Securing Data in IOT (Internet of Things) using Cryptography and Steganography Techniques

P. Sai Sruthi, P. Samhitha Reddy, P. Hameed Ali, Ankush thakur
Department of Computer Science and Engineering, Hyderabad Institute of Technology and Management,
Gowdavelly,Hyderabad,Telangana.

I.ABSTRACT

Internet of Things (IoT) is a domain in which the transfer of data is taking place every single second. To monitor the things that are connected using IoT devices from anywhere in the world over the network initially involves identification and authentication. On compromising, the IoT security can lead to attackers gaining access to the network, resulting in data leakage. Hence there is a need of securing the data in IoT. So our project aims to provide a solution to protect the privacy of the user by using both cryptography and steganography techniques at the time of authentication.

II.INTRODUCTION

Technology is growing and IoT plays an important role such as optimizing devices and connecting to devices without human interaction through which we can connect to the internet as this usage is increasing the generation of data so this is also increasing rapidly, Generally speaking, massive data is called big data, which mainly consists of unstructured data.

The data security of these IoT devices is not guaranteed at all because the computing power of IoT devices is low and the power consumption is basically low. AES, DES algorithms cannot provide as much security for these data. Therefore, we propose a new algorithm that lays the foundation for easy communication and secure transfer of data. In IoT technology, security is essentially done using cryptography and steganography techniques Cryptography involves converting plaintext to ciphertext. Steganography hides data in another form, such as images, audio or video data, or mixed data. The data transmitted over the Internet through these IoT devices is very sensitive data. While this sensitive data is transmitted between devices in IoT devices, the data should be encrypted. Data can be turned into meaningless text using cryptography. The main motto of this cryptography is authentication and confidentiality.

The source image is provided as the source and encrypted using encryption techniques, and other steganography techniques are also incorporated to provide greater data security. IoT is mainly composed of many sensors and RFIDS and communication networks. IoT is nothing more than connections between low-power devices to communicate and connect with each other and transmit a certain amount of data. This IoT technology mainly consists of small devices used for various applications, and through these IoT technologies, people interact less and life becomes easier. Even with IoT devices, there are constraints such as low computing power, connectivity and budget issues.

While IoT has made life easier, there are also very serious data security concerns.Today, the main motto of developers is to improve the capabilities and skills of IoT devices in protecting data by making small further improvements.The data sent over the IoT network becomes the attacker's asset. These data must be backed up to ensure the safety of user data. If it has nothing to do with data security, there is no knowledge leakage, so users' sensitive information can be easily compromised by attackers.

Most IoT concepts involve authentication, confidentiality, and identification.

III.LITERATURESURVEY

Earlier, there was a system with secure micro-hypervisors for storage isolation as well as security purposes and custom security. A low variant of datagram transmission is also proposed, which provides security with low computational power. This is also the previously proposed system, a medical chip-like device implanted in the human body to update breathing and blood pressure above normal levels, and then a warning message to send to the doctor, which basically works with wireless networks. The system uses important security technology to store the vast amount of information in the industry. These are previously proposed systems used to set goals for our proposed system. and improve the efficiency of the system.

IV.PROPOSED SYSTEM

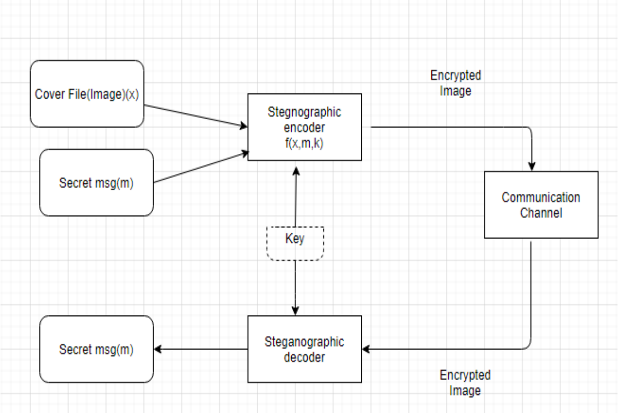
The proposed system proposes Elliptic Galois Cryptography(EGC) to encrypt the data, moreover, in our proposed system, the steganography technique is used to hide the data in the image, so the image is sent over the Interent where the information is hidden .Data hidden in image files cannot be found or tracked by intruders. The data or secret message is first encrypted by the EGC protocol, then the encrypted message is inserted into the image using XOR steganography, and then an optimization algorithm is added to create a more optimized steganography technology and cryptography to make data transmission in IoT devices more secure.

