Security Enhancement in Cloud Storage using ARIA and Elgamal Algorithms

Navdeep Kaur
Research Scholar
Department of IT
CEC Landran, Mohali, Punjab

Heena Wadhwa
Assistant Professor
Department of CSE
CEC Landran, Mohali, Punjab

ABSTRACT

Cloud Computing is not an improvement, excluding an income towards constructs information technology services that utilize superior computational authority & better storage space utilization. The major centre of Cloud Computing starts when the supplier vision as irrelevant hardware associated to sustain down-time on some appliance in the system. It is not a modification in the user viewpoint. As well, the user software picture should be simply convertible as of one confuse to a new. Though cloud computing is embattled to offer better operation of possessions using virtualization method and to receive up a great deal of the job load from the customer and provides safety also. Cloud Computing is a rising technology with joint property and lower cost that relies on pay per use according to the client order. Due to its description, it may face plenty of intimidation and trouble in the scopes of safety. In this thesis, we are going to implement ARIA and ELGAMAL algorithm over a cloud network for securing cloud data storage structure. The whole simulation is taken place in Net environment.

Keywords

Cloud computing, multimedia data security, ElGamal Algorithm, Aria Cipher Algorithm, existing issues

1. INTRODUCTION

Cloud computing services can be used from varied and prevalent property, slightly than distant servers or confined equipment[7]. There is rejection in normal description of cloud compute. Normally it consists of a group of dispersed servers recognized as masters, given that require services & possessions to dissimilar clients recognized as customers in a system with scalability & dependability of datacenter.

Fig 1. Cloud Computing

The dispersed computers offer on requirement services. Examination may be of software possessions (e.g. software as a service, SaaS) or corporeal possessions (e.g. platform as a service, PaaS) or hardware/communications (e.g. hardware as a service, HaaS or communications as a Service, IaaS). Amazon EC2 (Amazon stretchy Compute Cloud) is a case of Cloud Computing examination [3]. The cloud does appear resolve some ancient issues with the still growing costs of apply, preserve, & supporting an IT communications that is rarely utilized everywhere near its ability in the single-owner atmosphere. There is a chance to amplify competence & reduce expenses in the IT section of the commerce & decision-makers are commencement to pay concentration. Vendors who can supply a protected, high-availability, scalable communications to the loads may be poised to be successful in receiving association to accept their cloud services[20].

Due to the current development in computer network technology, giving out of digital multimedia pleased through the internet is massive. Nonetheless, the augmented number of digital documents, compact disk processing tools, and the international ease of use of Internet access has created a very suitable medium for exclusive rights fraud and disobedient distribution of multimedia satisfied. A major condition now is to defend the scholar possessions of multimedia content in compact disk systems. There are numerals of data types that can be characterize as multimedia data types. These are characteristically the basics for the building blocks of general multimedia environments, platform, or integrate tools. The essential type can be defined as text, images, audio, video and Graphic objects. Multimedia finds its purpose in various areas including, but not limited to, announcements, art, education, entertainment, engineering, medicine, mathematics, commercial, scientific investigation and spatial temporal applications. Chiefly in Medicine, doctors can get qualified by looking at a virtual surgery or they can replicate how the human body is precious by diseases extend by viruses and microorganisms and then develop technique to prevent it [8].

1.1 Advantages and Disadvantages of Multimedia Data Security

1. Cost
2. Upgradable
3. Compatibility
4. Storage

1.2 Disadvantages

1. Expensive
2. Not always easy to configure
3. Requires Special Hardware
4. Not only Compatible

1.3 Security in the Cloud

The previous main issue at the same time as in the make unclear is that of security issues. Before adopt this expertise, you should know that you will be yielding all your company's sensitive in sequence to a third gathering obscure service source. This might potentially position your corporation to huge hazard. Therefore, you require making totally sure that you decide the mainly dependable service supplier, who will keep your in sequence completely protected [18].

