Journal of Harbin Engineering University Vol 44 No. 7
ISSN: 1006-7043 July 2023

Enhancement In Data Security for Generation of Novel Encrypted Code Using Cryptography for Multiple Level Data Security

Bollepogu Venkateswarlu[1], Dr. Pramod Pandurang Jadhav[2]
Research Scholar
Department of Computer Science & Engineering, Dr. A.P.J. Abdul Kalam University, Indore
Corresponding Author: Bollepogu Venkateswarlu

ABSTRACT: In today's scenario, where everything is based, there is a huge demand for data security. A large number of cryptographic techniques are available to handle this problem. EPR is a collection of several private information related to a patient which needs data authenticity, data security as well as safe and secured transmission. The proposed methodology used both cryptography and image processing techniques to build a new type of encrypted information code in image format which can be transmitted and used like bar code, QR code but even more secure. The success rate of recovery of data is 100% for both short and long messages. The information can also be retrieved at the receiver side exactly same without any loss of information. Use AES algorithm consequently, with three keys and followed by some image processing techniques like complement, flip make the proposed algorithm more unbreakable. In this analysis a complete Graphical User Interface (GUI) has been developed for both encoder transmitter and decoder- receiver section. To increase data security, data can first be compressed using compression techniques and then encryption techniques can be applied. This technique increases the security and reduces the speed.

KEYWORDS: Cryptography, Data authentication, Content protection, Graphical User Interface (GUI)

I. INTRODUCTION

Data is collection of raw facts and figures. Security is the protection from danger or threat. Data security refers to the protection of data from unauthorized access. The purpose behind data security is to protect any kind of data so that privacy can be ensured. Any kind of data sent over the network has a possibility of being breached. So there is definitely a need of data security so as to protect our data from being brute forced.

Compression is reduction in the number of bits. It is achieved by eliminating redundancy in data. Data compression ensures minimum cost, lesser storage and it takes less amount of time to send a file from one place to another.

Cryptography refers to the use of mathematics for data security. Encryption is the conversion of original data i.e. Plain text into a private code i.e. Cipher text. Password is needed to access the encrypted data. To encrypt data, we use two types of techniques which are commonly called as symmetric (same key is used in encryption and decryption) and asymmetric (different keys are used in encryption and decryption) key algorithms. Cryptography is the study of information hiding and achieving security by encoding messages to make them non-readable. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and also enable verifiability [4]. Cryptography deals with four main objectives such as message confidentiality: where only the authorized recipient must be able to extract the contents of the message from its encrypted form, message integrity: where the recipient should be able to determine whether the message has been altered or tampered, sender authentication: where the recipient should be able to verify the identity of the sender, the origin or the path it travelled from the message, to validate the claims of emitter to the recipient expectations, and lastly sender non-repudiation: where the emitter should not be able to deny sending the message.

Recent development in modern communication and computer technology are moving to a digital world for perfection, effectiveness, convenience and security. As an example in medical field, traditional diagnosis is being replaced by e-

diagnosis. It makes possible for health professionals from different locations to serve a patient. The patient can get the possible best diagnosis and treatment from this medical process. The necessity of fast and secure diagnosis is vital in the medical world. The patients can be treated locally by effective and secured communication between remote hospitals and distant specialist [14]. The transmission of information among the geographically separated medical organizations is done in a secured way. The professionals use the Internet for transmitting the data [15]. The data is a collection of several private information or information related to a person and can be represented in various forms such as diagnostic reports, images etc. The data transmitted through the internet is very important since it contains the sensitive information of a person in digital format. This digitized data must be stored in a secured environment to preserve persons privacy. It is also important to prevent unintentional distortions and malicious modifications of the same [7]. For the security and of the data, cryptographic approaches are used as protection of data in digital system is very important. Currently in the exchange information system several software are used with easy to understand GUI. A Graphical User Interface (GUI) is a display in a window format having several edit and static boxes, push buttons etc. those enable an end user to perform interactive operation. Presently the use of bar code or QR code is very much popular to have the several information in an encrypted form in a small area.

