ISSN 2395-1621

Advance Data Theft Detection and Prevention System

[#1]Abhijeet Sawane, [#2]Sujit Tanpure, [#3]Prathamesh Padavekar

[1]abheejitbs@gmail.com
[2]sujittanpure77@gmail.com
[3]prathameshpadvekar@gmail.com

[#123]Department of Computer Engineering, University of Pune
TSSM"s Bhivarabai Sawant College of Engineering and Research, Pune, India

ABSTRACT

Cloud computing is basically an Internet-based formed by a large number of network servers - mostly based on open, modular and cost standards. 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, 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.

ARTICLE INFO

Article History

Received :3rd May 2016

Received in revised form :

5th May 2016

Accepted : 7th May 2016

Published online :

9th May 2016

Keywords— Cryptography, Steganography, AES algorithm.

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 OTP and at the same time our system will get terminate.

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

1.

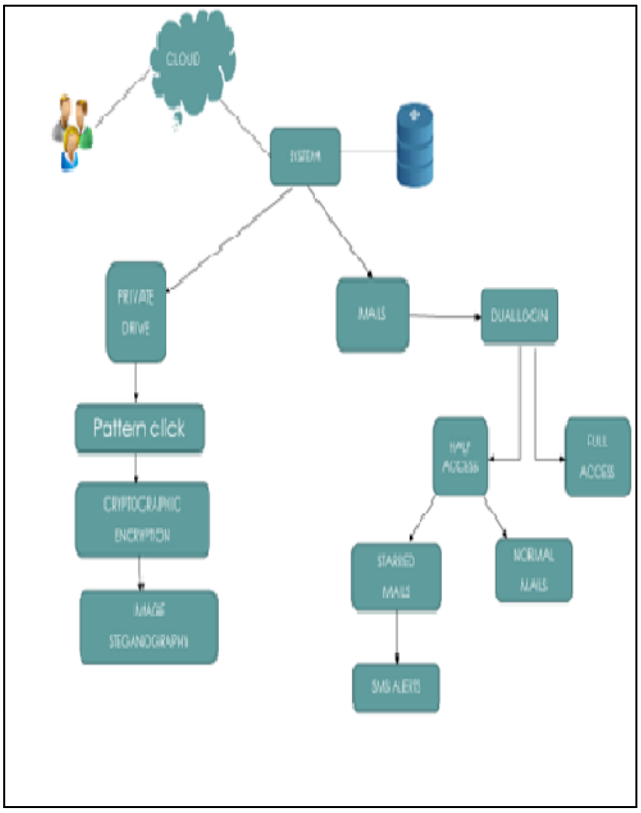


Fig. system architecture

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 module.

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

Here, User can login to his Account as Normal user id and password Login, And if incorrect password enterd then account holder get alerted by sms, suppose if unauthorized person login successfully, he only access normal mail and folder, But if he try to access stared mail or folder the user will get alerted and the account will be automatically signed out. Even if the hacker is successful in attempt for private drive he will prompt to upload image file, this file is nothing but the stenographic encryption on that folder in which cryptographic is hided. The half image is stored on server while it other image will stored on pen drive or mail and drive will wont access till the image get merged with server image. So in this way if even the hacker or unauthorized person is successful in breaking in , he/she won`t be able to access the private files of authorized user. Those the data theft will be detected and prevented 100%.

IV. ALGORITHMIC STEPS

Step 1: Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block.

Step 2: Initial Round
AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

Step 3: Rounds

i. Sub Bytes: it's substitution step where each byte is replaced with a subByte using s-box. S box is matrix given by rijndael.

