ISSN 2395-1621

Implementation of Data Theft Detection and Prevention using Encryption and Steganography

[#1]Shraddha Veer, [#2]Prof. S. N. Shelke

[1]shraddhakveer@gmail.com
[2]santo.shelke@gmail.com

[#1]Department of Computer Engineering
[#2]Prof. Department of Computer Engineering

Savitribai Phule Pune University
SAOE, Pune.

ABSTRACT

The clouds contain large amounts of information and provide a variety of services to a large number of people. The benefits of cloud computing data leakage are reduced, decreasing the acquisition time tests, which eliminate or reduce downtime of the service, the Forensic provision, which reduce the transfer time evidence the main factor discussed is the security of cloud computing, which is a risk factor involved in major fields of computing. Our goal is to get the most security for the data on clouds, the application is Java-based application that will work in 4 input modules logon, and star mark and SMS alert, encryption Cryptographic and Image steganography using the AES algorithm. This will benefit the security of cloud computing, as user data will be approximately 100% sure, because this technique has the cryptographic encryption and encryption steganography Image too. Early data theft detection and prevention is what we want to achieve.

Keywords: AES algorithm, Cloud computing, Cryptography, Data theft, Steganography.

ARTICLE INFO

Article History

Received: 17th June 2017

Received in revised form :

17th June 2017

Accepted: 20th June 2017

Published online :

20th June 2017

I. INTRODUCTION

Now a day's security of data is important. As we know there are thefts, hackers, intruders who keep watch on our confidential data. So we have to keep our sensitive data secure. In this project, we are implementing a process to detect theft of confidential data using AES cryptography algorithm. Also we are trying to hide of important mails using pattern locking. We are trying to apply this kind of security process to our mail system. We are providing a dual login for user. If third party users try to access our personal mail then the owner of account will get mail and at the same time our system will get terminate.

The aim of Information security is to provide a defending mechanism to protect the data from unauthorized user. Some of the security aspects include increased thread of attack, availability number of resources, and emerging growth of computer network.

There exists two types of attacks are passive attack, active attack. The information security can be classified based on three aspects are Security Attacks, Security Mechanism, Security Service. Security Goal contains Confidentiality-content is known only to the sender and receiver, Integrity- correctness is maintained during transfer, and Availability-maximum availability of resources.

Observation:

According to the FBI and CSI, theft of proprietary information has been one of the leading causes of financial loss. Also 68% of these losses were due to insider threats, so the proposed system security of cloud computing, as user data will be approximately 100% sure, becaus e this technique has the cryptographic encryption and encryption steganography Image too. Early data theft detection and prevention is what we want to achieve.

II. LITERATURE SURVEY

Patel et al proposed a system based on the fuzzy inference that can be used to distinguish copying from other types of operations and filter false positives generated by the stochastic method forensic system. This paper describes a method to distinguish the copy of another type of access. Experiments have shown highly satisfactory results. Limitation of this system is, these operations can generate a lot of false positives in a system that is in regular use by the fact that these operations are commonly performed regularly by users.

Papadimitriou et al presented a model for the evaluation of the "guilt" of agents. They also present algorithms for distributing objects to agents, so that improves your chances of identifying a leaker. Finally, also consider the option of adding "false" objects to the distributed set. These objects do not correspond to actual entities, but they seem realistic to agents. In a sense, false objects act as a kind of watermark for the entire set, without modifying any individual members. If it turns out that an agent was given one or more fake objects that were leaked, then the distributor can be more confident that agent was guilty. In their paper they can identify the leaker of data but can`t prevent data theft.

John et al proposed a system called SIDSCC and explains its overall operation. Moreover, a comparison of the system to other relevant research in terms of modeling has been carried out. Then they have been carried out and discussed SIDSCC system using SaaS Cloud and IDS Server. They have also evaluated the system SIDSCC various perspectives; CPU, memory load, available bandwidth, latency, and filter destination fee.

