RESEARCH ARTICLE OPEN ACCESS

Sensitive Based Privacy Preserving on Shared Data in Cloud using Reversible Data Hiding with Encryption

C.Surya*, V.Kalaivani**, K.Kaviya***, T.Thangamathi****

*(Assistant Professor/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: csurya714@gmail.com
** (Student/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: vkalaivani1707@gmail.com
*** (Student/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: kaviyakaviya125@gmail.com)
**** (Student/CSE, Sri Ramakrishna College of Engineering, and Perambalur)
Email: thangamathi000@gmail.com)

--************************----------------------------------

Abstract:

The patient health record maintenance is sensitive and crucial task in health care sectors. The patient medical care records are stored in a huge data set; it can be stored, maintained and traced every day. The objective of this project is to store patient's health reports safely. In Existing, Cryptographic-based encryption is to encrypt data into unreadable code; it is more likely to attract the attacker's attention. Once these ciphertext is intercepted, the attacker will try to decrypt these ciphertext to obtain some useful information, so as to carry out some illegal activities. Some health care information not only have high requirements for privacy protection, but also want to be able to express their preference in the decision-making of privacy protection, so they may want to define what information is sensitive to them and what is not. The proposed model can classify the data into sensitive data and non-sensitive data according to the user's preferences with SVM (Support Vector Machine) based machine learning classification. Since non-sensitive data pose no threat to user privacy, it can be transmitted directly on ordinary channels without being processed. While, sensitive data need to be processed before it can be transmitted. In terms of sensitive data processing, here proposes a method of combining data encryption with information hiding. Sensitive data are encrypted using Advanced Encryption Standard (AES) encryption algorithm before it can be transmitted, making it to unreadable code. Then, a novel information hiding method proposed, named the Modified LSB (MLSB) information hiding method is used to provide a second guarantee for the security of sensitive data. In other words, the sensitive information is hidden in the multimedia carrier, so that the adversary cannot notice the existence of sensitive information.

Keywords —**privacy, sensitive data, machine learning, fuzzy logic, data hiding and extraction**.

--************************----------------------------------

I. INTRODUCTION

Steganography is the practice of hiding secret messages (hidden text) within every day, seemingly innocuous objects (cover text) to produce a stego text. The recipient of a stego text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego text. The goal of steganography is to allow parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation. This sets steganography apart from cryptography which, although providing for private communication, can arouse suspicion based solely on the fact that it is being used.

Modern steganography was characterized by G J Simmons when he stated the problem in terms of prisoners attempting to communicate covertly in the presence of a warden. Alice and Bob, prisoners, are allowed to communicate, but their channel is through the warden, Ward. Alice wishes to pass secret messages to Bob in such a way that Ward can determine neither the contents of the secret messages, nor even that secret messages are being passed.

In modern times, this problem can be observed in national intelligence agencies attempting to detect public yet covert communication between terrorists, or communication between citizens in oppressive states which have outlawed cryptography.

II. EXISTING SYSTEM

The smart home network model is generally composed of four parts, they are smart sensors, gateway node, user terminal and server. Smart sensors (such as temperature and humidity sensors, imaging sensor, healthy care sensors, etc.) are mainly responsible for collecting information of the home environment and the health status of the family, and then transmitting the information to the gateway node through wired or wireless network.

As some information of the smart home is private to users, they do not want these data to be leaked, so it is necessary to put forward an effective privacy protection scheme. This paper proposes a scheme based on information hiding, it combines DES encryption algorithm with TTMSB information hiding method to protect the privacy of smart home system, during the sensitive data are transmitted.

In the smart home network model, gateway is a node with relative strong computing and storage capacity, which can be used to classify data into sensitive data and non-sensitive data, encrypt sensitive data and hide them into cover images. Sensitive information is hidden into the cover image before it is transmitted by ordinary channels, it will not be found easily by the adversary.