2. RELATED WORK

Prof. Radha.S.Shirbhate, Anushree A.Yerawar, Ankur M. Hingane[2],2012, protection is essential for the defence of liberation of multimedia information. Thus this safety is only if by encryption. There are lots of encryption scheme are there for suspicious multimedia information. In this paper, they by means of discerning encryption for suspicious program information takes less computational workload & provides 5 levels of safety from stage 0 to stage 4. **K. Kalaivani & B. R. Sivakumar[3],2012,**This paper, deal with the a assortment of method connected to safety facet of Multimedia information, mainly the Medical information, their recompense & complexity. The primary part describe the aperture of multimedia information & its use in medicinal field. The moment part describes a diversity of method that can be sensible for universal Multimedia data. The third Part describes an assortment of method that can be applied to medicical imagery. The Fourth part describe obligation to get improved the safety of Medical information & the need of novel algorithm for calming the safety & excellence of medical information capture by dissimilar image capture strategy like ultrasonography , positron production tomography, single photon production computed tomography, visual imaging , computed tomography , X-ray, ultrasound, MRI etc. **Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande[4],2014,**In today's globe most of the announcement is done using electronic media. Data Security is extensively used to make sure security in announcement, data storage & program. Security of compact disk data is a very important issue since of fast evolution of digital data uses the variation step, taking from Data Encryption Standard algorithm. An imaginary analysis & investigational have a fight prove that this method provide high speed as well as fewer connections or transport over unsecured system. Multimedia information security is achieved by technique of cryptography, which contract with encryption of information. criterion symmetric algorithms proffer improved security for the multimedia information. **Raymond B. Wolfgang & Edward J. Delp[5],1998**, The increase of networked multimedia systems has created a need for the exclusive rights protection of digital images & video. Official document protection involves the verification of image content and/or ownership. This can be used to recognize illegal copies of an image. One move toward is to mark an image by adding an imperceptible structure known as a digital watermark to the image. Technique of incorporating such a watermark into digital images includes spatial domain techniques, convert domain algorithms & sub band filter approach. **LI Baoping 1, WANG Yan[6],2010,**The instruction method of using multimedia equipment's in class improve schooling quality & competence, accelerating teaching reform in universities & colleges. However, sometimes it even harms the education effect. By doing surveys in four academies in Jiaozuo, & analysing the advantages of using multimedia, this broadside points out the difficulties in current teaching method & offers some suggestions & countermeasures. Thus multimedia knowledge could wield its magnificent power in instruction.

3. IMPLEMENT ALGORITHM

3.1 ElGamal Algorithm

The security of ElGamal is based on the discrete logarithm problem. To encrypt and separately decrypt a message, a discrete power is executed. This procedure is efficient to compute. An enemy that seeks to decrypt an interrupted message may try to recover the private key. To this end a logarithm needs to be calculated. No actual method exists for this, given certain needs on the initial group are met. Under these conditions, the encryption is secure[4,16,8].

Now the ElGamal algorithm is used in many cryptographic products. The open-source software GnuPG uses ElGamal as standard for crosses. On behalf of this software and its difficulties with ElGamal discovered in late 2003 we will show the vital of correct implementation of cryptographic algorithms [14].

- Its security based on the complexity of the discrete logarithm problem and the CDH and DDH difficulties.
- Message growth: the cipher text is twice as big as the real message.
- Uses randomization, each message has many dissimilar possible cipher texts.

1. Public Key is (p; g; b=g a mod p) – p is a large arbitrary prime number such that DLP is infeasible in Zp – g is a producer g of the multiplicative group Zp * – a is an arbitrary integer in [1..p-2].
2. Private Key is a.
3. The cipher text of a M is (g^k mod p, Mb k mod p) – k is randomly chosen such that 0< k< p-2 [12].

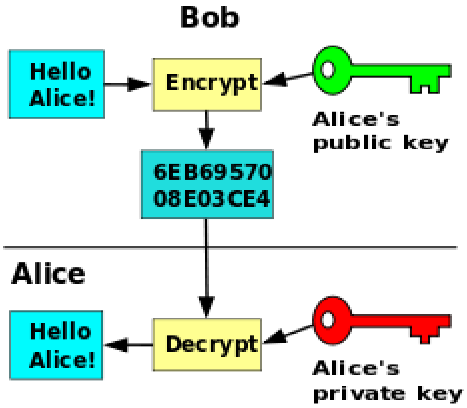


Fig 2: Public key Encryption

3.2 Aria Cipher Algorithm

ARIA is a block cipher with the following characteristics [21]:

- ARIA quarters key sizes of 128, 192, and 256 bits, and the block size is 128-bit long.
- ARIA uses a 16 × 16 evolutional binary matrix with maximum branch number of 8 as its diffusion layer.
- ARIA uses the same algorithm for encryption and decryption, taking advantage of its evolutional diffusion matrix.

