[1] **Ali Tariq Kalil Al-Khayyat ***

[2] **Osman Nuri Ucan**

[3] **Seyfi Yildiz**

A Simulation System Using the Internet of Things for Sevrity Sensing Services

Abstract: - IoT security has become very important in recent days because of the increase in applications and areas that can be used where the security of information is an important issue. In this work, a proposed system has been designed to secure communication between the client and the IoT device. The proposed system utilizes two strong security techniques, steganography and cryptography. The proposed system has taken advantage of these technologies where encryption protects the main authentication information as well as the IoT communication port and changes it to an unreadable form (Ciphertext), then embedding this Ciphertext within stego message to trick the observer there is any existing to the original message and prevent any suspension there is encryption in data. The overall test shows that this proposed method is very strong from a security point of view, and the operation test shows it works efficiently without any problem it fast takes about 2.5 seconds and is low in size which makes it useful even with low-speed internet. The main advantage is that no information can be obtained without passes successfully from all security strategies, which require first knowing if there is stego message, need to know which stego method is used, need to know which list is, need to know the encryption algorithm, the crypto key, and to have same mac that used in encryption. This is very hard and can say it is impossible to crack no one can connect an even know the IoT IP address without having the overall parts after that there is a need to right authentication information for IoT things.

Keywords: IOT, security, steganography, stego, cryptography, AES, HMAC.

I. INTRODUCTION

The Internet of Things usually which usually called (IoT) is a network of addressable, physical objects that includes embedded communication, actuating sensing, and technologies to sense and interact with their environment. IoT service can provide interconnection between 'Things' in various industrial fields, for example, home appliances, traffic, medical services, etc.). It can be classified by an interconnected set of private addresses and constrained (usually autonomous) devices in a distributed system, besides active/sensing units for physical phenomena, DAQ and applications via uses sensing, computation and actuation. Recently it has become possible there are billions of similar devices in the IoT cloud that are connected via the Internet with forecasts of 75.44 billion to 100 billion IoT devices may be connected to the Internet by 2025 [1].

This interconnected environment is subject to a variety of challenges that cause security problems concerning privacy and hacking attacks on IoT devices. Currently, it is estimated that 90% of the IoT units are subjected to security challenges, and, about 75% of the security experts have indicated that the security challenges of IoT are the most significant task. Additionally, IoT security could increase the critical issues that the IoT device and service is adopted almost anywhere in our real lives, and security issues can lead not only to data breach or monetary damages but also becoming a threat to our lives. At this point, IoT security requirements must be determined to help to make a secure and safe IoT environment. Many studies are likely to target on getting security concerns from a technological perspective [2].

This work has proposed a system that can achieve the security requirements to design a highly secure environment. The architecture presents the ability to combine two security techniques, steganography, and cryptography to achieve that purpose.

II. LITERATURE REVIEW

Srivastava, et al. (2015) [3], provide a review of IoT and discuss several security issues concerned with it. Aside from that, out of all security concerns, they focus on data transfer and it is authentication. Here they discuss the strategy for two security levels by utilizing two different techniques i.e. cryptography by AES and Steganography by an image and they simulated these two logics in MATLAB software.

[1] Institute of Graduate Studies, Electrical and Computer Engineering, Altınbaş University, Istanbul, Turkey.
College of Dentistry, Dental Basic Sciences, University of Mosul, Mosul, Iraq. 213720886@ogr.altinbas.edu.tr
[2] School of Engineering and Architecture, Electrical and Computer Engineering, Altınbaş University, Istanbul, Turkey.
osman.ucan@altinbas.edu.tr
[3] School of Engineering and Architecture, Electrical and Computer Engineering, Altınbaş University, Istanbul, Turkey.
saifabdalrhman@gmail.com
* Corresponding Author Email: 213720886@ogr.altinbas.edu.tr

Park and Kang (2015) [4], propose authentication for an inter-device in addition to a session-key system designed for IoT devices by only just encryption modules. In their proposed system, in contrast to existing network sensor environments in which the key distribution center provides the key, every sensor node is interested in the creation of session keys. Furthermore, in the proposed scheme, the improvement of system security performance has been achieved, in which the authenticated device can compute the session key in advance.

