A Protocol for Preventing Insider Attacks in Untrusted Infrastructure-as-a-Service Clouds

G.Revathi[#1],R.Sathiya[#2],Mrs. M.Kamarunisha, MCA.,M.Phil.,Ph.D., [#3]
Pg Scholar, Associate Professor &DSCASW College
Department of MCA &Dhanalakshmi Srinivasan College of Arts and Science for Women's- Perambalur, Tamilnadu, India
[1] revathimca97@gmail.com,[2]sathyadreamzpblr@gmail.com,[3]kamar6672@gmail.com

Abstract

Recent technical advances in utility computing have allowed small and medium sized businesses to move their applications to the cloud, to benefit from features such as auto-scaling and pay-as-you-go facilities. Before clouds ar wide adopted, there is a need to address privacy concerns of customer data outsourced to these platforms. In a practical approach for protecting the confidentiality and integrity of client data and computation from insider attacks such as cloud clients as well as from the Infrastructure-as-a-Service (IaaS) based cloud system administrator himself. We demonstrate a scenario of how the origin integrity and authenticity of health-care multimedia content processed on the cloud can be verified using digital watermarking in an isolated environment without revealing the watermark details to the cloud administrator. Finally to verify that our protocol does not compromise confidentiality and integrity of the client data and computation or degrade performance, we have tested a prototype system using two different approaches. Performance analysis of our implementation demonstrates that it adds negligible overhead.

Keywords: Network Security, Data mining, Consensus Rule, Cloud Computing, DDOS Attacts, IaaS

Introduction

In the encrypted domain (SPED) for privacy preserving has attracted considerable research interests in recent years. In cloud computing and delegated calculation, users who are unwilling to reveal contents of the original signal may send an encrypted copy to a remote server. The server has to accomplish signal processing in the encrypted domain. Many approaches have been proposed for different applications, for example, compressing encrypted images, signal transformation in cipher texts, pattern recognition in encrypted domain, watermarking in encrypted multimedia, data searching in encrypted dataset, etc. Reversible data hiding in encrypted images (RDH-EI) is another topic of SPED.

RDH-EI is useful in many applications. For example, in cloud storage as shown in a picture owner could store pictures within the cloud.. Before uploading the images, the owner encrypts the contents to preserve privacy. For management purposes, the cloud administrator can embed labels, such as user information, timestamps and remarks, into the cipher texts. Therefore, labels are attached inside these cipher texts, and storage overheads can be saved. The embedded information can also be extracted exactly by the administrator or authorized users. Meanwhile, when an authorized user downloads the encrypted image containing additional message from the cloud, RDH-EI protocol also guarantees that the original content can be lossless recovered after decryption.

Problem Definition

Cloud Computing is an exciting and promising new paradigm that allows clients to outsource storage and computational resources on demand. The wide adoption of cloud based services is badly suffering due to confidentiality and security concerns especially from insider attacks.

Proposed System

A protocol for secure launch of a client VM on a trusted cloud node. Other than secure launch, our second proposed protocol enables a client to protect the confidentiality and integrity of its data and computation from other client applications in the cloud and from the cloud system administrator. Here, verified the confidentiality and integrity security properties of our proposed protocols using the pro verifier automatic cryptographic protocol verifier.

Process

This project consists of 4 modules.

- File encryption using DES
- Hiding Data
- Transferring data
- Retrieving Data
- Redundancy evaluation
- Synchronization information and scrambling measure

File Encryption Using DES

The Data secret writing customary may be a block cipher, that means a science key and rule area unit applied to a block of knowledge at the same time instead of one bit at a time. To write a plaintext message, DES teams it into 64-bit blocks. The Data secret writing customary was once a predominant symmetric-key rule for the encryption of electronic knowledge. It was extremely prestigious within the advancement of contemporary cryptography within the educational world. Developed within the early Nineteen Seventies at IBM and supported an earlier style by crust Feistel, the rule was submitted to the National Bureau of Standards (NSB) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government knowledge. In 1976, when consultation with the National Security Agency (NSA), the NBS eventually chosen a rather changed version (strengthened against differential scientific discipline, however weakened against brute force attacks), which was printed as a politician Federal science customary (FIPS) for the us in 1977.The publication of AN NSA-approved secret writing customary at the same time resulted in its fast international adoption and widespread educational scrutiny. Controversies arose out of classified style parts, a comparatively short key length of the symmetric-key block cipher style, and also the involvement of the National Security Agency, nourishing suspicions about a backdoor.

