Journal of Engineering Sciences

Vol 13, Issue 06, June/2022
ISSN NO:0377-9254

SECURING DATA IN IOT USING CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

Mr. K Praveen Kumar, Assistant Professor, Department of CSE, praveenkumar.cse@cmrtc.ac.in

N. Sai Vardhan Reddy, BTech, Department of CSE, sainagam7@gmail.com

Swetha Errabelli, BTech, Department of CSE, serrabelli3@gmail.com

Nese Yashwanth Sai Venkateshulu, BTech, Department of CSE, 177r1a05m3@cmrtc.ac.in

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].

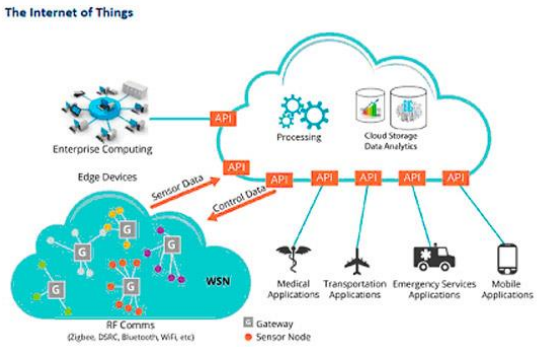

Fig.1: Example figure

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. 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.

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.

Big data security intelligence for healthcare industry 4.0

Nowadays, sensors are playing a vital role in almost all applications such as environmental monitoring, transport, smart city applications and healthcare applications and so on. Especially, wearable medical devices with sensors are essential for gathering of rich information indicative of our physical and mental health. These sensors are continuously generating enormous data often called as Big Data. It is difficult to process and analyze the Big Data for finding valuable information. Thus effective and secure architecture is needed for organizations to process the big data in integrated industry 4.0. These sensors are continuously generating enormous data. Hence, it is difficult to process and analyze the valuable information. This chapter proposes a secure Industrial Internet of Things (IoT) architecture to store and process scalable sensor data (big data) for health care applications. Proposed Meta Cloud-Redirection (MC-R) architecture with big data knowledge system is used to collect and store the sensor data (big data) generated from different sensor devices. In the proposed system, sensor medical devices are fixed with the human body to collect clinical measures of the patient. Whenever the respiratory rate, heart rate, blood pressure, body temperature and blood sugar exceed its normal value then the devices send an alert message with clinical value to the doctor using a wireless network. The proposed system uses key management security mechanism to protect big data in industry 4.0.

CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices:

Due to the rapid increasing of malware attacks on the Internet of Things in recent years, it is critical for resource-constrained devices to guard against potential risks. The traditional host-based security solution becomes puffy and inapplicable with the development of malware attacks. Moreover, it is hard for the cloud-based security solution to achieve both the high performance detection and the data privacy protection simultaneously. This paper proposes a cloud-based anti-malware system, called CloudEyes, which provides efficient and trusted security services for resource-constrained devices. For the cloud server, CloudEyes presents suspicious bucket cross-filtering, a novel signature detection mechanism based on the reversible sketch structure, which provides retrospective and accurate orientations of malicious signature fragments. For the client, CloudEyes implements a lightweight scanning agent

which utilizes the digest of signature fragments to dramatically reduce the range of accurate matching. Furthermore, by transmitting sketch coordinates and the modular hashing, CloudEyes guarantees both the data privacy and low-cost communications. Finally, we evaluate the performance of CloudEyes by utilizing both the campus suspicious traffic and normal files. The results demonstrate that the mechanisms in CloudEyes are effective and practical, and our system can outperform other existing systems with less time and communication consumption.

AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security

Benefits of Internet of Things and cloud–fog-edge computing are associated with the risks of confidentiality, integrity, and availability related with the loss of information, denial of access for a long time, information leakage, conspiracy and technical failures. In this article, we propose a configurable, reliable, and confidential distributed data storage scheme with the ability to process encrypted data and control results of computations. Our system utilizes Redundant Residue Number System (RRNS) with new method of error correction codes and secret sharing schemes. We introduce the concept of an approximate value of a rank of a number (AR), which allows us to reduce the computational complexity of the decoding from RNS to binary representation, and size of the coefficients. Based on the properties of the approximate value and arithmetic properties of RNS, we introduce AR-RRNS method for error detection, correction, and controlling computational results. We provide a theoretical basis to configure probability of information loss, data redundancy, speed of encoding and decoding to cope with different objective preferences, workloads, and storage properties. Theoretical analysis shows that by appropriate selection of RRNS parameters, the proposed scheme allows not only increasing safety, reliability, and reducing an overhead of data storage, but also processing of encrypted data.

3. IMPLEMENTATION

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.

In addition, to the cryptographic techniques, another method, named steganography is used in the proposed work which helps to provide additional security to the data. Steganography hides encrypted messages in such a way that no one would even suspect that an encrypted message even exists in the first place. In modern digital steganography, encryption of data occurs using typical cryptographic techniques. Next, a special algorithm helps to insert the data into redundant data that is part of a file format, such as a JPEG image. The proposed work uses Matrix XOR steganography to provide

additional security. The image block is optimized with the help of Adaptive Firefly algorithm in which the encrypted data is hidden in a selected block from a huge image block.