Yin, et al. (2015) [5] provide a secure system is suggested about employing image steganography to be an alternative security procedure when combined with a home server to protect the data transmission from an IP camera considering that it is an IoT device toward the other devices, by using WAN or LAN networks. In their work, a scheme is proposed based on the image steganography because the IP camera has low memory and processing capabilities and this method is used to solve the privacy issues through the transmission between the home server and the smart device.

Khambra and Dabas (2017) [6], provide a secure data transmission mechanism for IoT which uses AES to increase the security of data. The proposed system enhanced the AES algorithm in which several rounds or generation of private key increases will help in the generation of a more secure encrypted key through which devices can securely transmit data. To implement the proposed mechanism, they use MATLAB while to analyze performance they use metrics like execution time and throughput. Results show that in our mechanism throughput of the data transmission system increases.

Das and Chatterjee (2017) [7], suggested a security model based upon the combined two security approaches of the steganography technique with the cryptography technique to solve the data privacy issues through data transmission levels in a smart environment. They have recommended the use of an integrated methodology of DES and the Steganography methodology of Variable LSB Substitution to secure data transfer between the clouds and the home server.

Altameem, Ayman, et al.(2023) [8], By protecting the biometric data using encryption techniques, the security of IoTs was further enhanced. This study describes a novel picture encryption algorithm that combines the chaotic sequence with the AES algorithm. This method uses a random sequence to produce the encryption key. The original image is subsequently encrypted using the modified AES technique, which applies the round keys generated by the chaotic system. The encrypted images produced by the HAES-CM algorithm are more resilient to differential attacks because of these techniques, which also reduce the method's temporal complexity and dispersion. Furthermore, this function prevents unapproved users from decrypting the encrypted picture.

III. IOT SECURITY CONCEPT

A. Privacy and Security

Privacy is to make sure that people have the right to keep control over which information is gathered about them, who uses it, who maintains it, what purpose it is used for, and how it is used. The key privacy properties and services are as follows [9].

Un-link ability: Concealing info about the relationship between any kind of items, for example, messages, subjects, etc.

Un-Traceability: Making it hard for an attacker to recognize that the exact subject performed an offered set of actions.

Uno-bservability: Concealing the fact that the message has been sent.

Pseudonymity: It can use pseudonyms rather than using real identifiers.

Anonymity: It will Hide the information that achieves a given action or what which being described by a given dataset, Fig. 1. shows the main privacy properties and services.

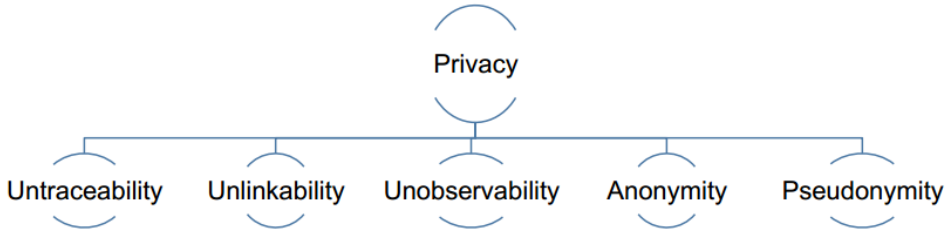


Fig. 1 Privacy properties and services

Additionally, the security should require blocking access to info or other objects from unauthorized users, along with securing from destruction of users' information and unauthorized alterations. The common security definition

equals it with availability, integrity, and confidentiality, known as (the CIA triad) by its acronym. The ISO7498-24 standard expands the security description of the following requisites that can be used [10]:

1) *Authentication:* The identifying process of an individual, is usually based upon identifying a username or email and password.
2) *Access control:* Users can access just those services and resources that allow to be access, and certified users are not denied access to services that they legally expect to receive.
3) *Availability:* A system is functional and operational at a certain moment.
4) *Confidentiality:* The data is not to be disclosed or available to unauthorized processes, users, or entities.
5) *Integrity:* The information has not been destroyed or altered in an unauthorized manner.
6) *Notarization:* The data registration with a certified third party who assures the data characteristics accuracy, for example, creation time, origin, and content.
7) *Nonrepudiation:* The senders and receivers of the messages are not denying that they sent and received the messages. Fig. 2. illustrates the security services requirements.