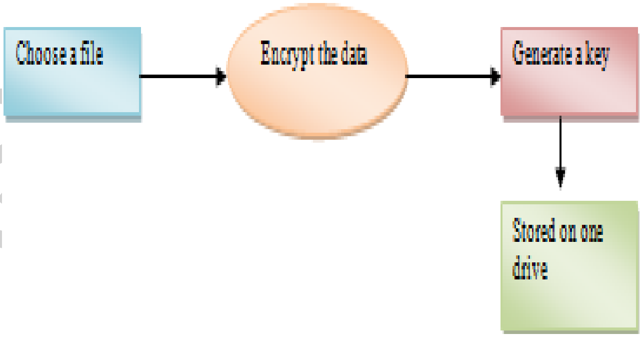


Fig 1 File encryption process

In 1976, when consultation with the National Security Agency (NSA), the NBS eventually chosen a rather changed version (strengthened against differential scientific discipline, however weakened against brute force attacks), which was printed as a politician Federal science customary (FIPS) for the us in 1977.The publication of AN NSA-approved secret writing customary at the same time resulted in its fast international adoption and widespread educational scrutiny. Controversies arose out of classified style parts, a comparatively short key length of the symmetric-key block cipher style, and also the involvement of the National Security Agency, nourishing suspicions about a backdoor.

The intense academic scrutiny the algorithm received over time led to the modern understanding of block ciphers and their cryptanalysis.DES is currently thought of to be insecure for several applications. This is mainly because of the 56-bit key size being too small; in Gregorian calendar month, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in22 hours and 15 minutes (see chronology).There also are some analytical results that demonstrate theoretical weaknesses within the cipher, though they're impracticable to mount in apply. The rule is believed to be much secure within the sort of Triple DES, though there area unit theoretical attacks. In recent years, the cipher has been outmoded by the Advanced secret writing customary (AES).Furthermore, DES has been withdrawn as a regular by the National Institute of Standards and Technology(formerly the National Bureau of Standards).

Hiding Data

This is process were the data can be hidden in a wave file for this the user as to provide two values one is the key file and the next is file data to hide. The data is hidden in another wave file with the combination of wave file, key file and hidden data file. These data are combined and stored in the output wave file.

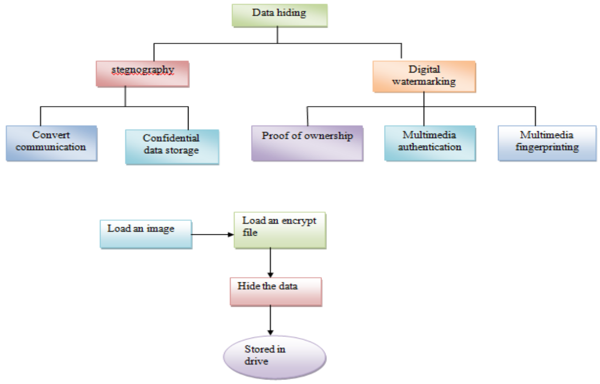


Fig 2 Hiding data

To hide the text we need two file one is the image and another one is the text contain file which text is to be hided in that particular image file. For that we have to mention the image file along with the correct path of the file and then we have to mention the text file which as to be hided in that image now the text has been hided in the image. Data concealment may be a package development technique specifically employed in object-oriented programming (OOP) to cover internal object details (data members). Data concealment ensures exclusive information access to category members and protects object integrity by preventing unplanned or supposed changes. Data concealment additionally reduces system quality for inflated hardiness by limiting interdependencies between package parts. Data concealment is additionally referred to as information encapsulation or info concealment.

Transferring data

Images are the most popular cover objects for steganography because of large amount of redundant bits which are suitable for data transmission on the Internet An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) JPEG is the most popular image file format on the Internet and the image sizes are small because of the compression, thus making it the least suspicious algorithm to use. The JPEG format uses a discrete cosine transform to image content transformation is a widely used tool for frequency transformation The working method of Steganography is discussed as follows. In order to compress a picture into JPEG format, the RGB colour representation is first converted to a YUV representation space and break up each colour plane into 8x 8 blocks of pixels In this representation the Y component corresponds to the luminance (or brightness) and the U and V components correspond to chrominance (or colour) The human eye is a lot of sensitive to changes within the brightness (luminance) of a picture element than to changes in its color. Thus it is possible to remove a lot of colour information from an image without losing a great deal of quality The fact is exploited by the JPEG compression by down sampling the color knowledge to scale back the dimensions of the file. The colour parts (U and V) square measure halved in horizontal and vertical directions, thus decreasing the file size by a factor of 2.The next step is that the actual transformation of the image.