II. LITERATURE SURVEY

J.Wang, N. N. Xiong, J.Wang andW. Yeh et al [1] compact the scale of access policy through greedy compacting algorithm, so that the ciphertext redundancy can be reduced due to the decreased policy scale. Multiple users share the public policy nodes. By introducing flexible factor and overlap factor, the policy-computing efficiency and compact ratio are analyzed. Policy-compacting fundamentally solves the problem of ciphertext redundancy caused by the large scale of policy, which is of great significance to improve the performance.

J. Li, X. Lin, Y. Zhang and J. Han et al. [2] presented an outsourcing KP-ABE scheme with efficient query processing, which implements outsourcing key-issuing and outsourcing decryption. The data owner uploads the ciphertext with a keyword set to the storage cloud service provider. Users submit a trap door for a keyword such as "book" to the cloud service providers to request keyword search. After receiving the client's request, cloud service provider immediately performs partial decryption and keyword search on the ciphertext, and returns the matching results to the user. Outsourcing decryption enables users to save a lot of computing resources on the premise of maintaining confidentiality of data. Using trapdoor instead of keyword plaintext to perform query processing avoids cloud service provider using cookie records to pry into users' privacy and preferences.

M. Usman., I. Ahmed , M. Imran , S. Khan, U. Ali, et.al [3] described the light-weight cryptographic algorithm for the internet of thing (IoT) named as the secure internet of thing SIT. The proposed algorithms are designed for the internet of thing to deal with the safety and resources utilization challenges. The architecture of proposed algorithm introduced easy structure suitable for implementing on the internet of thing environment. A lot of well-known block cipher including AES (Rijndael), 3-Wa, SAFER, SHARK, Grasshopper PRESEN, and Square use Substitution Permutation SP NW. various alternative rounds of substitution and transposition satisfy Shannon's confusion plus diffusion properties which ensure that the cipher text is changed in a pseudo random way. Other common ciphers including SF, Blowfish, Camelia, and data encryption standard use the Feistel architecture. One of the main advantages of using Feistel architecture is that the encryption plus decryption procedures are almost self-same. A suggested algorithm is a hybrid approach based Feistel plus Substitution-Permutation SP networks. Therefore, creating use of properties of both approaches to improve a light-weight algorithm that presents substantial security in the internet of thing environment while keeping the computational complexity at the mild level.

J. Li, J. Li, X. Chen, C. Jia and W. Lou et al. [5] improved the result of with introducing outsourced computation into Identity-Based Encryption (IBE) revocation and showed the security definition of outsourcing revocable IBE for the first time. In this scheme, PKG no longer undertakes the task of key update except to send a private key for decryption to the user at the beginning.

Y. Shi, Q. Zheng, J. Liu, and H. Zhen et al [6] presented a Key-Policy Attribute-Based Encryption (KP-ABE) scheme with direct revocation and verifiable ciphertext delegation. In their scheme, trusted authority revokes users via updating revocation list and any interaction with non-revoked users at the same time. After receiving the new revocation list, the third party (such as cloud service provider) updates the ciphertext using public information, and this ensure the new ciphertext cannot be decrypted by revoked users. Finally, any authorized auditor has the privilege to verify if the third party has updated the ciphertext correctly. This scheme not only forbids revoked users to decrypt the new ciphertext, but also provides verifiable function for data owners to ensure that ciphertext has been updated under the new revocation list.

S.Mohsen, Ghoreishi, S. Abd Razak, I. Fauzi Isnin, H. Chizari, et.al [8] analyzed an encoding and decoding protocol to satisfy efficiency plus security requirements, the author use of Elliptic Curve ECC based cryptosystems leads to implementing more effective symmetric- key cryptographic scheme, this led to that the result is made other researchers capable of classifying the challenges over provably safe cryptosystem or light-weight ones.

K. Biswas, et.al [9] presented a secure and light-weight encryption scheme based on the chaotic map and genetic operations. This scheme is secure, light-weight and suitable for use in wireless sensor networks WSNs.

K. Nur, Y. Purwanto, D. Darlis et al [10] implemented the Data Encryption for IoT Using Blowfish Algorithm on FPGA" the author presents a Blowfish algorithm is executed on Field Programmable Get Array (FPGA)by use Very High Speed Integrated Circuit Hardware Description Language (VHDL)it is a programming language. Using field programmable get array (FPGA) implementation is simple to implement, cheap, high speed, and reprogrammed. Decrease total encryption time, give better throughput and not affective avalanche effect significantly.