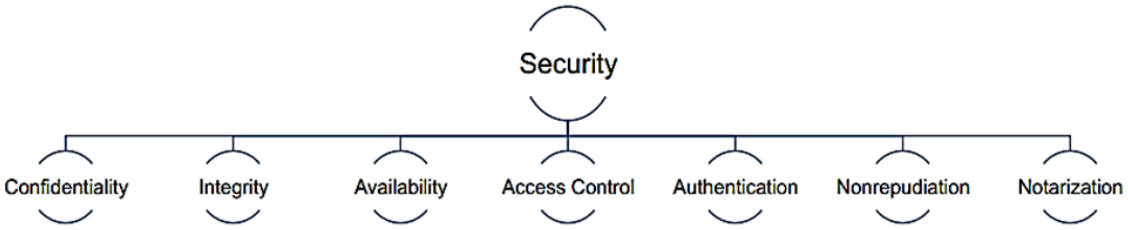


Fig. 2 Security services

As reviewed, the security and privacy are different. Even so, in the IoT field, the relationship in-between these two concepts are protection of the data. Fig. 3. illustrates the common relationship between privacy and security, which is, the confidentiality that is located in the intersection of security and privacy [11].

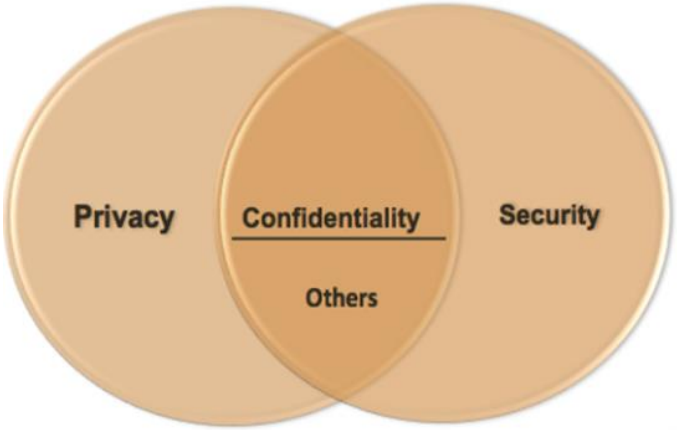


Fig 3 Security and privacy mutual relationship

B. IoT Security

The key to IoT security issues is the need for identification of both the mechanisms of authentication and confidentiality protection of the data. The 3 standard areas are the availability, confidentiality, and integrity of the data. Breaking any one of these 3 basic security aspects may lead to security damage to the IoT system. Data security, medium security, channels security, etc. a significant factors with which IT corporations are generally concerned Despite the theoretical concepts of smart devices and secured servers, efficient implementation of these security aspects is minimal [12].

The privacy and security qualifications can be described as follows:

- Information processing safety: The security of data processed at the IoT that reflected in the middleware layer,
- Terminal security issue: The terminal devices are almost easy to access and can cause modifications or damage to data. Integrity and authentication of the data is a past concern. As the passive RFID tags are not able to exchange a great number of messages with the authentication servers, the most important issues that

exist in the perception terminal involve terminal viruses, terminal-sensitive data leakage, copying, tampering, and various other issues,

- Information transmission security: security associated with the IoT security risk and the protocol weaknesses and defects,
- Sensor network security problem: sensors aren't just responsible for the transmission of data but are also for collaboration, integrity, and data acquisition. As a result, the security risk in data transmission and malicious code attacks could happen,
- Data Security: the data required to be transferred should be encrypted before transmission. Its goals are to secure the integrity and confidentiality of the data transmission and to protect against data tampering.

Depending on the security issue and security strategy of IoT devices it appears that the most efficient and common security method is based on cryptography techniques such as encrypted data by AES and secure authentication by Hash function such as SH1 [13]. However, these techniques are subject to different attacks which make the security of information case sensitive and can be stolen by attackers when taking into consideration that IoT devices do not convert its symmetric key, so it may be cracked dependent on the time computational hardware used [14]. In this steady, we have focused on combining some security techniques to get a high-security model that can be used in IoT security.