- ARIA is designed to resist many known attacks on block ciphers, including differential cryptanalysis and linear cryptanalysis.
- ARIA is designed to be efficient both in software and hardware implementations [13,5].

ARIA is a SPN block cipher with 128-, 192-, and 256-bit keys. It processes 128- bit blocks, and the number of rounds is 12, 14, and 16, dependent on the key size of 128, 192, and 256 bits, individually. The ARIA algorithm can be measured as a series of operations done to 128-bit array called the state. The state is prepared as the plaintext input, and each operation in each round changes the state. The final value of the state is the output of the ARIA algorithm. Most of the processes of ARIA are byte-oriented, therefore occasionally the state is considered as an array of 16 bytes [4,1,2].

3.3 Proposed Algorithm

Input: File bytes N for encryption

Output: Encrypted file after process through Hybrid algorithm.

```
1.  Start
2.  Upload and extract file in bytes
3.  Init ElGamal Keys and ARIA encryption scheme
4.  Blocks=UploadedBytes.getBlocks();
5.  For I=0 to Number of blocks
6.  Process encryption for blocks
7.  Repeat till all blocks processed
8.  File.merge(Blocks)
9.  Key. Forward().toSmtp().
10. Stop.
```

The proposed algorithm works with two different algorithms to process a file over cloud storage. These two algorithm used to design a hybrid algorithm to enhance security in cloud computing. Elgamal algorithm is used to process key generation phase in this algorithm. It works with input bytes and generate two different keys for encrypt the file and authentication of users which decryption. In other hand ARIA algorithm is used to encrypt file bytes over a cloud server with the use of Elgamal key instead of their own. This process make the encryption scheme more secure than own structure. Hybrid processing probability is more secure than work with any single encryption technique. This structure divide the file into various small block and use threading technique to process them faster than process the whole file once in the system. Blocks are processed with the ARIA Hybrid algorithm and merge into a single file to store over a cloud server. At the time of decryption system ask their users to enter the private key to decode the bytes. Here the private used for two purposes one is for authentication and other is for decrypt the file with using hybrid scheme. The entered key extracted from the data and system merge original bytes into a single file as original file. The key sharing in this is done with the help of SMTP protocol due to remote login restrictions on internet.

4. EXISTING ISSUES

Security is the main limitation while storing data over cloud server. Various security threats in cloud computing are information loss, escape of information, customer‘s verification, Spiteful users treatment, Wrong practice of Cloud computing & its military, hijack of assembly while admission information, insider intimidation, foreigner spiteful attacks, information defeat, loss of organize, & examination disturbance. Therefore ornamental the safety for multimedia information storage room in an obscure centre is of supreme significance [16]. Just beginning such a structural design which ensures the consumer that its data is protected is the main purpose. To expand such a replica, a sufficient & nearby information of cloud computing has to be physically influential. Therefore the basic concept & preceding security method engaged in cloud computing have to be deliberate & unspoken. The method to amass information in the cloud is deliberate. A 3 tier structure is urbanized to enhance refuge while store multi-media records which comprise role base admission organize, encryption, & cross corroboration**.** The preceding work talk about only concerning the security majors but not concerning the encryption scheme [8]. The problem statement would comprise a primary & usual customer idea in which a main user would get a usual speed but the extended user would obtain additional bumper speed. The primary & the extended user would be decided. The signature in this scheme would also be a wave file bits. If the wave file bits of the uploaded sign would competition with the bits of uploaded data at scamper time, simply then the information would be downloaded. The proposed work will use encryption algorithms like ARIA & Key exchange algorithm use in Elgamal.