A. Sahai, H. Seyalioglu, and B. Waters et al. [11] presented a practical revocable storage attribute based encryption, where the database will regularly update the stored ciphertext with the available public information, and any revoked user will lose access privileges after the ciphertext is updated.

T. Eisenbarth C. , Paar, A. Poschmann, S Kumar., L. Uhsadel et.al [12] developed the light-weight PRESENT signified a milestone, block cipher in light-weight cryptography with many light-weight designs being proposed afterward. The primary survey on light-weight was held in the same-self year, reviewing many asymmetric and symmetric ciphers for embedded “hardware H/W and software S/W”.

J. Bethencourt, A. Sahai and B. Waters et.al [13] provided the first construction of Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In CP-ABE, the policy is embedded in the ciphertext, and data owner can define the access policy to determine which attributes the person with can access the ciphertext. User’s private key is related to the set of corresponding attributes. From a mathematical point of view, access structures can be seen as a monotonic " access tree", and its nodes consist of threshold gates and the leaves describe attributes.

III. Enhancement In Data Security For Generation Of Novel Encrypted Code Using Cryptography For Multiple Level Data Security

The block diagram of the enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security is represented in fig.1.

Here a new type of encrypted EPR code is generated to hide several information related to a patient for privacy, secrecy and data authenticity. This method is the combination of substitution and transposition cipher. Here, confusion is achieved by shifting of the letters of the input file and diffusion by reversing and swapping the input data as plaintext.

The input Electronic Patient Records (EPR) is then converted to its corresponding ASCII values. This ASCII values are at first inverted then encrypted using the RSA Algorithm which needs two prime numbers as two encryption keys which produce the encrypted ASCII values. In the next step the RSA encrypted ASCII values are again encrypted using the AES Algorithm with a user input key which construct a binary array of 1 's and O's. This binary array is converted into a binary image containing black and white dots, which is the information image. The three keys which were used for RSA and DES encryption process are also converted into a binary image and it is appended to the lower portion of the information image. To keep the keys separate from the information image one row of O's followed by one row of l's are padded in between keys and information image. In the next step some basic image processing techniques are used to achieve more security for protection of the EPR.

The information image is also converted into binary array which is at first decrypted using AES algorithm with the exact key used for AES encryption. In the next step the AES decrypted values are again decrypted using the RSA algorithm with the two exact keys used for RSA encryption. The obtained ASCII values from RSA decryption is then inverted to have information of the electronic patient record depicted to its respective area.