ADVANTAGES OF PROPOSED SYSTEM:

Fireflies are unisex, so they are attracted to each other. The attraction between the fireflies will increase, and then the brightness will also increase. The lower the brightness the firefly is attracted to, the brighter the firefly will become, increasing its brightness. Fireflies achieve their brightness through their gravitational pull.The two main issues in the firefly algorithm is:

a) The attractiveness of firefly and b) the intensity variation in the light.

IV.METHODOLOGY



Architecture:

Cover file image:

We are going to take a cover file (image){x} here to cover the msg(m) and apply steganography techniques to encrypt the message into image file using a user defined key(k).

Secret message (m):

The secret message is the message that we can to attach into the image using the steganographic encoder and concert onto a stegano image.

Steganographicencoder f (x, m, k):

Steganographic encoder is a function which is used to encrypt the message into the image here the steganographic encoder function will play a major role in doing the encryption of message into image. In this function we are using the cryptography technique to do encryption. It takes the input as the image file(x) and secret message and also a user defined key (k). It processes and gives the output as encrypted image.

Communication channel:

Here the communication channel is to send the encrypted image from the source to destination by taking the input as IP address of the sender. Here we are using the TCP to transfer the encrypted image to receiver.

Steganographic decoder:

Here the steganographic decoder is made to decrypt the encrypted image file. This steganographic decoder is also a function which is used to decrypt the secret message data from the image file by taking the user defined key as mentioned in the sender.

ALGORITHM:

In this we majorly have 3 modules

Sender

In this module, sender has to login with valid username and password. After login successfully 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 steganographic techniques.

Receiver

In this module, there are n number of users are present and 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.

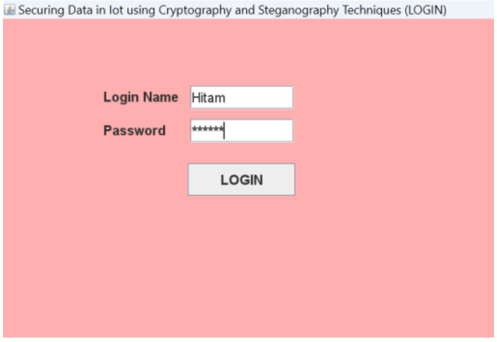
IOT Router

The IOT router acts as a middle ware between sender and receiver to receive and read encrypted image to an appropriate receiver.

- Firstly, login valid username and password then you will go to main menu page.
- After that click on the encrypt button and browse the source file that is jpg file and also enter the message in below box then click on the next button it will ask for 4 digit key for encryption give the user defined key and click on ok then take the image by clicking the image save button.
- The image will be encrypted and saved in the location as it mentioned.
- To send the encrypted image go to the main menu window and select the send image button and browse the encrypted file then select the receiver and click on ok then enter the IP address click on ok.

- You will find the image on IOT router window like forwarding your encrypted image
- In receiver you will get the encrypted image. To decrypt this encrypted image, go to the main menu window and select the decrypt button then browse your received encrypted file and also enter the encrypted key and click on ok.
- If you have entered correct encrypted key then you will get the secret message sender by the sender. If you have entered the wrong encrypted key then secret message will not be displayed.

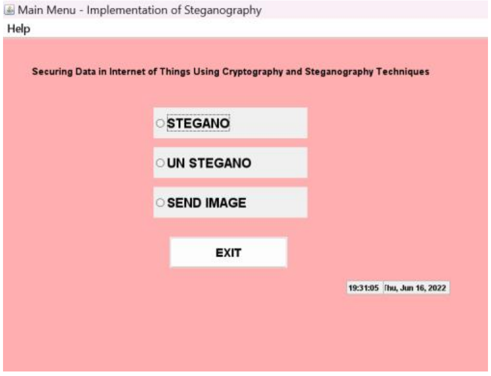
V.RESULTS


Securing Data in Iot using Cryptography and Steganography Techniques (LOGIN)

Login Name: Hitam
Password: ******

Fig-1 Login Page

The above image represents the Admin login page.