5. RESULT AND DISCUSSIONS

In this section discussed the result with respect to performance parameters i.e Encryption time, Decryption Time, Probability and accuracy.

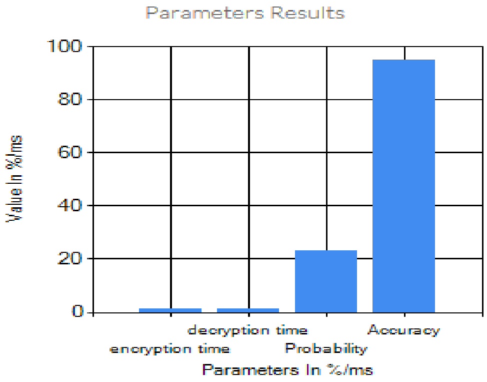
The result of proposed algorithm is compared with the existed one using various performance parameters like encryption time, decryption time, probability value, accuracy per frame. Using this hybrid algorithm time of encrypting and decrypting the multimedia get decreased as

comparison to the existed algorithm. We can see results in following graph:

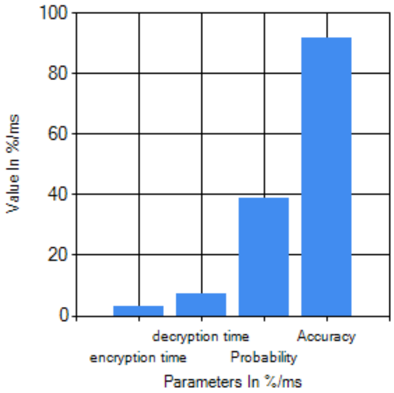
Table 1: Performance Parameters

Performance Parameters	Value /Units(MR Encryption)	Value/Units (Proposed)
Encryption Time	3ms	1ms
Decryption Time	7ms	1ms
Probability Value	39%	23%
Accuracy Per Frame	92%	95%

Various parameters which were used to find the performance of the proposed algorithm are shown in the above table. Some other graphical calculcations are also shown below.



(i)Performance Parameters With Mr Technique



(ii)Performance Parameters With Hybrid Technique

Fig no: 4 (i) and (ii) Comparison between performances parameters (proposed and existing)

The parameter table shows various parameters with their values for both MR technique and existing Hybrid algorithm. Here the values of proposed parameters show better results than the existing MR technique in all the cases for all parameters. there are various parameters to check the performance of these algorithms like Probability, Accuracy, Encryption time and decryption time. Probability value shows the security of any algorithm. Here the less probability shows less chance to get the original file in unauthorized way. here the proposed hybrid encryption scheme provide better results than existing as the probability is less than MR encryption. The other parameters used to measure time consumption of algorithm which is used for both encryption and decryption. Less time consumption shows the better performance of algorithm and high speed processing. The third parameter Accuracy is used to check the processed file is accurately extracted or not. In all these parameter values the proposed scheme shows better results as compared to existing MR technique.

6. CONCLUSION AND FUTURE SCOPE

Multimedia has turn out to be essential in every domain for its quality. On the other hand, due to the problems of handling peta-bytes of such kind of multimedia data in words of calculations, sharing, communications, as well as storage, there is a rising request of an substructure in the direction of having on-request admission towards a distributed group of configurable calculating assets (For instance, servers, linkages applications, stowage's, as well as facilities). Cloud computing is the latest uprising in IT industry which is fundamentally connected to the budget. Increase amount of data sharing has led to various loads balancing. We have presented a secure data exchange through key exchange algorithm using ARIA & Elgamal algorithm. We applied the scheme to secure data exchange. We projected Elgamal encryption comes up to for shielding information. This move towards decrease the computational workload. Selective encryption is the procedure of encrypting only parts of a multimedia satisfied. Since the computational workload is fewer. This results in command of cloud computing. Other than, due to a variety of safety problems during sharing of data, some faults occur. The future works include the implementation of the proposed system into Cross breed approach using Triple DES & Serpent Encryption algorithm, & implemented in mini PC act as small system.

