IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A COMMON METHOD OF SHARING AUTHENTICATION IN IMAGE SECRET SHARING

Mr.Bhanu Prasad Gorantla[1], A.yogitha[2], A Shruthi[3], ch.sindhuta[4], ch.soumya [5]

[2,3,4,5] UG Scholars, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, India.

[1]Assistant Professor, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, India.

ABSTRACT:

Secure Computing 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

.

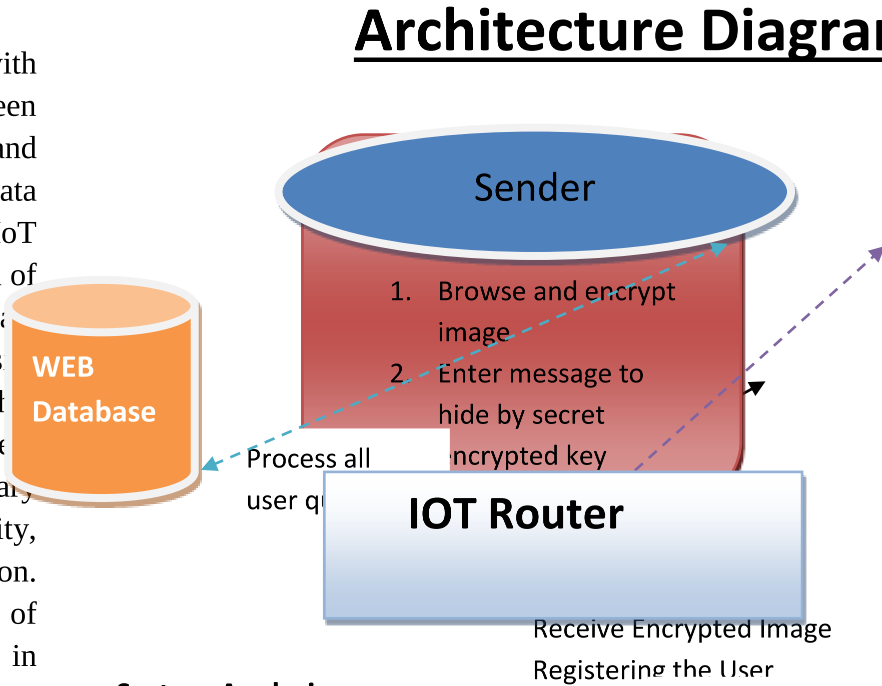
INTRODUCTION

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. 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 da from intruders. The data can be eas encrypted with the help of cryptograph which is the process of converting simple te 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



System Analysis

EXISTING SYSTEM:

- Daniels *et al.* [3] introduced secu microvisor (SμV) middleware, wh uses software virtualization assembly level code verification 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.

PROPOSED SYSTEM:

- ❖ 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 image based 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 Image Encryption 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 Image Encryption. 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

Implementation

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.

CONCLUSIONS

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. Vuˇcini´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.

[11] A. K. Bairagi, R. Khondoker, and R. Islam, “An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures,” *Inf. Security J. Glob. Perspective*, vol. 25, nos. 4–6, pp. 197–212, 2016.

[12] C.-T. Huang, M.-Y. Tsai, L.-C. Lin, W.-J. Wang, and S.-J. Wang, “VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements,” *J. Supercomput.*, vol. 74, no. 9, pp. 4295–4314, 2018.

[13] T. Shanableh, “Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 455–464, Apr. 2012.

[14] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, “Medical JPEG image steganography based on preserving inter-block dependencies,”

Comput. Elect. Eng., vol. 67, pp. 320–329, Apr. 2018.

[15] C. J. Benvenuto, *Galois Field in Cryptography*, Univ. Washington, Seattle, WA, USA, 2012.

[16] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[17] A. H. Gandomi, X. S. Yang, and A. H. Alavi, "Mixed variable structural optimization using firefly algorithm," *Comput. Struct.*, vol. 89, nos. 23–24, pp. 2325–2336, 2011.

[18] R. Hegde and S. Jagadeesha, "An optimal modified matrix encoding technique for secret writing in MPEG video using ECC," *Comput. Stand. Interfaces*, vol. 48, pp. 173–182, Nov. 2016.