Satarkar et al Decoys He said the legitimate user files are strategically placed in conspicuous places in their own file system, but there is no guarantee that fake user will surely play these files. So to overcome this limitation proposed system, which will generate in documents lure demand, if the user is suspected masquerader for behavioural profile. Any access to these documents lure is then considered as indicative of malicious activity insider

Winkelmann et al said that their objective in this paper is to review the literature on data protection and privacy in conjunction with Cloud technologies in order to establish a better understanding of the status of existent law in this environment as well as to provide an overview of problems regarding the topic discussed in recent academic publications. Limitation of their study is the lack of detailed investigation in relation to the imminent General Data Protection Regulation since the currently accessible information is rather vague.

III. PROPOSED SYSTEM

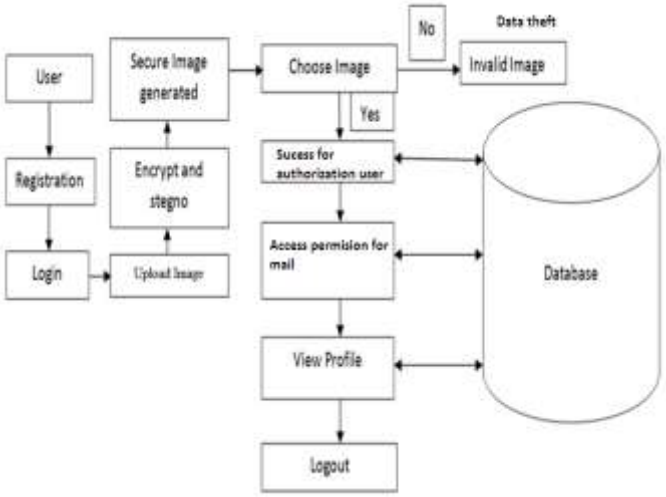

Fig 1. System architecture

We are building a java based platform project. In which our aim is to provide 100% Data security on cloud. This project will contain 4 modules.

1. Normal entry login.
2. Data Theft and Email Alert.
3. Cryptographic Encryption for private drive on cloud.
4. Image stenographic Encryption on that private folder.

Model Description:

We are building a java based platform project. In which our aim is to provide 100% Data security on cloud. This project will contain 4 modules.

1. Normal entry login.

Here user go through normal entry login without giving to the security access to the other user. If user give the access using YES/NO.

if give the YES- then it is security access mail to the other user.

if give the NO- then it is no security access mail to the other user, normal mode.

2. Data Theft and Email Alert.

Here user identified the theft if no any privacy access given to the mail then theft will not happen, if privacy access then theft will generated.

3. Cryptographic Encryption for private drive on cloud.

Here we apply the encryption for the personal data on storage the cloud.

4. Image stenographic Encryption on that private folder.

Here we apply the steganography for the uploaded images to personal data on storage the cloud.

IV. GOALS AND OBJECTIVES

Goals:

- Data security
- Privacy protection
- Personal and sensitive data stored
- Unauthorized user cannot access the data.

Objectives:

- Protect user data from unauthorized access, disclosure, modification, and monitoring.
- Prevent unauthorized access to cloud computing infrastructure resources.
- Protect from different attacks to mitigate end-user security vulnerabilities.
- Data Confidentiality
- Data Integrity

V. ALGORITHM

AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. We propose AES with 128 bit key length. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical.

AES performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP's.

- Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
- This algorithm has speedy key setup time and good key agility.
- It requires less memory for implementation, making it suitable for restricted-space environments.
- The structure has good potential for benefiting from instruction-level parallelism.
- There are no serious weak keys in AES.

AES Algorithm1:

Step1: import all packages.