7. REFERENCES

[1] Adjeroh, Donald A., & Kingsley C. Nwosu. "Multimedia database management—requirements & issues." IEEE multimedia 4.3 (1997): 24-33

[2] Anderson, Ross, Eli Biham, & Lars Knudsen. "Serpent: A proposal for the advanced encryption standard." NIST AES Proposal 174 (1998).

[3] Biswas, Rajorshi, Shibdas Bandyopadhyay, & Anirban Banerjee. "A fast implementation of the RSA algorithm using the GNU MP library." IIIT–Calcutta, National workshop on cryptography. 2003.

[4] Xu, Dingbang, & Peng Ning. "Privacy-preserving alert correlation: a concept hierarchy based approach." Computer Security Applications Conference, 21st Annual.2013.

[5] Cox, Ingemar J., et al. "Secure spread spectrum watermarking for multimedia." Image Processing, IEEE Transactions on 6.12 (1997): 1673-1687.

[6] Elbirt, Adam J., & Christof Paar. "An FPGA implementation & performance evaluation of the serpent block cipher." Proceedings of the 2000 ACM/SIGDA eighth international symposium on Field programmable gate arrays. ACM, 2000.

[7] Elgamal, Taher. "Method and apparatus for providing electronic accounts over a public network." U.S. Patent No. 6,138,107. 24 Oct. 2000.

[8] Islam, Mohammad Manzurul, Sarwar Morshed, & Parijat Goswami. "Cloud computing: A survey on its limitations & potential solutions." *International Journal of Computer Science Issues* 10, no. 4: 159-163.

[9] Kalaivani, K., & B. Sivakumar. "Survey on multimedia data security."International Journal of Modeling & Optimization 2.1 (2012): 36-41.

[10] Kawle, Pravin, et al. "Modified Advanced Encryption Standard.", International Journal of Soft Computing & Engineering, Volume-4, Issue-1, March 2014.

[11] Kiltz, Eike, and Krzysztof Pietrzak. "Leakage resilient elgamal encryption." In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 595-612. Springer Berlin Heidelberg, 2010.

[12] LI, Baoping, & Yan WANG. "Analysis of the Advantages & Disadvantages of Multimedia Teaching in Colleges.",2010.

[13] Li, Shenhua, and Chunyan Song. "Improved impossible differential cryptanalysis of ARIA." Information Security and Assurance, 2008. ISA 2008. International Conference on. IEEE, 2008.

[14] Li, Wei, Dawu Gu, and Juanru Li. "Differential fault analysis on the ARIA algorithm." *Information Sciences* 178, no. 19 (2008): 3727-3737.

[15] Menezes, Alfred J. Elliptic curve public key cryptosystems. Vol. 234. Springer Science & Business Media, 2012.

[16] Prof. Radha.S.Shirbhate, 2Anushree A.Yerawar, 3Ankur M. Hingane," Features Preserving Data Encryption Used to Secure Multimedia Data", International Journal of Emerging Technology & Advanced Engineering, Volume 2, Issue .1, January 2012.

[17] Schnorr, Claus Peter, and Markus Jakobsson. "Security of signed ElGamal encryption." In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 73-89. Springer Berlin Heidelberg, 2000.

[18] Shamily, P. Bindhu, and S. Durga. "A Review on Multimedia Cloud Computing, its Advantages and Challenges." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1.10 (2012): pp-130.

[19] Singh, Ajit, & Swati Malik. "Securing Data by Using Cryptography with Steganography." International Journal of Advanced Research in Computer Science & Software Engineering (IJARCSSE) ISSN 2277 (2013).

[20] Wolfgang, Raymond B., & Edward J. Delp III. "Overview of image security techniques with applications in multimedia systems." Voice, Video, & Data Communications. International Society for Optics & Photonics, 1998.

[21] Xu, Dingbang, & Peng Ning. "Privacy-preserving alert correlation: a concept hierarchy based approach." Computer Security Applications Conference, 21st Annual.2013.

[22] Yang, Sangwoon, Jinsub Park, and Younggap You. "The smallest ARIA module with 16-bit architecture." Information Security and Cryptology–ICISC 2006. Springer Berlin Heidelberg, 2006. 107-117.