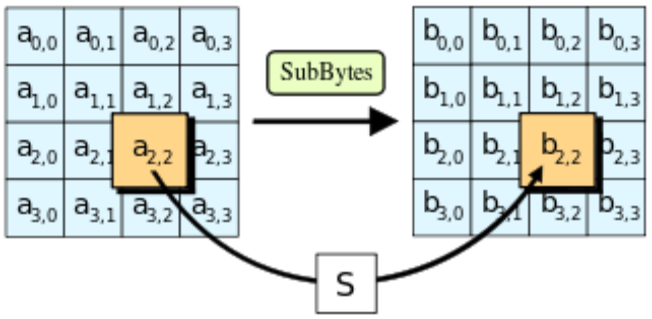
ii. Shift Rows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

iii. Mix Columns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.

iv. AddRoundKey

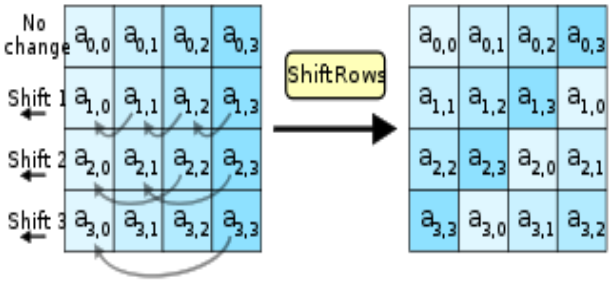
Step 4: Final Round (no Mix Columns)

i. Sub Bytes step: each byte in the state matrix is replaced with a Sub Byte using an 8-bit substitution box, the Rijndael S-box.



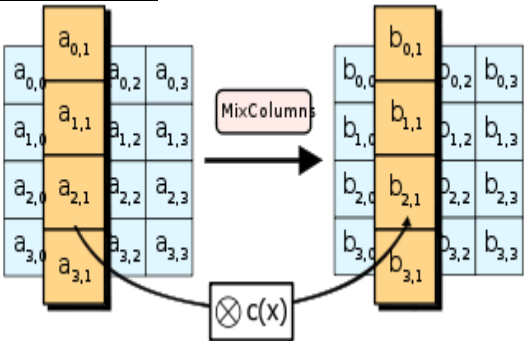
Sub Bytes

ii. Shift-row step: The first row is left unchanged. it cyclically shifts the bytes in each row.



Shift Rows

iii. Mix Column step: The four bytes of each column of the state are combined using an invertible linear transformation.



Mix Column

iv. AddRoundKey step: In the this step, the sub key is combined with the state. For each round, a sub key is derived from the main key using Rijndael's key schedule;

V. 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.
4.

VI. 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. Future studies can install this system in the cloud to improve data security in the cloud and we can possibly achieve high level security and privacy of data in the cloud.

ACKNOWLEDGEMENT

We express gratitude to our lead authorities such as University, The guide and the head of our Department Dr. N .B. Pokale in valuable guidance for the success of this project.

This research is developed for the completion of final year project for B.E. (Computer), Department of Computer Engineering, BSCOER, Pune.

REFRENCES

[1] Pratik C. Patel1 and Upasna Singh2," Detection of Data Theft using Fuzzy Inference System", IEEE International Advance Computing Conference (IACC)(2013)

[2] Panagiotis Papadimitriou1 and Hector Garcia-Molina2, "Data Leakage Detection". IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 1, JANUARY 2014

[3] Robert John1, Maqbool Al Balushi2 and Saeed M. Alqahtani3, "An Intelligent Intrusion Detection System for Cloud Computing (SIDSCC) ". International Conference on Computational Science and Computational Intelligence (2014)

[4] Kunal Madhukar Shirkande1 and Prof. Prajakta A. Satarkar2 "Insider Data Theft Prevention System ".International Journal of Scientific and Research Publications, Volume 5, Issue 7, July 2015

[5] Axel Winkelmann1, Thomas Buckel2 and Florian Pfarr3, "Cloud Computing Data Protection – A Literature Review and Analysis". 47th Hawaii International Conference on System Science

[6]P.Jyothi1, R.Anuradha2 and Dr.Y.Vijayalata3 "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 Ghanam1, Jennifer Ferreira2 and Frank Maurer3 "Emerging Issues & Challenges in Cloud Computing— A Hybrid Approach". Journal of Software Engineering and Applications, 2012, 5, 923-937

