SECURING DATA IN INTERNET OF THINGS (IOT) USING CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

[1]K.Ramya,[2]Dr. D. Srinivas Reddy
[1]Mtech, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, H.no: 20S41D5809, ramyareddykuthuru1@gmail.com
[2]Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, srinivasreddydhava@gmail.com

ABSTRACT: Internet of Things (IoT) is a domain wherein which the transfer of data is taking place every single second. The security of these data is a challenging task; however, security challenges can be mitigated with cryptography and steganography techniques. These techniques are crucial when dealing with user authentication and data privacy. In the proposed work, the elliptic Galois cryptography protocol is introduced and discussed. In this protocol, a cryptography technique is used to encrypt confidential data that came from different medical sources. Next, a Matrix XOR encoding steganography technique is used to embed the encrypted data into a low complexity image. The proposed work also uses an optimization algorithm called Adaptive Firefly to optimize the selection of cover blocks within the image. Based on the results, various parameters are evaluated and compared with the existing techniques. Finally, the data that is hidden in the image is recovered and is then decrypted.

Keywords *– Confidential data, cryptography, data security, Internet of Things (IoT), steganography, user authentication.*

1. INTRODUCTION

The internet of Things (IoT) is a network of connected vehicles, physical devices, software, and electronic items that facilitate data exchange. The purpose of IoT is to provide the IT-infrastructure for the secure and reliable exchange of "Things" [1]. The foundation of IoT mainly consists of the integration of sensors/actuators, radio frequency identification (RFID) tags, and communication technologies. The IoT explains how a variety of physical items and devices can be integrated with the Internet to permit those objects to cooperate and communicate with each other to reach common goals. The IoT consists mostly of little materials that are associated together to facilitate collaborative calculating situations. Constraints of the IoT include energy budget, connectivity, and computational power [2]. Although IoT devices have made life easier, little attention has been given to the security of these devices. Currently, the focus of developers is to increase the capabilities of these devices, with little emphasis on the security of the devices. The data that is transferred over the IoT network is vulnerable to attack. This data is needed to be secured to protect the privacy of the user. If there is no data security, then there is a possibility of data breach and thus, personal information can be easily hacked from the system.

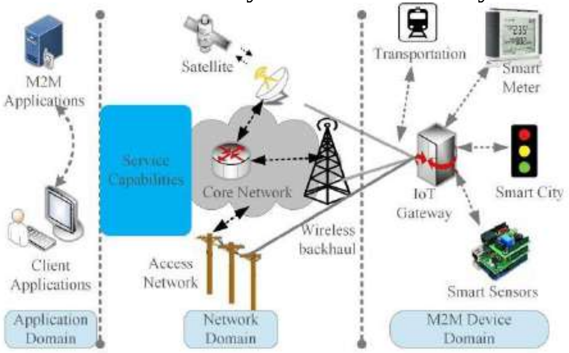


Fig.1: Example figure

Some of the important concepts of IoT involve identification and authentication. These concepts are inter-related to each other as cryptographic functions that are necessary to ensure that the information is communicated to the correct device and if the source is trusted or not. With the lack of authentication, a hacker can easily communicate to any device. Whenever two devices communicate with each other, there is a transfer of data between them. The data can also be very sensitive and personal. Therefore, when this sensitive data is moving from device to device over the IoT network, then there is a need for encryption of the data. Encryption also helps to protect data from intruders. The data can be easily encrypted with the help of cryptography, which is the process of converting simple text into unintelligible text. The primary objectives of cryptography are confidentiality, integrity, nonrepudiation, and authentication. Elliptic curve cryptography (ECC) is one of the cryptographic algorithms that is used in the proposed work. ECC is a public key cryptographic technique based on the algebraic structure of elliptic curves over finite fields.