IV. Proposed Day Structure

As described in section 3 (IoT Security), the effective way to secure data is to combine some techniques to get a more secure communication method. The best method is combining cryptography with steganography to secure data transmission between either IoT devices or IoT servers. The first part should use symmetric encryption that utilizes (a message authentication code (HMAC) and then an advanced encryption standard (AES) algorithm) to encrypt secret messages and transform them. The second part used the steganography technique (Text, Image, Audio, and Video) to hide encrypted (or encrypted-compressed) data. In this work, we have designed a proposed communication system with IoT based on encryption of the authentication information (username, password) and the IoT IP address by using HMAC then embedding this information within text stego message and transfer to server in fully automated operation. In case the encryption key used in the decoder is true and the encryption/encoding strategy same as the server then the decoder will retrieve encrypted/hidden information and redirect to the requested IoT device by using the retrieved IP address and authentication information to log in to the IoT device. In case the encryption key is false no information gain and then server redirect to tricky page that there is no such IoT available.

A. Crypto Side

The AES algorithm can have utilized to encrypt transferred data based on the Rijndael algorithm. The AES block cipher can be processing (128 bits) of data blocks by using cipher keys of bits lengths (128, 192, and 256). The Rijndael input/output sequences length can be any of the three allowed values (128, 192, and 256) bits, but for AES the length which allowed is just 128bit. The common best practice for symmetric encryption is to use Authenticate Encryption with Associated Data (AEAD). In the proposed system, we can use AES with HMAC, which is a unique structure used to compute the MAC that makes use of a hash function combined with a secret cryptographic key. The AES-256 and then HMAC SHA-256, a two-step Encrypt and MAC that requires additional keys and additional overhead. The approach function takes the key(s), secret text string, and an option non-secret payload after that returns an encrypted string prepended with the nonsecure data with a 256-bit key(s) generated. Furthermore, it has helper options that utilize a string password for the generation of the keys. The proposed algorithm that utilized AES and HMAC is as follows:

1. Encryption Algorithm

Input:	**Secret message, cryptography keyword**
Output:	**Cipher Text**
Step 1.	Start.
Step 2.	Insert text for encryption.
Step 3.	Use Random Salt to block pre-generated poor password attacks. The bit size of salt is 64 (initially salt-1 is generated then derived and utilized for the encryption key in AES and also slat-2 is made then produced and utilized for the HMAC authentication key).

Step 4. Run the AES algorithm by utilizing a 128-bit block size and 256 key sizes.

- Convert secret data to UTF8.
- Chang encrypted text to Hexadecimal formatting, based on 64 strings then ASCII code.
- Apply encryption by AES and then utilize HMAC for a UTF-8
- Prepend nonsecure payload then IV
- Generate Cipher text.
- Collect encrypted data and apply HMAC SHA-256 to put authentication.

Step 5. Create encrypt secret data

Step 6. End.

B. Steganography Part

This technique can be used for a hiding process that can be utilized to hide the authentication data into the trick cover [15]. The cover and stego method should be dependent on the data type, in case it very large the Image, audio, and video are the best choices, However, the text stego is the best way to trick the attacker into that the data sent (cover text message) from IoT device is the original data while it hid within the secret message. The most effective stego method that can be utilized in text steganography as it cannot give any attention that there is any unusual modification of data.

TABLE I. keyword Assigned to Ciphertext

Ciphertext Value	**A**	**B**	**C**	**D**
Corresponding	00	01	10	11

whether Then the Stenographer's text can be like the following paragraph: (00 01 10 1). However, these lists depend on the random entry that should be the same in both server and client and can be a part of a sequence that changes its value for more security.

The decoded process of Text

1) Take the stenography text as input.
2) Traverse the text to search for the keywords.
3) Take the alphabet assigned for each keyword and form the string to decrypt.