Main Menu - Implementation of Steganography

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

19:31:05 Thu, Jun 16, 2022

Fig-2 Main Menu Page

The above image represents the menu window for encryption and decryption and sending image.

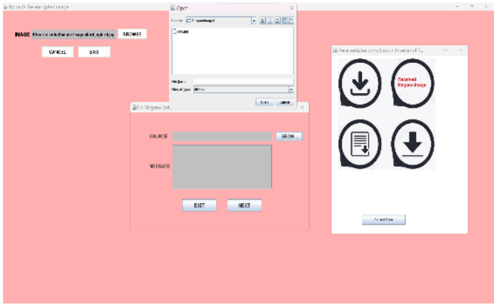
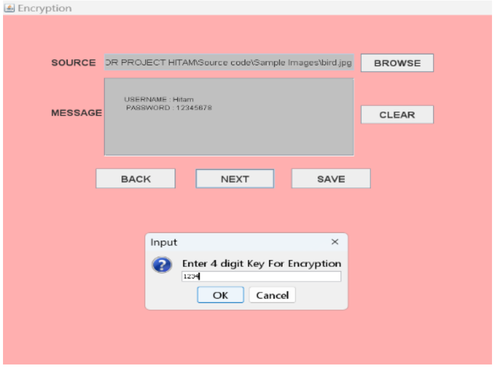


Fig-3 Steganoimage

The above image represents encryption window.


Encryption

SOURCE: DR PROJECT HITAM\Source code\Sample Images\bird.jpg

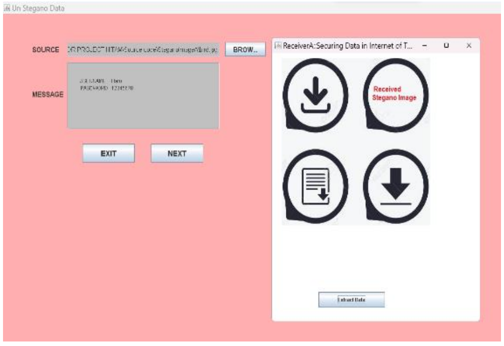
MESSAGE:
USERNAME : Hitam
PASSWORD : 12345678

Input

Enter 4 digit Key For Encryption: 1234

Fig-4 Encryption Key

The above image represents encryption key defined by user.


Un Stegano Data

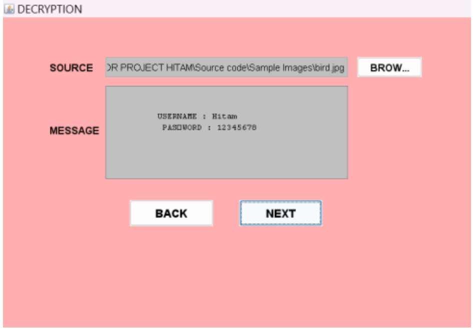
SOURCE: DR PROJECT HITAM\Source code\Stegano\image\bird.jpg

MESSAGE:
USERNAME : Hitam
PASSWORD : 12345678

ReceiverA:Securing Data in Internet of T...

Fig-5 UnStegano

The above image represents decryption of the Un Stegano image.

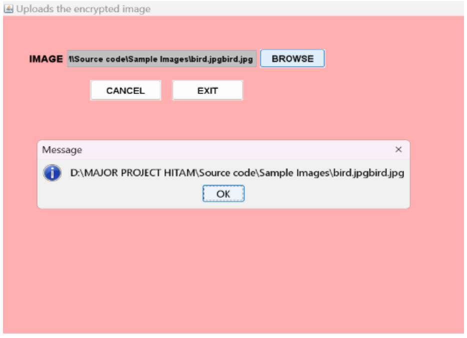

DECRYPTION

SOURCE: DR PROJECT HITAM\Source code\Sample Images\bird.jpg

MESSAGE:
USERNAME : Hitam
PASSWORD : 12345678

Fig-6 Decryption Key

The above image represents the key for decryption.