2. LITERATURE REVIEW

Internet of Things—New security and privacy challenges

The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, access control and client privacy need to be established. An adequate legal framework must take the underlying technology into account and would best be established by an international legislator, which is supplemented by the private sector according to specific needs and thereby becomes easily adjustable. The contents of the respective legislation must encompass the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

Embedded security for Internet of Things

Internet of Things (IoT) consists of several tiny devices connected together to form a collaborative computing environment. IoT imposes peculiar constraints in terms of connectivity, computational power and energy budget, which make it significantly different from those contemplated by the canonical doctrine of security in distributed systems. In order to circumvent the problem of security in IoT domain, networks and devices need to be secured. In this paper, we consider the embedded device security only, assuming that network security is properly in place. It can be noticed that the existence of tiny computing devices that form ubiquity in IoT domain are very much vulnerable to different security attacks. In this work, we provide the requirements of embedded security, the solutions to resists different attacks and the technology for resisting temper proofing of the embedded devices by the concept of trusted computing. Our paper attempts to address the issue of security for data at rest. Addressing this issue is equivalent to addressing the security issue of the hardware platform. Our work also partially helps in addressing securing data in transit

.

eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things

In the fast growing world of the Internet of Things (IoT), security has become a major concern. Datagram Transport Layer Security (DTLS) is considered to be 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. In this work, we profile the energy costs of DTLS 1.3, using experimental models for cryptographic computations and radio-frequency (RF) communications. Based on this analysis, we present eeDTLS, a low-energy variant of DTLS, that provides the same security strength as DTLS, but has 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 be used to improve the energy efficiency of custom IoT security architectures.

Lithe: Lightweight Secure CoAP for the Internet of Things

The Internet of Things (IoT) enables a wide range of application scenarios with potentially critical actuating and sensing tasks, e.g., in the e-health domain. For communication at the application layer, resource-constrained devices are expected to employ the constrained application protocol (CoAP) that is 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 comparably powerful devices that are interconnected via reliable, high-bandwidth links. In this paper, we present Lithe-an integration of DTLS and CoAP for the IoT. With Lithe, we additionally propose a novel DTLS header compression scheme that aims to significantly reduce the energy consumption by leveraging the 6LoWPAN standard. Most importantly, our proposed DTLS header compression scheme does not compromise the end-to-end security properties provided by DTLS. Simultaneously, it considerably reduces the number of transmitted bytes while maintaining DTLS standard compliance. We evaluate our approach based on a DTLS implementation for the Contiki operating system. Our evaluation results show significant gains in terms of packet size, energy consumption, processing time, and network-wide response times when compressed DTLS is enabled.

Lightweight break-glass access control system for healthcare Internet-of-Things

Healthcare Internet-of-things (IoT) has been proposed as 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 of patient files in emergency situations. In this paper, we 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 of the medical file 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 are conducted to demonstrate its efficiency.

3. METHODOLOGY

Daniels *et al.* [3] introduced security microvisor (SμV) middleware, which uses software virtualization and assembly level code verification to provide memory isolation and custom security. Banerjee *et al.* [4] presented energy-efficient datagram transport layer security (eeDTLS), which is a lowenergy variant of datagram transport layer security (DTLS) that had the same security strength but a lower energy requirement. Manogaran *et al.* [5] proposed a system in which 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, with the help of a wireless network. This system uses a vital management security mechanism to protect large amounts of data in the industry.

- ❖ Sun *et al.* [6] proposed CloudEyes, a cloud-based antimalware system. The proposed system provided efficient and trusted security services to the devices in the IoT network. Ukil *et al.* [2]

studied the requirements of embedded security, provided methods and solutions for resisting cyber-attacks, and provided technology for tamper proofing the embedded devices based on the concept of trusted computing.

- ❖ Yang *et al.* [10] proposed the lightweight break-glass access control (LiBAC) system in which 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 is used that can bypass the access policy of the medical file so that emergency medical care workers or rescue workers can access the data in a timely fashion.
- ❖

Disadvantages

- ➢ There is no effective secret key used for data hiding.
- ➢ Less security cryptographic techniques have been used.

The proposed system proposes the elliptic Galois cryptography (EGC) protocol for protection against data infiltration during transmission over the IoT network. In the proposed work, different devices in the IoT network transmit data through the proposed protocol as a part of the controller. The encrypted algorithm within the controller encrypts the data using the EGC protocol and then the encrypted and secured message is hidden in layers of the image, with help from the steganography technique.