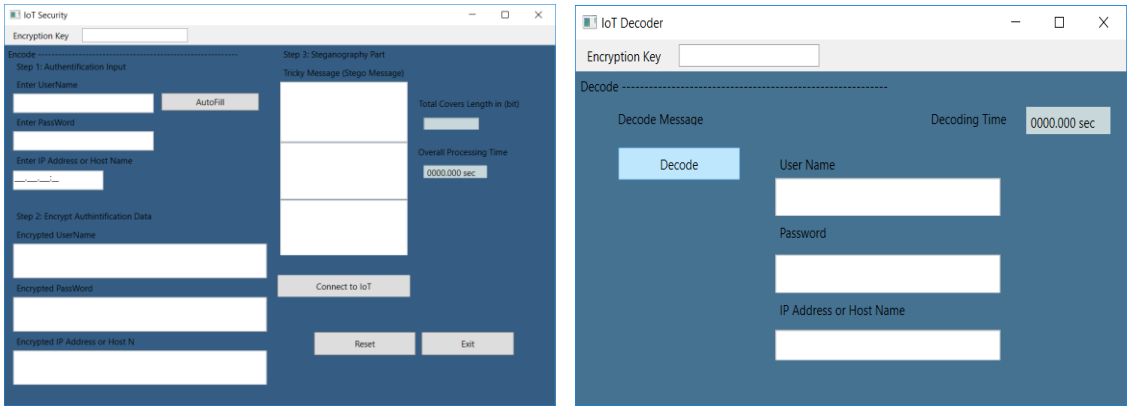
The stego algorithm is described as follows:

1. Stego Algorithm – Encoding

Input:	**Ciphertext, Binary words list**
Output:	**Cover Message**
Step 1.	Start encoder
Step 2.	Get the ciphertext string.
Step 3.	Start binary list compiler
Step 4.	○ Load binary list from file ○ Read ciphertext from left and replace each ciphertext character with corresponding binary value. Repeat operation for all authentication values and IoT device IP address
Step 5.	Rewrite the new value as binary cover message
Step 6.	Send Message

V. Result And Discussion

We have tested the operation of the system in communication between IoT devices and clients. We have simulated and tested the communication between client/server and IoT. C# language has been used for design and simulation operation between client-server-IoT. Fig. 4. shows the graphical user interface of the program.



(a) (b)

Fig. 4 The GUI of proposed security system for IoT. (a) The Encoder Side (b) The Decoder Side.

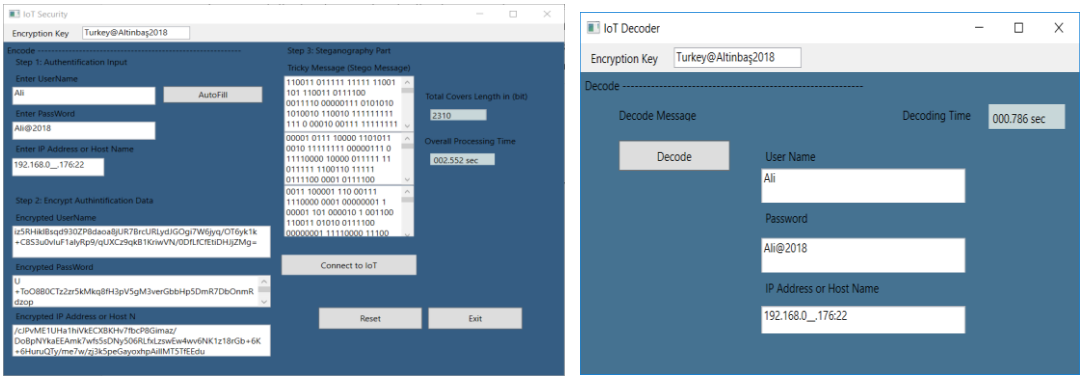
The GUI of the program has simulated and details the overall process that happens including the client-side encryption and decoding process, the chipper text generated, the cover message, and the time requested for overall operation. The client-side has a button named “connected to IoT” which works as a login button that sends the encrypted and hidden login information to the server. After pressing the button, the information is sends and server-side dialog will be appearing which is the decoder which can decode and decrypt the encrypted message. The decoder details the retrieved information including the username, password, and IP address. The retrieved information is then used to connect with the IoT device automatically where the IP/Hostname represents the IoT address and login information. If this information is true, the server will allow communication with IoT if not the server will show the tricky message that there is no IoT device to communicate. In this test we have used a selectable authentication information shown in table II.