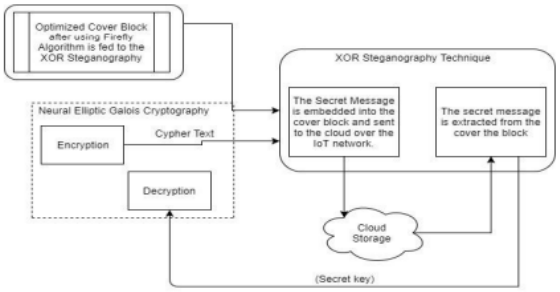

Fig.2: System architecture

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 intheIOTnetworktransmitdatathroughtheproposedprotocolasapartofthe 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 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 fire flies is proportional to their brightness; thus, a less bright fireflywillmovetowardabrighterone.Withincreaseddistancebetweenfireflies, 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.

4. METHDODOLOGY

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.

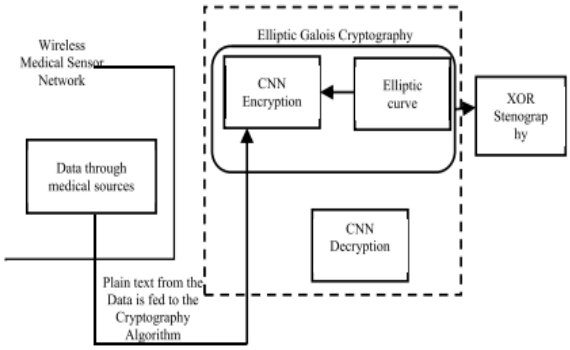

Fig.3: EGC

4.1.1. Elliptic Galois Cryptography: EGC, 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 thanone.

4.1.2. Matrix XOR: Matrix XOR is a technique for hiding encrypted data in which the encrypted data is hidden inside the H.264 video file .For this technique, the Firefly optimization technique is used to optimize the blocks of the image. With the help of this optimization technique, block selection among the whole image is possible.

4.1.3. OM-XOR Steganography Technique: The initial image is tiled and the secretdata is hidden on the cover block with the help of Adaptive Firefly optimization. The tiled image is recombined and decoded. Finally, the encrypted message is decoded byusing the secret key.

5. EXPERIMENTAL RESULTS

Fig.4: Output

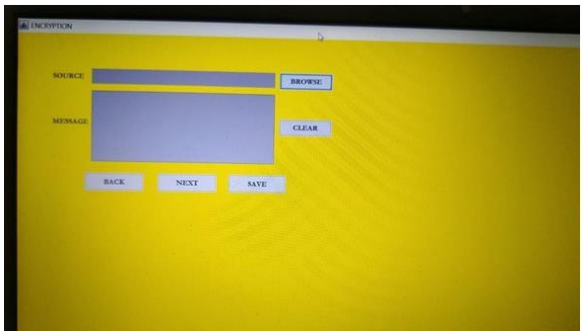

Fig.5: Output

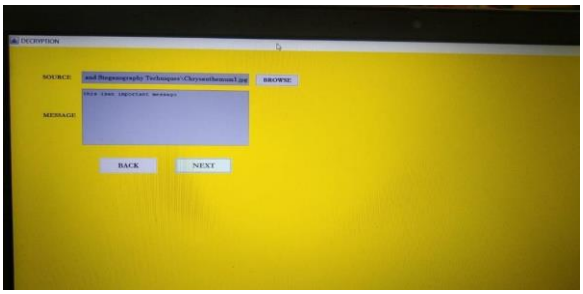

Fig.6: Output

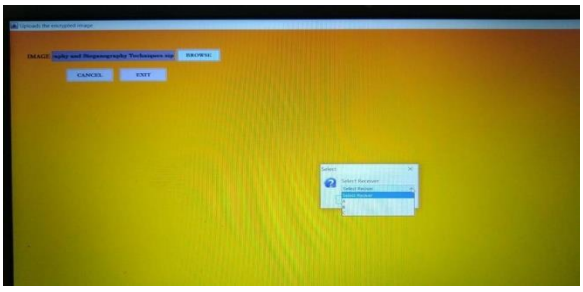

Fig.7: Output

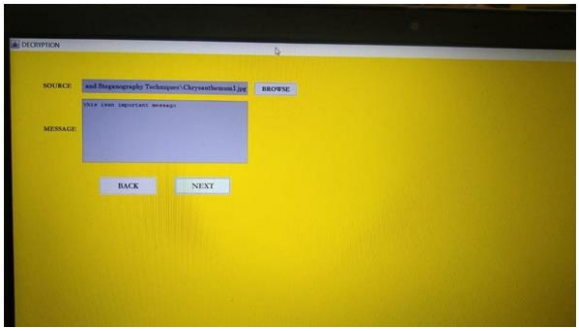

Fig.8: Output

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.