International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1175-1179 www.ijaem.net ISSN: 2395-5252

"Secure Data Transmission Using Cryptography"

Prof.G. R. Kulkarni1, Miss.Kolle Sarika2,Miss. Yanganti Mahalaxmi3,Miss.Korud Shravani4, Miss.Parhe Payal5

[1]Professor, BMIT college of Engineering, Solapur, Maharashtra, India[2,3,4,5]Student, Dept of Computer Science & Engineering, BMIT, Solapur, Maharashtra, India

Submitted: 25-06-2021 Revised: 04-07-2021 Accepted: 07-07-2021

ABSTRACT—One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. Ciphertext policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue. Cipher text – Attribute Based Encryption scheme enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. It is proposed to use CP-ABE scheme to improve security and efficiency in attribute based multimedia data sharing. The proposed multimedia data sharing system includes Key Generation Center, Data Owner, Data User, Data Storing Center system entities that helps to share image securely using CP-ABE scheme. Here, specifically focus is on sharing image in '.jpg' format.

Keyword: Image Secure sharing Encryption Chaotic theory Linear independence

I. INTRODUCTION

Network and computing technology enables many people to easily share their data with others are using online external storages. People can share their lives with friends by uploading their private photos or messages into the online social networks; or upload highly sensitive personal health records (PHRs) into online data servers such as Microsoft Health Vault, Google Health for ease of sharing with their primary doctors or for cost saving. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified.Attribute based encryption (ABE) comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encryptor determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is more appropriate to the data sharing system because it puts the access policy decisions in the hands of the data owners [2], [3].

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information [4], [5], [9]. Thus, the key escrow problem is inherent such that the KGC can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. Chase and Chow [6] presented a distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system. Chow [7] proposed an anonymous private key generation protocol in identity-based literature such that the KGC can issue a private key to an authenticated user without knowing the list of users' identities Bethencourt et al. [4] and Boldyreva et al. [8] proposed first key revocation mechanisms in CP-ABE and KP-ABE settings, respectively. These schemes enable an attribute key revocation by encrypting the message to the attribute set with its validation time. It would be interesting to consider attribute-based encryption systems by applying advanced cryptosystem for data sharing. Proposed system should encrypt multimedia content i.e. images.

II. LITERATUREREVIEW:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1175-1179 www.ijaem.net ISSN: 2395-5252

In ref[10] paper they were used the algorithm of encoding technique to secure the medical documents such as patient details. But From a security point of view, even if it had worked in practice, this would have been a very weak encryption algorithm for two reasons. First, there is no secret key. Therefore, it is not a true encryption scheme, but an encoding scheme. Anyone who knows its operation method can easily recover the original text. Second, even if the operation method is unknown to an attacker or even if a secret key is introduced, the algorithm is a simple substitution cipher, which means that the same plain character will always be encrypted into the same cipher character under the same key. In[11] Block-Based Algorithm there are various technique used as follows Blowfish algorithm has best performance for the smallest image block size so it is not applicable for large images. It resulted in higher correlation and lower entropy .So they proposed new algorithm In that original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm and then the transformed image was encrypted using the Blowfish algorithm but for rearranging the images it take lot of time than the actual encryption of images. The algorithmswere commercially available, so they applied them on the ciphered image that resulted from applying the proposed algorithm on different block sizes of the original image using the proposed algorithm along With the other algorithms resulted in a better performance compared to using the other algorithms alone.

In ref[12] Steganography is the art of covering secret and confidential information within a carrier which could be an image file, video file or audio file. It was a technique which provides invisible communication since an image file which had the secret information embedded within it is delivered to the receiver instead of the secret information itself. It is a technique of protecting information by transforming into unreadable format called cipher text. Only those who possess a secret key can decrypt or decode the message into plain text.

In ref[13] they discussed the Particle swarm optimization (PSO) for image authentication and tamper proofing. This scheme provide solutions to the issues such as robustness, security and tamper detection with precise localization. The features were extracted in Daubechies4 wavelet transform domain with help of PSO to generate the image hash. This scheme was moderately robust against attacks and to detect and locate the tampered areas in an image. In this they were used Hash based techniques. Hash based techniques are differed from the watermark based techniques in an image authentication. An image hashing techniques are extract a set of features from the image to form a compact representation that can be used for authentication. The advantages of hash based techniques are no distortion is introduced in the image to be authenticated and content hash generated in frequency domain which has more robust to geometric distortions compared to their spatial domain counterparts

In [14] They used the techniques virtual private network (VPN), data encryption, and data embedding is being used for additional data protection in other fields of applications like financing, banking, and reservation systems. However, these techniques have not been systematically applied to medical imaging partly because of the lack of urgency until the recent HIPAA proposed requirements in patient data security. To overcome this drawback the Picture archiving and communications system (PACS) is an integrated management system for archiving and distributing medical image data was introduced. Communication of medical images in a PACS environment is usually over the internal hospital network that is protected by a firewall from outside intruders.

In[3] one policy is cipher text Policy Attribute Based Encryption (CP_ABE).for example primary health care center scenario for a patient attribute.The major drawback is key escrow problem. Advantage is to data owner can access easily with the patient details. In key generation center decryption carried out by private keys. In data sharing scenarios, attribute based methods are not highly suitable, since we can share only to the designated users.