- ❖ The image can then be easily transferred throughout the Internet such that an intruder cannot extract the message hidden inside the image. Initially, the EGC technique encrypts confidential data. Subsequently, the encoded secret message is inserted within the image by the XOR steganography **technique**. Next, an optimization algorithm called the Adaptive
- ❖ *Elliptic Galois Cryptography:* ECC, commonly known as the public key encryption technique, is based on elliptic curve theory. The keys are generated by using the properties of elliptic curve equations instead of traditional methods. The proposed work uses EGC. For improving the efficiency of calculations and to reduce the complexities of rounding errors, the elliptic curve over the Galois field (*Fa*) is used. The value of the Galois field must be greater than one.

Advantages:

- ❖ All the fireflies are unisex so that all fireflies are attracted to each other.
- ❖ Attractiveness between the fireflies is proportional to their brightness; thus, a less bright firefly will move toward a brighter one. With increased distance between fireflies, both the 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) formulation of the attractiveness and b) the variation of light intensity

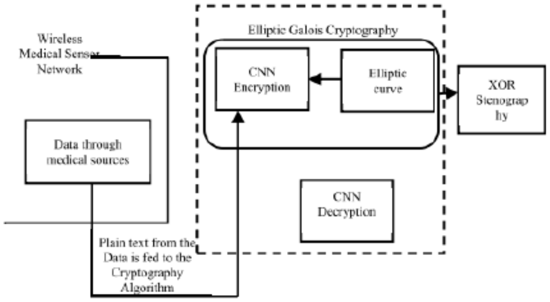


Fig.2: System architecture

Elliptic Galois Cryptography and Steganography Protocol This paper proposes the elliptic Galois cryptography (EGC) protocol for protection against data infiltration during transmission over the IoT network. In the proposed work, different devices in the IoT network transmit data through the proposed protocol as a part of the controller. The encrypted algorithm within the controller encrypts the data using the EGC protocol and then the encrypted and secured message is hidden in layers of the image, with help from the steganography technique. The image can then be easily transferred throughout the Internet such that an intruder cannot extract the message hidden inside the image. Initially, the EGC technique encrypts confidential data. Subsequently, the encoded secret message is inserted within the image by the XOR steganography technique. Next, an optimization algorithm called the Adaptive Firefly algorithm is used to select a block in the image.

4. IMPLEMENTATION

The major modules of the project are

Sender

In this module, Sender has to login with valid username and password. After login successful he can do some operations such as Browse and encrypt image, Enter message to hide by secret encrypted key, Hide message into encrypted image using Cryptography and Steganography Techniques

Receiver

In this module, there are n numbers of users are present and will do some operations like Browse and select encrypted image, Decrypt image and extract Hidden data by ,Cryptography and Steganography Techniques by entering data hidden key, save message or file

IOT Router

The IOT Router acts as a middleware between sender and receiver to receive and re route the encrypted image to an appropriate Receiver.

5. EXPERIMENTAL RESULTS

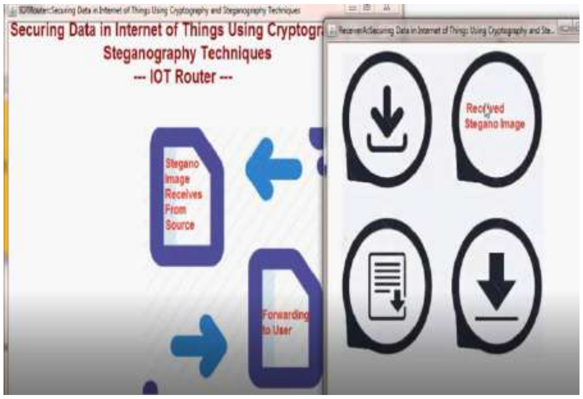

IOTRouter::Securing Data in Internet of Things Using Cryptography and Steganography Techniques
Securing Data in Internet of Things Using Cryptogr
Steganography Techniques
--- IOT Router ---
Stegano Image Receives From Source
Forwarding to User
Receiver::Securing Data in Internet of Things Using Cryptography and Ste...
Recived Stegano Image

