy efficiency of custom IoT security architectures.

S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt state that the Internet of Things (IoT) enables a wide range of application scenarios with potentially critical actuating and sensing tasks, such as in the e-health domain. For communication at the application layer, resource-constrained devices are expected to use the constrained application protocol (CoAP), currently being standardized at the Internet Engineering Task Force. To protect the transmission of sensitive information, secure CoAP mandates the use of Datagram Transport Layer Security (DTLS) as the underlying security protocol for authenticated and confidential communication. DTLS, however, was originally designed for more powerful devices interconnected via reliable, high-bandwidth links. In their paper, they present Lithe, an integration of DTLS and CoAP for the IoT. Lithe includes a novel DTLS header compression scheme that aims to significantly reduce energy consumption by leveraging the 6LoWPAN standard. This scheme does not compromise the end-to-end security properties provided by DTLS and considerably reduces the number of transmitted bytes while maintaining DTLS standard compliance. Their evaluation shows significant gains in packet size, energy consumption, processing time, and network-wide response times when compressed DTLS is enabled.

Y. Yang, X. Liu, and R. H. Deng propose that the healthcare Internet-of-Things (IoT) is a promising means to greatly improve the efficiency and quality of patient care. Medical devices in healthcare IoT measure patients' vital signs and aggregate these data into medical files, which are uploaded to the cloud for storage and accessed by healthcare workers. To protect patients' privacy, encryption is normally used to enforce access control of medical files by authorized parties while preventing unauthorized access. In healthcare, it is crucial to enable timely access to patient files in emergency situations. They propose a lightweight break-glass access control (LiBAC) system that supports two ways for accessing encrypted medical files: attribute-based access and break-glass access. In normal situations, a medical worker with an attribute set satisfying the access policy of a medical file can decrypt and access the data. In emergent situations, the break-glass access mechanism bypasses the access policy to allow timely access to the data by emergency medical care or rescue workers. LiBAC is lightweight since very few calculations are executed by devices in the healthcare IoT network, and the storage and transmission overheads are low. LiBAC is formally proved secure in the standard model and extensive experiments demonstrate its efficiency.

3.EXISTING SYSTEM

Daniels et al. introduced Security Microvisor (SμV) middleware, which utilizes software virtualization and assembly-level code verification to provide memory isolation and custom security. Banerjee et al. [presented energy-efficient Datagram Transport Layer Security (eeDTLS), a low-energy variant of Datagram Transport Layer Security (DTLS) that offers the same security strength but with a lower energy requirement. Manogaran et al. proposed a system where medical sensor devices are embedded in the human body to collect clinical measurements of patients. Significant changes in respiratory rate, blood pressure, heart rate, blood sugar, and body

temperature that exceed standard levels are detected by the sensors, which generate an alert message containing relevant health information that is sent to the doctor via a wireless network. This system employs a vital management security mechanism to protect large amounts of data in the industry.

Sun et al. proposed CloudEyes, a cloud-based anti-malware system that provides efficient and trusted security services to devices in the IoT network. Ukil et al. studied the requirements of embedded security, offering methods and solutions for resisting cyber-attacks, and provided technology for tamper-proofing embedded devices based on the concept of trusted computing.

Yang et al. proposed the Lightweight Break-Glass Access Control (LiBAC) system, where medical files can be encrypted in two ways: 1) attribute-based access and 2) break-glass access. In standard situations, a medical worker can decrypt and access data if the attribute set satisfies the access policy of a medical file. In an emergency, a break-glass access mechanism bypasses the access policy of the medical file, allowing emergency medical care workers or rescue workers to access the data in a timely manner.

3.1DRAWBACKS

No effective secret key is used for data hiding.

Less secure cryptographic techniques have been employed.

4.PROPOSED SYSTEM

The proposed system introduces the Elliptic Galois Cryptography (EGC) protocol to protect against data infiltration during transmission over the IoT network. In this system, different devices in the IoT network transmit data through the EGC protocol as part of a controller. The encryption algorithm within the controller encrypts the data using the EGC protocol, and the encrypted, secured message is then hidden within layers of an image using the steganography technique.

The image can be easily transferred over the Internet such that an intruder cannot extract the hidden message. Initially, the EGC technique encrypts the confidential data. Subsequently, the encoded secret message is embedded within the image using the XOR steganography technique. Next, an optimization algorithm called the Adaptive...

Elliptic Galois Cryptography (EGC) is an enhancement of Elliptic Curve Cryptography (ECC), a public key encryption technique based on elliptic curve theory. Keys are generated using the properties of elliptic curve equations rather than traditional methods. The proposed work uses EGC to improve the efficiency of calculations and reduce the complexities of rounding errors by employing elliptic curves over the Galois field (F_a). The value of the Galois field must be greater than one.