Step2: Upload file

Step3: Method void doEncode(String infile)

Step4: FileInputStream inFile = new FileInputStream(infile);

int dot = infile.indexOf(".");
String encfile = infile.substring(0,dot)+".des";

// encrypted file

Step5: FileOutputStream outFile = new FileOutputStream(encfile);
// password to encrypt the file
String password = "sai";

Step6: Byte calculation
byte[] salt = new byte[8];
FileOutputStream saltOutFile = new FileOutputStream ("salt.enc");

saltOutFile.write(salt);
saltOutFile.close();

Step7: SecretKey secretKey = factory.generateSecret(keySpec);

SecretKey secret = new SecretKeySpec(secretKey.getEncoded(), "");

//file encryption

Step8: byte[] input = new byte[64];
int bytesRead;

while ((bytesRead = inFile.read(input)) != -1) {
byte[] output = cipher.update(input, 0, bytesRead);
if (output != null)
outFile.write(output);
}

Step9: byte[] output = cipher.doFinal();
if (output != null)
outFile.write(output);
Step10: File Encrypted;

Algorithm 2:

Step 1. Given a web P, extract its identity and generate features.

Step 2. Classify P by K-Means classifier and return result (+1, -1 or 0).

//+1: legitimate, -1: phishing, 0: suspicious

Step 3. If result=+1 or -1, output the phishing site,
If result=0, go to Step 4.

Step 4. If P has not a text input, output the phishing label (1).
If P has a text input, go to Step 5.

Step 5. Extract its webpage identity and generate features.

Step 6. Classify P by Navie Bayes classifier and output the phishing site.

Mathematical model:

Let us consider a set S where S={U,R,SER,D,S,A,P, SUCCESS,FAILURE,DD,NDD}
Where S is system which includes
U is The Set of System users, U= {U1,U2,U3-----,Un}
SER is the Server
R is the Set of Request , R={R1,R2.R3----,Rn }
D is The Database
S is the steganography Generation Parameter
A is the Admin Data
P is the Private Mail Access
SUCCESS – Desired OUTPUT Generated. i.e. Data theft can be detected.
FAILURE - Desired OUTPUT NOT Generated. i.e. Data theft cannot detected.

VI. APPLICATIONS

1. It helps in detecting whether the distributor's sensitive data has been leaked by the trustworthy or authorized agents.
2. It helps to identify the agents who leaked the data.
3. Reduces cybercrime.

VII.SOFTWARE REQUIREMENT SPECIFICATION

We have created system in java programing. Data is stored in mysql database. We have created a web application with local server. Web application that communicates with local server and Trustee Server using REST API. We have uploaded image on cloud, add profile, post comment, apply security, privacy on online social network.

VIII. RESULT

Table I. Show the result of the particular user on sending the mail

Sr no	User list	Mail send	Security
1	Shradaha	Securely transfer	Encryption apply
2	Seema	Not securely transfer	Encryption not apply
3	Akshay	Not securely transfer	Encryption not apply
4	Amol	Securely transfer	Encryption apply

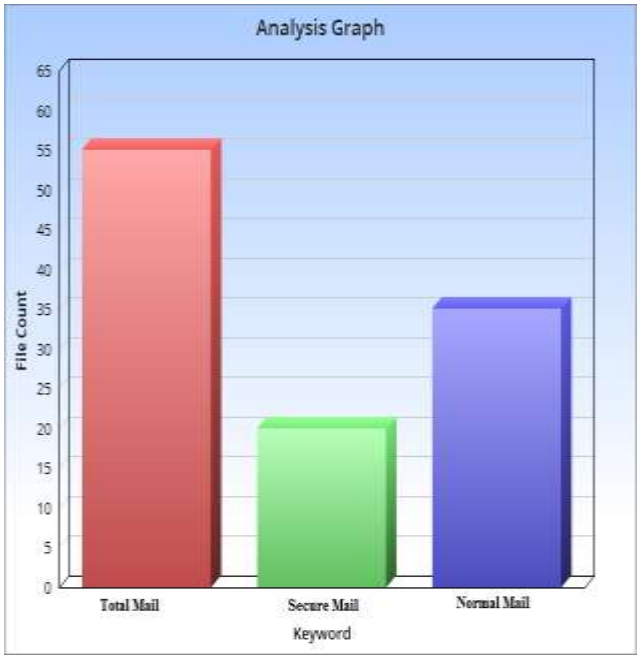

Fig 2. Calculate the no of mail with secure and normal

A result of our system suggests that, user can free from malicious data attackers and hackers. In each user registration into the cloud, he needs to mention a security image upload for his self security. After registration he can able to login into the cloud and upload many files into cloud. Once uploading process is completed, cloud also protects data by using encryption decryption methods. Users also take care of that data file by putting security access permission for each data file. This security access protects data from hackers.