Cloud over data privacy is achieved by using encryption techniques. The security of network is consisting of different approaches and techniques to achieve the data cryptographic security. The most commonly used method in recent time is Attribute-based encryption (ABE). If a user sends through the access request to the cloud, the cloud will return to the same cipher text data user, a user to decrypt the data using your private key. But this manner would lead to some problems: (1) to be able to encrypt data, the data owner needs to obtain the data user's public key to complete this; (2) a lot of storage overhead would spend because of the same plaintext with different public keys In order to overcome these limitations, and so forth, an attribute-based encryption (ABE).

III. OBJECTIVE

Objective of modern cryptosystem is not to provide perfect or risk-free security. Rather the objective of cryptography based system is to protect information resource by making unauthorized

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1175-1179 www.ijaem.net ISSN: 2395-5252

acquisition of the information or tempering with the information more costly than the potential value that might be gained. For well-designed and analysed cryptosystem with no known flaws, the primary defence against attack is the length of the encoding key.All cryptosystem with encoding key shorter than the plaintext message are subject to exhaustive search attack where the attacker tries all possible combination of keys until the key is found. Another objective of all information security system including cryptography based security system is to protect information resource at less cost than the value of the information that is being protected. A cryptography based security system must provide information security at acceptablecosts.

A. Problem Statement

To provide secure image sharing over the network by using Dynamic Key Generation technique that depends on system time.

.

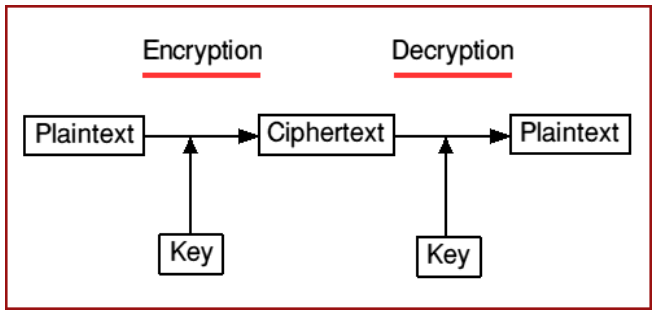
B. Project Idea

- We proposed a novel CP-ABE scheme for a secure data sharing system. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing center in the proposed scheme. The proposed system share image securely using CP-ABE scheme.

CRYPTOGRAPHY

Itisatechniqueofsecuringthecommunicationprocessfrom attackers. Cryptography is about using protocols that prevent attackers from accessing data, various aspects in information security such as data confidentiality, dataintegrity,authenticationandnon-repudiationarethebaseof the moderncryptography.

Fig-1: Cryptography



Cryptography includes different encryption and different decryptiontechniquesforencryptingand transferringdata [4]. Encryption techniques are of twotypes:

a) Symmetric: It uses the same key at the time of encrypting and decrypting the data. Eg. AES, DESetc.

b) Asymmetric: It uses different keys at the time of encrypting and decrypting the data. Eg. RSAetc.

In Symmetric encryption and decryption process, both the senderendandthereceiverendusethesamekeytoencrypt as well as decrypt data. In Asymmetric encryption and decryption process, both the sender end and receiver end usethedifferentkeyandthisproposestheconceptofusing public and private key in encryption and decryption phenomenon in the communication process. Receiver's publickeyisbroadcastedandavailabletoeveryoneanditis usedforencryptionbutthedecryptionoftheencryptedfile canbedoneonlyusingreceiver'sprivatekeywhichisonly known to the receiver.

PROPOSED SYSTEM

Theproposedsystemisdividedintostpesforbetterunderstanding.Beforegoingtoanyprocess ontheimagefirstwedividetheimageintousingsomecommandoralgorithmwewilldividethe imageintoJ*Jpartsi.e.(2*2,4*4)parts.Each parts of the image will be treated as a singleimage.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1175-1179 www.ijaem.net ISSN: 2395-5252

Figure1Original

FigureSplitedImages(4*4)

IV. CONCLUSION

Thisprojecthaspresentedforimageencryption usingAES256bitalgorithmforcryptography,imagesteganographyandimagesecurity.Astheimagetobesentisbrokendownintopartsandencryptedindividuallyandsentoverthenetworkitbecomesdifficultoftheintrudertogetaccessofalltheparts.Alsointrudercannotaccesstheencrypted ciphertextfrompartoftheimage.Thus wehaveincreasedthesecurityofanimagefor transmissionoveranetworkuptontimesorwe can increase2n number of timesinsteadof one ina singleinformationtransmission,morenumberof splited blocks means more secure information.

V. FUTURE WORK

- It can be used in different fields like private companies, different govt. organizations like aeronautical agencies, research and development organizations, intelligence agencies etc.
- In the future the levels of encryption process can be increased multiple times and also the technique used in steganography can be optimized and can be made muchbetter to make this research more versatile and agile.

REFERENCE

[1]. J.-M. Zhu and J.-F. Ma, “Improving Security and Efficiency in Attribute Based Data Sharing,” IEEE Transactions on knowledge and data engineering , vol. 25, no. 10, october 2013

[2]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application,” Proc. Int’l Workshop Information Security Applications (WISA ’09), pp. 309-323,

2009.

[3]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[4]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[5]. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. Int'l Symp. Inf