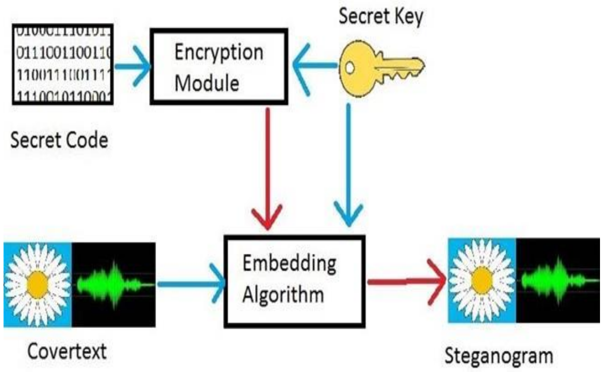


Fig 3 Transferring data

Retrieving Data

To retrieve the data we need that image file alone. Just we have to give the image with the full file path then just mention the file name in which we have to retrieve the data and the file path where we have to deliver the data. This is one of the more secured way to send a data without knowing the intruders that whether we are sending an image or a test so that will be no possibility that of loss of data or stealing of data. The application also adopts the more secured language as tool to execute the application process. This will be more helpful in the military point of view to send the data with more security than the normal encryption and decryption. Data retrieval means obtaining data from a database management system such as ODBMS. In this case, it is considered that data is represented in a structured way, and there is no ambiguity in data. In order to retrieve the required knowledge the user gift a collection of criteria by a question .Then the Database Management System (DBMS), software for managing databases, selects the demanded data from the database. The retrieved knowledge could also be keep in an exceedingly file, printed, or viewed on the screen. A query language, such as Structured Query Language (SQL), is used to prepare the queries.SQL is an yank National Standards Institute (ANSI) standardized command language developed specifically to jot down info queries. Each DBMS may have its own language, but most relational DBMSs also support SQL.

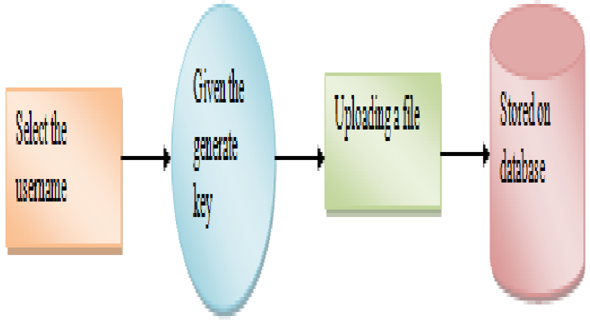


Fig 4 retrieving data

Redundancy Evaluation

The redundancy of uniform division is evaluated in keeping with the visual masking impact and brightness sensitivity of human sensory system. In this section, wavelet coefficients are processed to do redundancy evaluation, but not to be encoded. The calculation on self-contrast impact and neighborhood masking impact has been per the extended system of JPEG2000 for realizing heterogeneous division .The extended a part of JPEG2000 commonplace is consulted to pick parameter values within the 1st 2 steps. In the first step, self-contrast masking effect is taken into account. In the second step, the neighborhood masking effect is exploited to process the wavelet coefficients as the following:

Synchronization information and scrambling measure

Synchronization data is embedded into each code block before the key message. The first a part of the synchronization data may be a 2-bit flag that indicates whether or not a definite code block contains secret message. The flag can be set to “11” or “00,” that means “yes” or “no,” respectively. Only double zeros are to be embedded into a code block when it has too small hiding capacity to hold the synchronization information. The decoders are enlightened by the flag to relinquish up extracting from this code block. The second part of the synchronization information is a 12-bit fragment that indicates the length of the secret message embedded in this code block.

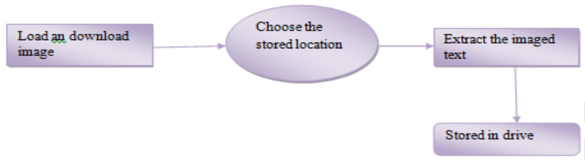
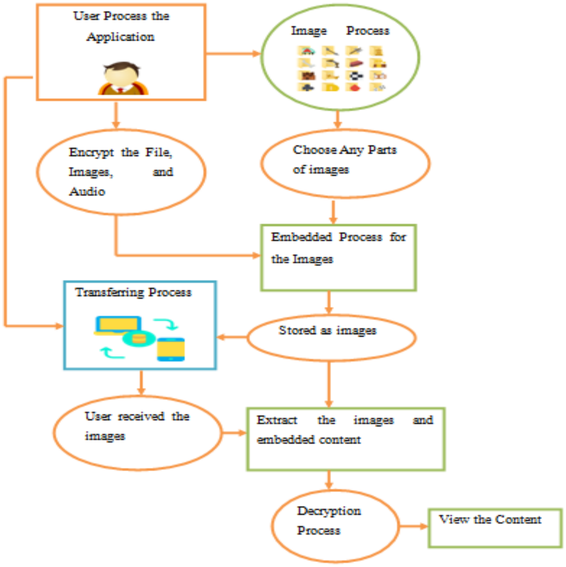