In our proposed strategy in a three ways security is provided for each data file.

Those security ways are

- Security question from user
- Cloud computing encryption and without decryption

IX. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide **Prof. S. N. Shelke Sir** for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

X. CONCLUSION

The main objective of the proposed system is to find out who is trying to gain unauthorized access. We have provided an email with two logins, so that we can share if the log normal user without letting the user know about other important mail is necessary. We are also providing input stenographic hidden pattern and encryption of

private unit. We have proposed in advance data theft detection and prevention system (ADTDAPS), which will provide maximum data security. The approach is based on Java-based application and the standard AES algorithm, the cryptographic encryption and steganography image is being used to provide data security.

XI. FUTURE WORK

In future work we proposed system illustrates the work on various security issues available in online social networks. The future direction of the research will be modeling effective security algorithms to defend the security issues exist in online social networks.

REFRENCES

[1]Pratik C. Patel and Upasna Singh Detection of Data Theft using Fuzzy Inference System, IEEE International Advance Computing Conference (IACC)(2013)

[2]Panagiotis Papadimitriou and Hector Garcia-Molina,Data Leakage Detectio. IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 1, JANUARY 2014

[3]Robert John1, Maqbool Al Balushi2 and Saeed M. Alqahtani, An Intelligent Intrusion Detection System for Cloud Computing (SIDSCC) . International Conference on Computational Science and Computational Intelligence (2014)

[4]Kunal Madhukar Shirkande and Prof. Prajakta A. Satarkar Insider Data Theft Prevention System. International Journal of Scientific and Research Publications, Volume 5, Issue 7, July 2015

[5]Axel Winkelmann1, Thomas Buckel and Florian Pfarr3,Cloud Computing Data Protection – A Literature Review and Analysis. 47th Hawaii International Conference on System Science

[6]P.Jyothi, R.Anuradha and Dr.Y.Vijayalata Minimizing Internal Data Theft in Cloud Through Disinformation Attacks. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013.

[7] Yaser Ghanam, Jennifer Ferreira and Frank Maurer Emerging Issues & Challenges in Cloud Computing— A Hybrid Approach. Journal of Software Engineering and Applications, 2012, 5, 923-937.

[8] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "Computer crime and security survey," CSI/FBI, Tech. Rep., 2006.

[9] H. Kevin and H. L. Collier, Gale encyclopedia of small business, 2nd ed., H. Kevin and H. L. Collier, Eds. Farmington Hills, MI, USA: Gale Group/Thomson Learning, 2002.

[10] L. Yali, C. Cherita, C. Ken, A. Rennie, M. Biswanath, and G. Dipak, "SIDD: A framework for detecting sensitive data exfiltration by an insider attack," in Hawaii Int Conf Syst Sci, 2009, pp. 1–10.

[11] C. Harlan, Windows forensic analysis DVD Toolkit, 2nd ed. Syngress Publishing, 2009, p. 217.

[12] J. Grier, "Detecting data theft using stochastic forensics," Digital Investigation, vol. 8, Supplement, no. 0, pp. S71 – S77, 2011.

[13] P. C. Patel and U. Singh, "Detection of data theft using fuzzy inference system," in 3rd IEEE International Advance Computing Conference,
2013, pp. 694–699.

[14] K. Chow, Y. L. Frank, Y. K. Michael, and K. L. Pierre, "The rules of time on ntfs file system," in Proceedings of the second international workshop on systematic approaches to digital forensic engineering. Washington, DC, USA: IEEE Computer Society, 2007, pp. 71–85.

[15] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, pp. 338–353, 1965.

[16] T. J. Ross, Fuzzy Logic with Engineering Applications. John Wiley and sons, 2010.

[17] E. Mamdani and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," International Journal of Man-Machine Studies, vol. 7, pp. 1–13, 1975