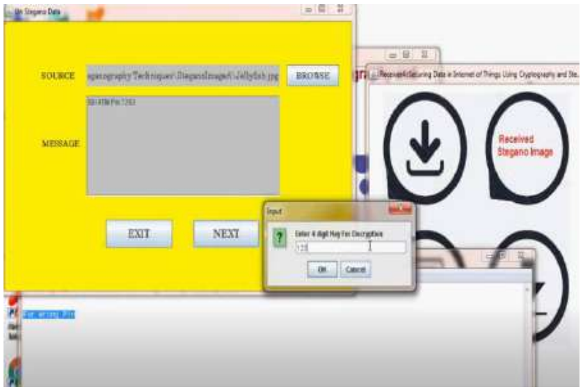
Fig.3: Home screen

Congestion Avoidance for Smart Devices by Caching Information in MANETS and IoT

Login Name Admin

Password ^^^^^

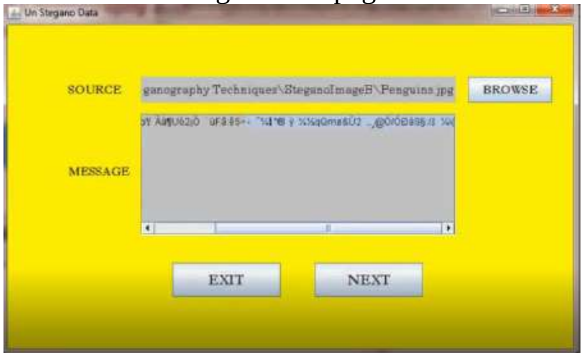
Fig.4: login



SOURCE: eganography Techniques\SteganoImageB\Jellyfish.jpg

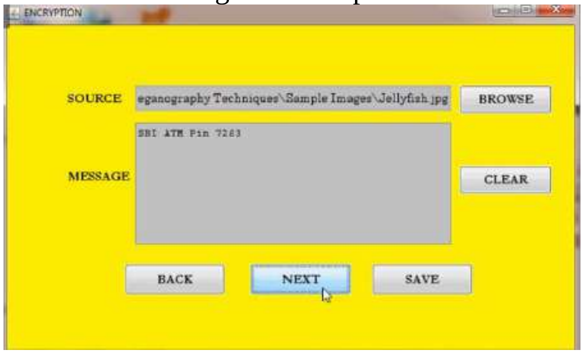
MESSAGE: SBI ATM Pin 7263

Fig.5: main page



SOURCE: ganography Techniques\SteganoImageB\Penguins.jpg

Fig.6: User input



SOURCE: eganography Techniques\Sample Images\Jellyfish.jpg

MESSAGE: SBI ATM Pin 7263

Fig.7: Prediction result

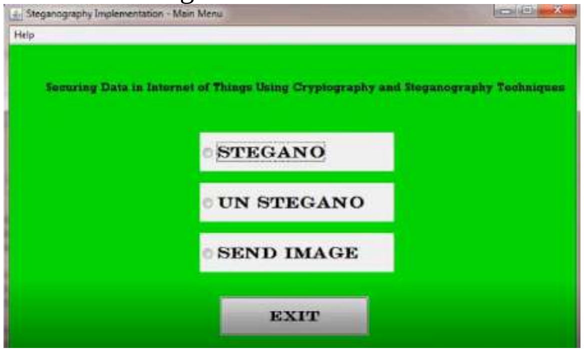

Steganography Implementation - Main Menu
Help
Securing Data in Internet of Things Using Cryptography and Steganography Techniques
○ STEGANO
○ UN STEGANO
○ SEND IMAGE
EXIT

Fig.8: Details screen

6. CONCLUSION

The EGC protocol generated high levels of data security to serve the purpose of protecting data during transmission in the IoT. With the novel ECC over Galois field, the proposed EGC protocol provided better security. Due to the enhanced embedding efficiency, advanced data hiding capacity can be achieved. With the help of the proposed protocol and Adaptive Firefly optimization, any amount of data can be easily transmitted over the IoT network securely hidden within the profound layers of images. Performance is evaluated with parameters, such as embedding efficiency, PSNR, carrier capacity, time complexity, and MSE. Finally, the proposed work is implemented in a MATLAB simulator, and approximately 86% steganography embedding efficiency was achieved. Results from this proposed protocol were compared to existing methods, such as OMME, FMO, and LSB.

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] A. 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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] M. Vucini ˇ c´ et al., “OSCAR: Object security architecture for the Internet of Things,” Ad Hoc Netw., vol. 32, pp. 3–16, Sep. 2015.

[10] 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.