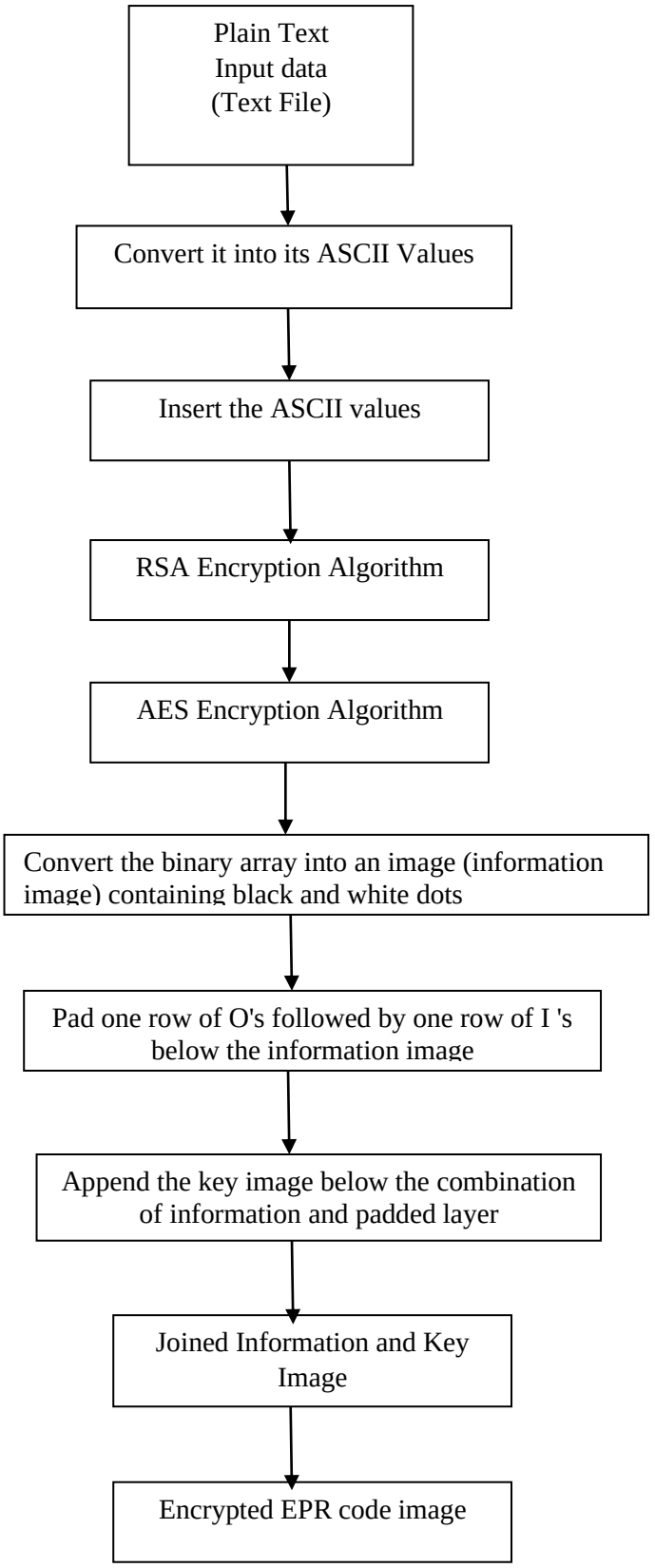

Fig.1 Block Diagram Of The Enhancement In Data Security For Generation Of Novel Encrypted Code Using Cryptography For Multiple Level Data Security

IV. RESULT ANALYSIS

The result analysis of framework of enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security is demonstrated in this section.

Table.1 Performance Analysis

	Efficiency (%)	Speed (Sec)
Multiple Level Data Security Using AES	99	0.35
Multiple Level Data Security Using DES	91	0.69

The above table shows that the performance analysis of the enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security gives high, efficiency and speed.

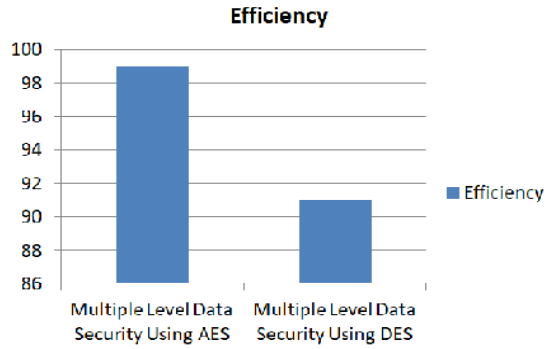

Fig.2: Efficiency Comparison Graph

Fig.2 shows the efficiency comparison graph for enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security.

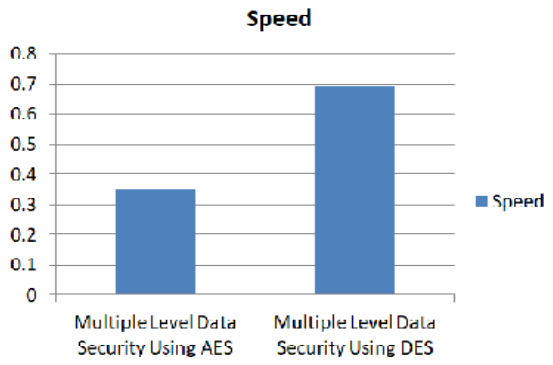

Fig.3 Speed Comparison Graph

Fig.3 show speed comparison graph for Multiple level data security using AES and Multiple level data security using DES.

In Fig.2 and Fig.3 comparison graph between the Multiple level data security using AES and Multiple level data security using DES for the enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security in terms of efficiency and speed is shown.