4.1ADVANTAGES

The attractiveness between fireflies is proportional to their brightness; thus, a less bright firefly will move toward a brighter one. As the distance between fireflies increases, both attractiveness and brightness decrease.

The brightness of a firefly is determined by the landscape of the objective function. Two important issues persist in the Firefly

algorithm: a) the formulation of attractiveness and b) the variation of light intensity.

5.SYSTEM ARCHITECTURE

The system architecture revolves around an IoT router serving as the linchpin, orchestrating secure data exchange between sender and receiver components. The sender initiates the process by selecting an image, encrypting it with a secret key, and embedding a message within using both Cryptography and Steganography techniques. On the receiving end, the recipient decrypts the image, extracts the hidden message using the provided key, and saves the information securely. Throughout this process, the IoT router ensures efficient data routing, implements security protocols, and manages connectivity between components. It acts as the guardian of data transmission, safeguarding sensitive information while optimizing communication paths for seamless exchange. By leveraging cryptographic and steganographic methods, the system ensures not only confidentiality but also the covert transmission of data, enhancing overall security and reliability in IoT-based communication scenarios.

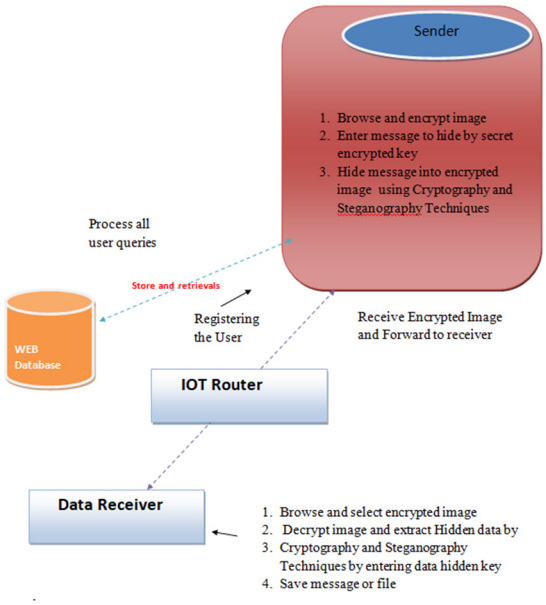


Figure 1. System Architecture

6.IMPEMENTATION

MODULES

The major modules of the project are:

Sender:

In this module, the sender must log in with a valid username and password. After successfully logging in, the sender can perform various operations such as:

Browsing and encrypting an image.
Entering a message to hide using a secret encrypted key.
Hiding the message in the encrypted image using cryptography and steganography techniques.

Receiver:

In this module, there are multiple users who can perform operations such as:

Browsing and selecting an encrypted image.

Decrypting the image and extracting the hidden data using cryptography and steganography techniques by entering the data hidden key.

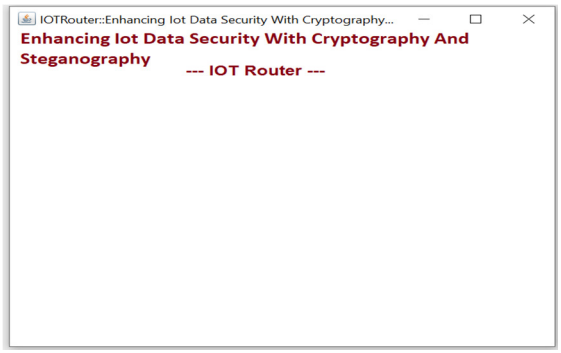
Saving the message or file.

IoT Router:

The IoT Router acts as middleware between the sender and receiver, receiving and rerouting the encrypted image to the appropriate receiver.

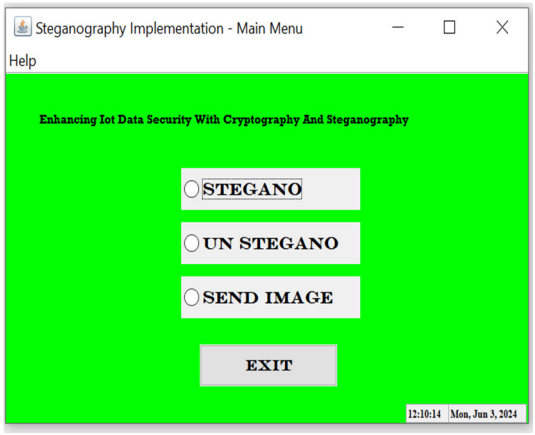
7.RESULTS

IOT Router:

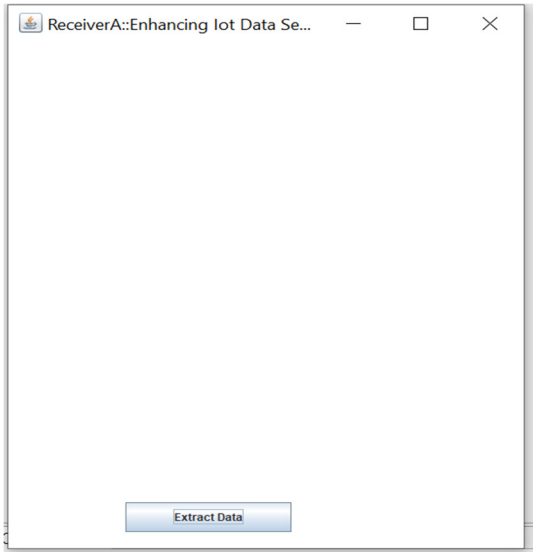


Sender Login:

Home Page:



Receiver Page:



8.CONCLUSION

The EGC protocol, leveraging ECC over Galois field, represents a significant advancement in data security for IoT transmissions. By enhancing embedding efficiency, it enables greater data hiding capacity, crucial for safeguarding information across IoT networks. Through integration with Adaptive Firefly optimization, the protocol ensures secure

transmission of large volumes of data concealed within image layers. Evaluation metrics including embedding efficiency, PSNR, carrier capacity, time complexity, and MSE highlight the protocol's superior performance. Implementation in MATLAB yielded an impressive 86% steganography embedding efficiency. Comparative analysis against established methods like OMME, FMO, and LSB underscores the superiority of the proposed protocol. In summary, the EGC protocol emerges as a formidable solution for fortifying data security in IoT environments, offering both efficiency and efficacy.

9.FUTURE ENHANCEMENT

The future scope for the EGC protocol involves enhancing security features and optimizing performance metrics. Integration with emerging technologies like blockchain and edge computing holds promise for improving data integrity and efficiency. Real-world implementations and standardization efforts are crucial for validating and fostering widespread adoption. Addressing privacy concerns will be imperative for maintaining trust and confidence in IoT ecosystems.

10.REFERENCES

1. R. H. Weber, “Internet of Things—New security and privacy challenges,” Comput. Law Security Rev., vol. 26, no. 1, pp. 23–30, 2010.
2. Ukil, J. Sen, and S. Koilakonda, “Embedded security for Internet of Things,” in Proc. 2nd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS), Mar. 2011, pp. 1–6.
3. W. Daniels et al., “SμV-the security microvisor: A virtualisation-based security middleware for the Internet of Things,” in Proc. ACM 18th ACM/IFIP/USENIX Middleware Conf. Ind. Track, Dec. 2017, pp. 36–42.
4. U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, “eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things,” in Proc. GLOBECOM IEEE Glob. Commun. Conf., Dec. 2017, pp. 1–6.
5. Boddupalli Anvesh Kumar, Dr.V.Bapuji ,”Efficient Privacy Preserving Communication Protocol For IoT Applications” ,The Brazilian Journal of Development ISSN 2525-8761, published by Brazilian Journals and Publishing LTDA.(CNP)32.432.868/000157)Vol.No.10,Pages:402-419 January 2024. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/66113
6. G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, “Big data security intelligence for healthcare industry 4.0,” in Cybersecurity for Industry 4.0. Cham, Switzerland: Springer, 2017, pp. 103–126.
7. H. Sun, X. Wang, R. Buyya, and J. Su, “CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices,” Softw. Pract. Exp., vol. 47, no. 3, pp. 421–441, 2017.
8. Sathish Polu and Dr. V. Bapuji, “Distributed Denial of Service (DDOS) Attack Detection in Cloud Environments Using Machine Learning Algorithms”, International Journal of Innovative Research in Technology, (IJIRT), Volume 9, Issue7, ISSN:2349-6002.December 2022, (UGC CARE LIST – I).

https://scholar.google.co.in/citations?view_op=view_citation&hl=en&user=6hPSwVgAAAAJ&citation_for_view=6hPSwVgAAAAJ:hqOjcs7Dif8C

9. N. Chervyakov et al., “AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security,” Future Gener. Comput. Syst., vol. 92, pp. 1080–1092, Mar. 2019.
10. S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe:
storage systems for Internet of Things to ensure security,” Future Gener. Comput. Syst., vol. 92, pp. 1080–1092, Mar. 2019.
11. S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe: Lightweight secure CoAP for the Internet of Things,” IEEE Sensors J., vol. 1, no. 10, pp. 3711–3720, Oct. 2013.
12. M. Vucini ˇ c´ et alzz., “OSCAR: Object security architecture for the Internet of Things,” Ad Hoc Netw., vol. 32, pp. 3–16, Sep. 2015.
13. Y. Yang, X. Liu, and R. H. Deng, “Lightweight break-glass access control system for healthcare Internet-of-Things,” IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3610–3617, Aug. 2017.