Table II. Information Used in Authentication Test

User Name	**Ali**
Password	Ali@2018
IP Address of IoT Device	192.168.0.176:22
Encryption Key	Turkey@ Altinbaş2018

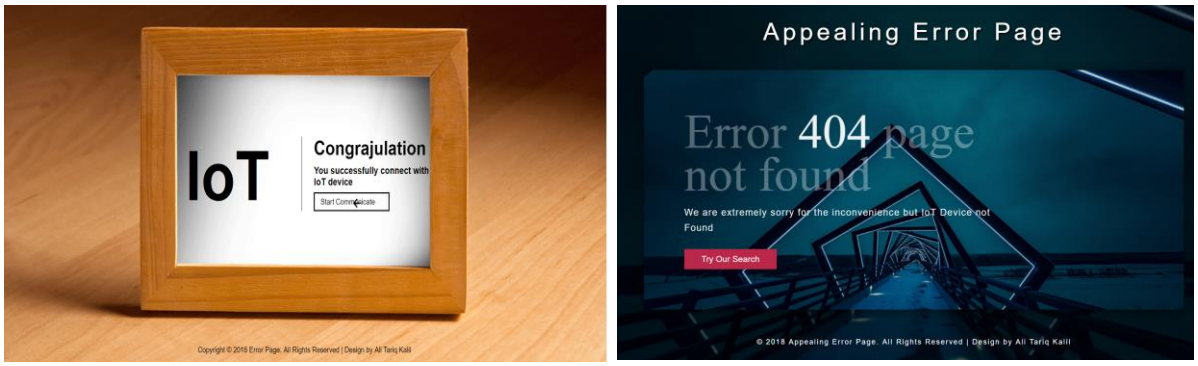
Note After putting communication information in the GUI and pressing the connection button, the proposed system successfully encrypted the authentication data and generated ciphertext for each data then embedded it in side tricky stego messages “binary text messages” then sent it to server/IoT side. The processing time is relatively fast which is all done in about ~2.5 seconds, the cover needed for embedding encrypted message is little which is about 2.3kb, and the stego message appears normal and tricky which appears as a normal binary message. Fig. 5. shows the Encoder GUI and its results.

On the server side the decoder runs automatically when received communication is requested, when put true key it successfully retrieves information data and redirects to IoT by using the IP address got from the decryption process and IoT authentication information (username and password) to connect with IoT. The decoding process run in very fast in about 0.78 second and work smoothly, automatically, and effectively. Fig. 5. shows the Decoder GUI and its results.



(a) (b)

Fig. 5 The encoder/decoder results. (a) Encryption and imbedded results on the client side, (b) The decrypted/decoded results on the client side.



(a) (b)

Fig. 6 The authentication messages when the user inputs connection information: (a) success login when the user puts the correct information, (b) failed login (Tricky message) when the user puts incorrect information.

For hiding, we have tested the ability to detect the unusualities in the cover message that give suspension by observer and attacker. In this part, we used two printed paper that included a cover message and made questionnaire questions in three stages as follows:

In the first questionnaire question, we asked the following question: "What is this message and what represent?", In the second questionnaire question we explained this is an IoT message and asked the following question: "This is an IoT message what the content of Message is?", In third questionnaire question we explained this is stego message and ask the following question: "This is stego message, if you detect something unusual please verify?"

These questionnaire question has been asked to a range of people home specialist in information technology and security. The questionnaire results show that the stego method is hard to detect and the first two questions show that no one can recognize there is a cover message, the third question appears even when explained there is stego message when one detects the method, and the unusuality in the cover message. The questionnaire results are detailed in Table III.

Table III. Questionnaire Results For Visibility

Questions	Number of People Detect the Unusuality	Several Person Cannot Detect the Unusuality	Several Person suspect there is Unusuality
First Question	0	15	0
Second Question	0	15	0
Third Question	0	11	4

Finally, we have tested the ability to crack the encryption data (ciphertext). We have used some common attacks that can be used to crack ciphertext, we have checked the ciphertext in different sites and software that offers most attacks such as dictionary attacks, rainbow attacks, etc. These sites and programs included (The crackStation site[16], Hash Cracker site [17], OnlineHashCrack site [18], RainbowCrack program [19], and John the Ripper Hash Cracker software [20]). The test result shows hash password is invalid and cannot be cracked.