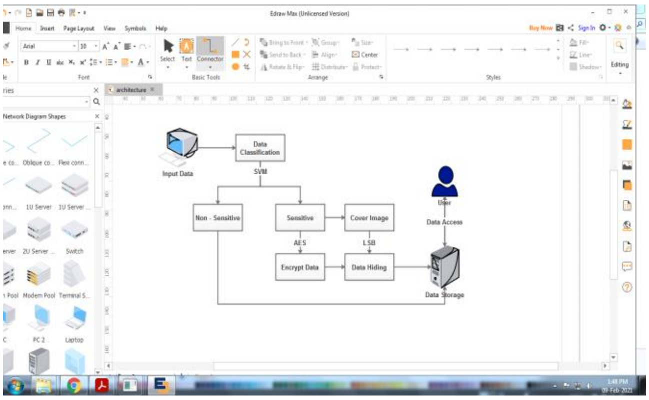
The server has a strong computing power, and it is completely trusted by the user. When it receives the data transmitted by the gateway, it extracts the ciphertext from the stego image and decrypts it into plaintext (original sensitive data). After that, the server calculates and analyzes the data and feeds the final result back to the user terminal.

III. PROPOSED SYSTEM:

For providing security to the shared medical data, the proposed system combines encryption and steganography approach.

Before applying encryption on data, the data could be classified sensitive and non sensitive. Uploaded data are classified into sensitive data and non-sensitive data according to the preference of users. Sensitive data are automatically classified with the help of SVM (Support Vector Machine) classification.

The encryption is done in specified number of rounds. This makes the data secure. Then hide the encrypted sensitive information in cover image using Modified LSB Technique. In Modified LSB, the cover image is divided into non-overlapping pixel blocks of 3x3 pixel blocks. The patient gives the different users the corresponding decryption key. Using the key the users will be able to access the relevant data only.



A. Framework Creation

Health care data sharing is the process share patient's health information to the requester. Here create an application for secure health care information sharing using data hiding and encryption approach. Before accessing application user should enroll in this application.

User enrolment is the process of registering with application to make communications. Here users are defined as sender and receiver. Both are registered in this application and get authentication factors for login process.

Authentication is the process of verifying whether the user is valid or not. Authenticated users are only allowed to access application. Otherwise the system shows invalid access message.

B. Data Categorization

Before transmitting health care information to the server, they are classified into sensitive data and non-sensitive data according to the preference of users. For the classification purpose here utilize machine learning based SVM (Support Vector Machine) algorithm.

At first, users label the dataset according to their own preference, and then the classifier trains the classification model. In order to reduce the complexity of the classifier and give consideration to the universality of the classifier, this paper decides to adopt SVM as the classify model. In the first line, users label the sensor dataset according to their preference. After training the label dataset generates a classifier.

The classifier is input by healthcare data, it can distinguish sensitive data and non-sensitive data. The non-sensitive data can be transmitted directly on the ordinary channel without being processed. While, the sensitive data is firstly encrypted, and then the ciphertext that present with garbled code state is hidden into the cover image.

C.Encrypt Sensitive Data

Data encryption is the process of converting the plain text information into unreadable form. Here sensitive information could be encrypted using AES algorithm. Because the health care system focuses on lightweight, in order to reduce the complexity of data encryption operation and take the security of encryption into consideration, the scheme decides to use AES data encryption algorithm. AES encryption is performed in multiple rounds.

Each round has four main steps including sub-byte, shift row, mix column and add round key. This will enhance the security of shared secret image.

D.Sensitive Data Hiding

Data hiding is the process of hiding secret message into cover file. Secret message is present in the form of text and cover file is selected in form of image. The encrypted sensitive health care information was hidden within the image to create stegno image.

Generate key for securely sharing the information to receiver. In the process of embedding, the cover image is divided into non-overlapping pixel blocks of 3x3 pixel blocks. Block levels are based cardinality of the cover image. If secret bit is 1 and LSB of stego pixel is 0 or vice-versa, then 1 is added or subtracted to the stego pixel.