Fig 5 Synchronization process

Architecture Diagram



User Process the Application
Image Process
Encrypt the File, Images, and Audio
Choose Any Parts of images
Embedded Process for the Images
Transferring Process
Stored as images
User received the images
Extract the images and embedded content
Decryption Process
View the Content

Fig 6 Architecture Diagram

Conclusion

The developed stenographic tool is used to encrypt and decrypt the image. In this project, security to confidential data is achieved through multiple levels with the combination of both cryptographic and stenographic strategies. In the method of embedding info into the duvet image, a successful threshold strategy is used. A bit of information is inserted into a pixel only if the pixel satisfies threshold value and position constraint. The embedding image can be of any format (jpeg, pjg, gif, png). The generated stegno-image is in .png format because the image quality of this format is reasonable with the file size. All the operations are done with user-friendly interface. Any user, either a sender or receiver will operate the tool with none basic data simply by clicking a number of buttons.

References

[1] Z. Liu, L. Xu, C. Lin, J. Dai, and S. Liu, “Image encryption scheme by using iterative random phase encoding in gyrator transform domains,” Optics and Lasers in Engineering, vol. 49, no. 4, pp. 542–546, 2011.

[2] G. Zhang and Q. Liu, “A novel image encryption method based on total shuffling scheme,” Optics Communications, vol. 284, no. 12, pp. 2775 – 2780, 2011.

[3] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” Int. J. Bifurcat. and Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

[4] Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz and G.M. Bhat, “Data hiding in scrambled images: A new double layer security data hiding technique,” Computers and Electrical Engineering, vol. 40, pp. 70-82, 2014.

[5] Bala Krishnan Raghupathy, N. Rajesh Kumar and N.R. Raajan., “An Enhanced Bishop Tour Scheme for Information Hiding”. Internationa

Journal of Applied Engineering Research, Volume 9, Number 1(2014) pp: 145-151.

[6] D. Narasimhan et al., “An Improved Dual Enciphering Intrigue for Banking Process using Adaptive Huffmann Coding”, IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015,doi: 10.1109/ICECCT.2015.7226094.

[7] Y. Wu, S.S. Agaian, J.P. Noonan, “Sudoku Associated Two Dimensional Bijections for Image Scrambling,” arXiv:1207.5856, 2012. [8] Guosheng Gu and Jie Ling, “A fast image encryption method by using chaotic 3D cat maps,” Optik, vol.125, pp. 4700-4705, 2014.

[9] G. Manikandan, M. Kamarasan and N.Sairam, “A New Approach for Secure Data Transfer based on Wavelet Transform”, International Journal of Network Security, vol. 15,no. 1,pp. 88-94, Jan 2013.

[10] R. Zunino, “Fractal circuit layout for spatial de correlation of images,” Electronics Letters, vol. 34, no. 20, pp. 1929–1930, 1998.

BIOGRAPHICAL NOTES

	Mrs.Kamarunisha.M - Received M.C.A.,M.Phil.,Degree incomputer Science.She has 19 Years of Teaching Experience.She is Guided 7 Students in M.Phil.,She had Presented 8 Papers in International Conference and also She Presented 7 Papers in National Conference.She is Currently Working has Associate Professor in Department of Computer Applications in Dhanalakshmi Srinivasan College of Arts & Science for Women(Autonomous),Perambalur,TamilNadu,India.
	Ms.G.Revathi.,PG Scholar,[Department of Computer Applicatons],pursuing MCA in Dhanalakshmi Srinivasan College of Arts & Science for Women(Autonomous),Perambalur-621212,TamilNadu,(India).
	Ms.R.Sathya.,PG Scholar,[Department of Computer Applicatons],pursuing MCA in Dhanalakshmi Srinivasan College of Arts & Science for Women(Autonomous),Perambalur-621212,TamilNadu,(India).