VI. CONCLUSION

In this paper we propose a system that combines two security strategies, cryptography to change the authentication and connection information to an unreadable form, and steganography to hide encrypted information to prevent any suspension there is any communication security has been used. The encryption has been done by using AES256 and the HMAC algorithm. The steganography method is based on text steganography. The strategy is based on used a list of text that each ciphertext character has a corresponding binary value, where the final cover message appears as a binary message transfer between the user and IoT device. The communication and authentication information has been encrypted then hidden in text cover then transferred between users worldwide and local servers of IoT. All information including the IP address or hostname of the IoT device has been encrypted and hidden, so no one can identify or pass to IoT without passing the three stages of authentication. In the first stage, the user should encrypt information in the same key used in the server where this key can be static or dynamic (RSA), in addition, the server and client should have and share a Mac (v Key) in which there is no encryption if the user not has the authorized in server. In the second stage, the user should have the same stego strategy used in embedding encrypted data. In the third stage, the user should have the correct authentication of the IoT device. In case fails in any part no IoT device can be detect or reached and its location stay hided in cloud.

REFERENCES

[1] Rizvi, S., et al., Threat model for securing internet of things (IoT) network at device-level. Internet of Things, 2020. 11: p. 100240.

[2] Zhou, W., et al., The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of things Journal, 2018. 6(2): p. 1606-1616.

[3] Srivastava, A.K., A. Agarwal, and A. Mathur, Internet of Things and its enhanced data security. International Journal of Engineering and Applied Sciences, 2015. 2(2): p. 257986.

[4] Park, N. and N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. Sensors, 2015. 16(1): p. 20.

[5] Yin, J.H.J., et al. Internet of Things: Securing data using image steganography. in 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS). 2015. IEEE.

[6] Khambra, D. and P. Dabas, Secure data transmission using AES in IoT. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2017. 6(6): p. 283-289.

[7] Das, R. and P. Chatterjee. Securing data transfer in IoT employing an integrated approach of cryptography & steganography. in Proceedings of the International Conference on High Performance Compilation, Computing and Communications. 2017.

[8] Altameem, A., et al., A hybrid AES with a chaotic map-based biometric authentication framework for IoT and Industry 4.0. Systems, 2023. 11(1): p. 28.

[9] Kizza, J.M., Internet of things (iot): growth, challenges, and security, in Guide to Computer Network Security. 2024, Springer. p. 557-573.

[10] Mendez Mena, D., I. Papapanagiotou, and B. Yang, Internet of things: Survey on security. Information Security Journal: A Global Perspective, 2018. 27(3): p. 162-182.

[11] Ahmed, S. and Khan, M., 2023. Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. AI, IoT and the Fourth Industrial Revolution Review, 13(9), pp.1-17.

[12] Swamy, S.N. and S.R. Kota, An empirical study on system level aspects of Internet of Things (IoT). IEEE Access, 2020. 8: p. 188082-188134.

[13] Moradi, M., M. Moradkhani, and M.B. Tavakoli, Security-Level Improvement of IoT-Based Systems Using Biometric Features. Wireless Communications and Mobile Computing, 2022. 2022(1): p. 8051905.

[14] Sadhu, P.K., Yanambaka, V.P. and Abdelgawad, A., 2022. Internet of things: Security and solutions survey. Sensors, 22(19), p.7433.

[15] Wang, Z., Byrnes, O., Wang, H., Sun, R., Ma, C., Chen, H., Wu, Q. and Xue, M., 2023. Data hiding with deep learning: A survey unifying digital watermarking and steganography. IEEE Transactions on Computational Social Systems, 10(6), pp.2985-2999.

[16] Patel, P.N., J.K. Patel, and P.V. Virparia, A Cryptography Application using Salt Hash.

[17] “hash-cracker.com - This website is for sale! - hash cracker Resources and Information.” http://www.hash-cracker.com/

[18] “Professional cloud password testing & recovery services.” https://www.onlinehashcrack.com/

[19] “RainbowCrack - Crack Hashes with Rainbow Tables.” http://project-rainbowcrack.com/

[20] “Openwall - bringing security into open computing environments.” https://www.openwall.com/