Uploads the encrypted image

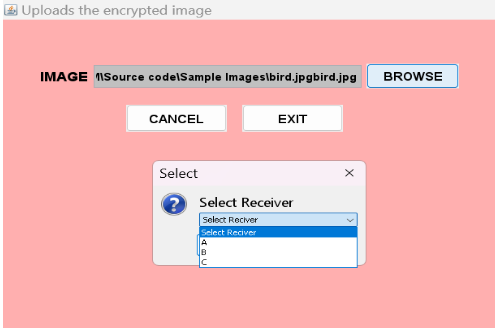
IMAGE 1\Source code\Sample Images\bird.jpgbird.jpg

Message

D:\MAJOR PROJECT HITAM\Source code\Sample Images\bird.jpgbird.jpg

Fig-7 Send Image

The above window represents the sending of encrypted image to Receiver.



Uploads the encrypted image

IMAGE 1\Source code\Sample Images\bird.jpgbird.jpg

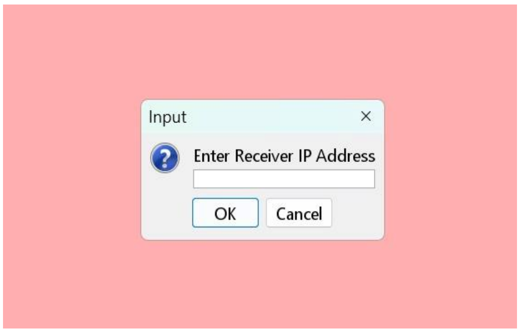
Select

Select Receiver

Select Reciver

Fig-8 Send To Receiver

The above image represents sending of encrypted image to particular receiver

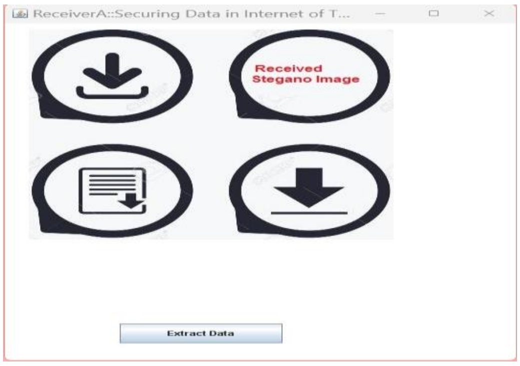


Input

Enter Receiver IP Address

Fig-9 Receiver IP Address

The above image represents the destination receive ip address.



ReceiverA::Securing Data in Internet of T...

Fig-10 Receiver

The above image represents the destination receiver where the stegano image will be sent.

VI .CONCLUSION

In our system the merging of two techniques cryptography and steganography made the message encrypted using cryptography and that message is made to hide inside image using steganography, thus the proposed system can be achieved the increase of efficiency securing the data over transmitting through the internet.

VII. REFERENCES

[1] R. Heber, “Internet of Things—New security and privacy challenges, “compute. Law Security Rev., vol. 26, no. 1, pp. 23–30, 2010.

[2] A. Ukil, J. Sen, and S. Koilakonda, “Embedded security for Internetof 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-basedsecurity middleware for the net of Things,” in Proc. ACM 18thACM/IFIP/USENIX Middleware Conf. Ind. Track, Dec. 2017, pp. 36–42

[4] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, “eeDTLS:Energyefficient datagram transport layer security for the web ofThings,” in Proc. GLOBECOM IEEE Glob. Commun. Conf., Dec. 2017,pp. 1–6

[5] G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, “Big datasecurity intelligence for healthcare industry 4.0,” in Cybersecurity forIndustry 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 a reversible sketch for resource-constrained IoT devices,” Softw. Pract. Exp., vol. 47, no. 3, pp. 421– 441,2017.

[7] N. Chervyakov et al., “AR-RRNS: Configurable reliable distributed datastorage systems for Internet of Things to make sure 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 to net of Things,” IEEE Sensors J.,vol. 1,no. 10, pp. 3711–3720, Oct. 2013

[9] M. Vucini´c et al., “OSCAR: Object security architecture for the IOTs,” Ad HocNetw., vol. 32, pp. 3–16, Sep. 2015.

[10] Y. Yang, X. Liu, and R. H. Deng, “Lightweight break-glass accesscontrol system for healthcare IOT,” IEEE Trans. Ind.Informat., vol. 14, no. 8, pp. 3610–3617, Aug. 2017