V. CONCLUSION

The proposed encryption and decryption technique is a combination of cryptographic algorithm and image processing techniques. A complete GUI for the proposed methodology clearly describes the outcomes for the both encryption and decryption algorithm. In the encryption part the GUI takes several information related to patient as inputs which form the EPR. Several cryptographic encryption steps for RSA, DES algorithm and the formed information image and key image from binary array is shown in the GUI along with some basic image processing techniques like flip, complement etc. The final image termed as encrypted EPR code image obtained from the GUI is being written in a .bmp file to keep all information intact. At the decryption part the GUI accepts the stored image file as input from where it retrieves all the information related to the patient exactly same. The recovered information is also placed in the relevant areas in the GUI for clear understanding. In Fig. 2 and Fig. 3 the screen shots of the proposed GUI is given where the both the encoder and the decoder part are shown. The recovery process is quite efficient to retrieve all the information from the encrypted EPR code image. Hence, to increase data security, data can first be compressed using compression techniques and then encryption techniques are applied. Therefore this technique increased the security and reduces the speed.

REFERENCES

[1] J.Wang, N. N. Xiong, J.Wang andW. Yeh, “A Compact Ciphertext-Policy Attribute-Based Encryption Scheme for the Information-Centric Internet of Things,” IEEE Access, vol. 6, pp. 63513–63526, 2018.

[2] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: Outsourced Attribute- Based Encryption with Keyword Search Function for Cloud Storage," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 715–725, Sept. 2017

[3] M. Usman., I. Ahmed , M. Imran , S. Khan, U. Ali , "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

[4] B.A.Forouzan, Cryptography & Network Security,McGraw-Hill, 2015

[5] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, Feb. 2015

[6] Y. Shi, Q. Zheng, J. Liu, and H. Zhen, "Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation," Information Sciences, vol. 295, pp. 221-231, Feb. 2015

[7] S. Koley, K. Pal, G. Ghosh, M. Bhattacharya, Secure Transmission and Recovery of Embedded Patient Information from Biomedical Images of Different Modalities through a Combination of Cryptography and Watermarking, International Journal of Image, Graphics and Signal Processing (IJIGSP), volume 6, number 4, pp- 18-31, 2014, ME CS Publisher.

[8] S.Mohsen, Ghoreishi, S. Abd Razak, I. Fauzi Isnin, H. Chizari, "Security Evaluation Over Lightweight Cryptographic Protocols," International Symposium on Biometrics and Security Technologies (ISBAST) 2014.

[9] K. Biswas ," Light-weight Security Protocol for Wireless Sensor Networks," School of ICT, Griffith University 2014.

[10] K. Nur, Y. Purwanto, D. Darlis. "An Implementation of Data Encryption for Internet of Things using BlowFish Algorithm on FPGA," In Information and Communication Technology 2014, 2nd International Conference on, pp. 75-79. IEEE, 2014.

[11] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption," in Proc. CRYPTO, Berlin, Germany: Springer, 2012, pp. 199–217.

[12] T. Eisenbarth C. , Paar, A. Poschmann, S Kumar., L. Uhsadel, "A survey of lightweight cryptography – implementations," IEEE Design and Test of Computers. 2007*;* 24*(6):*522–533.

[13] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy AttributeBased Encryption," in Proc. IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 321–334.

[14] F. Cao, H. K. Huang, X. Q. Zhou, Medical image security in a HIPAA mandated PA CS environment, Computerized Medical Imaging and Graphics, 27 (2-3), pp- 185-196, 2003.

[15] H. M. Chao, C. M. Hsu, S. G. Miaou, A data-hiding technique with authentication, integration, and confidentiality for electronic patients records, IEEE Transactions Information Technology inBiomedicine, pp- 46-53, 2002.

[16] Miodrag J. Mihaljevic´, Ryuji Kohno, "Cryptanalysis of Fast Encryption Algorithm for Multimedia FEA-M", *IEEE Communications Letters*, vol. 6, no. 9, pp. 382-384, Sept. 2002, IEEE

[17] Ahmet M. Eskicioglu and Edward J. Delp, "A KEY TRANSPORT PROTOCOL BASED ON SECRET SHARING APPLICATIONS TO INFORMATION SECURITY", *IEEE Transactions on Consumer Electronics*, vol. 48, no. 4, pp. 816-824, Nov. 2002, IEEE

[18] Robert M. Bevensee, "Feigenbaum encryption of messages", *IEEE Potentials*, pp. 39-41, Feb. /Mar. 2001, IEEE

[19] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proc. CRYPTO, Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.

[20] D. Song, D. Wagner and A. Perrig, "Practical techniques for searches on encrypted data," in Pro. 2000 IEEE SP, Berkeley, CA, USA, 2000, pp. 44– 55.