E.Data Extraction

Data extraction is the process of extracting the original data. Receiver gets the sensitive information with cover image. Specific key is generated and shared to the receiver during the process of data sharing. The stego image is same as the cover image, because it hasn't been modified at all when hiding the sensitive data into the cover image, the attacker can hardly notice the presence of ciphertext in the stego image.

After receiving the stego image, the receiver extracts the ciphertext from the stego image with the extraction key, and then decrypts the ciphertext with the decryption key to obtain the plaintext data.

IV. CONCLUSIONS

This paper proposes a reversible data hiding technique for sensitive information hiding using SVM classification technique. The data hiding capacity and speed is increased by combining Modifiedconfirmation, outfitted with the thought behind the strategy guarantees that an unknown user can't access the information from server, *which* makes its security analysis less *difficult and more pragmatic. It* will share information in a secure manner with the help of key distribution and verification method. The combined cryptography and steganography approach reduces the success rate attacker, when try to access data from server

FUTURE ENHANCEMENT

In future work, an efficient video data steganography method based on IWT shall be implementing. In the video data steganograohy , the host video is split into frmes and high frequency bands are performed to offer data hiding space.

REFERENCES

[1] Patel, Arpit, and Tushar A. Champaneria. "Fuzzy logic based algorithm for Context Awareness in IoT for Smart home environment." In 2016 IEEE Region 10 Conference (TENCON), pp. 1057-1060. IEEE, 2016

[2] Mehrotra, Sharad, Alfred Kobsa, Nalini Venkatasubramanian, and Siva Raj Rajagopalan. "TIPPERS: A privacy cognizant IoT environment." In 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), pp. 1-6. IEEE, 2016.

[3] Keshavarz, Mahsa, and Mohd Anwar. "Towards improving privacy control for smart homes: A privacy decision framework." In 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1-3. IEEE, 2018.

[4] She, W. E. I., Zhi-Hao Gu, Xu-Kang Lyu, Q. I. Liu, Zhao Tian, and Wei Liu. "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving." IEEE Access 7 (2019): 62058-62070.

[5] Zhou, Zhili, Huiyu Sun, Rohan Harit, Xianyi Chen, and Xingming Sun. "Coverless image steganography without embedding." In International Conference on Cloud Computing and Security, pp. 123-132. Springer, Cham, 2015.

[6] Bilal, Muhammad, Sana Imtiaz, Wadood Abdul, Sanaa Ghouzali, and Shahzad Asif. "Chaos based Zero-steganography algorithm." Multimedia tools and applications 72, no. 2 (2014): 1073-1092.

[7] Zheng, Shuli, Liang Wang, Baohong Ling, and Donghui Hu. "Coverless information hiding based on robust image hashing." In International Conference on Intelligent Computing, pp. 536-547. Springer, Cham, 2017

[8] Zou, Liming, Jiande Sun, Min Gao, Wenbo Wan, and Brij Bhooshan Gupta. "A novel coverless information hiding method based on the average pixel value of the sub-images." Multimedia tools and applications 78, no. 7 (2019): 7965-7980.

[9] Chen, Min. "Towards smart city: M2M communications with software agent intelligence." Multimedia Tools and Applications 67, no. 1 (2013): 167-178.

[10] Qin, Jun, and Zhong-Shi He. "A SVM face recognition method based on Gabor-featured key points." In 2005 international conference on machine learning and cybernetics, vol. 8, pp. 5144-5149. IEEE, 2005

[11] Yang, Yi, Min Shao, Sencun Zhu, and Guohong Cao. "Towards statistically strong source anonymity for sensor networks." ACM Transactions on Sensor Networks (TOSN) 9, no. 3 (2013): 1-23.

[12] Sianaki, Omid Ameri, and Mohammad AS Masoum. "A fuzzy TOPSIS approach for home energy management in smart grid with considering householders' preferences." In 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), pp. 1-6. IEEE, 2013.

[13] Yadav, Er Pooja, Er Ankur Mittal, and Hemant Yadav. "IoT: Challenges and issues in indian perspective." In 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1-5. IEEE, 2018.