ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Privacy Preservation of Sensitive Data Exposure by using ECC Algorithm

Uma Ashok Huljanti[1], Srinivasa Narasimha Kini[2]

M.E. Student, Department of Computer, Jayawantrao Sawant College of Engineering, Hadapsar, Pune, India[1]

Professors, Department of Computer, Jayawantrao Sawant College of Engineering, Hadapsar, Pune, India[2]

ABSTRACT: The openness of perceptive information in storage and transportation becomes a dangerous concern to organizational and individual security. Data leak detection has goal i.e. scanning contents of transmission process for opened perceptive information. There present numerous techniques to detect perceptive information leaks due to human mistakes and to provide alerts for organizations. To prevent data leak researchers have created privacy models same as k-anonymity. K-anonymity used to avoid node re-recognition by structure information. Screen content in storage and transportation is a general method for opened perceptive information. Screen content specifically requires the detection procedure addressed in security. But there is possibility of using this privacy method, an attacker able to breach security and figure out personal information in the case, group of nodes broadly contribute the similar perceptive labels. There is strong need to focus on data leakage and misuse in the case of data security. To overcome this problem author demonstrates privacy preserving data-leak detection (DLD)is robust technique for detection or avoidance of data leakage and misuse in the information security. The advantage of proposed method allows the data of user to securely representative the detection procedure to a semi honest provider while not revealing the perceptive data to the provider. In contribution we enhance bloom filter and encrypt data and hash using Elliptic Curve Cryptography (ECC).

KEYWORDS: Data leakage, Data misuse, Insiders, Network Security, Privacy.

I. INTRODUCTION

Now day's from the point of manual review the network movement can be very high [11]. To deal with such problems related to data leaks, must have set of strong methods. These new method must include data-leak detection and data restriction with it. Data in any organization is a vital and also plays a main role in organizations power and which must be preserved and maintained. On the other side, the data saved can be used for various processes in day to day work.

Information assignment systems [12] will increase the chances of distinguishing leakages. These methods are not depending on updating of related data. Author may introduce "realistic but fake" records of data to maximize the cases of detecting leakage and also finding the faulty party. A method based on content which is used for finding the data leakage is known as Fingerprinting. In fingerprinting, marks of private content are deleted and also managed with active content keeping final goal in mind for differentiating leakage of important content. User of data from the organization i.e. employees or partners does various methods on the information as well as they can have access to the vital data while using the information.

Because of the processing as well as action which can cause the data leakage and misuse. Due to the large use of pc's in company, the risk for security of data from insider's threat is becoming highly critical as well as communication system. There are various techniques are present for avoiding the attack on information from attacker. The methods available are not providing security of information from well-known users who may mishandle their privilege doing malevolent activities.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A. *Motivation*:

Increasing number of accidental data leak issues in organizational personal environments. Another motivation for our privacy-preserving DLD work is cloud computing, which provides a natural platform for conducting data-leak detection by cloud providers as an add on service. Data leakage is the greatest source of financial loss of organization. This issues motivated to us to present a privacy preserving data-leak detection (DLD) solution to solve the issue where a special set of sensitive data digests is used in detection.

II. RELATED WORK

In [2], author shows the new system called as Panorama to detect malware designed by authors. Proposed system automatically analyzes examples for malicious data acquire and procedure conducts due to its design. As perthe observation proposed system successfully finds each malware examples and had nominal wrong positives. The malware example comprises of a variety of various categories of malware, like key loggers, password sniffers, packet sniffers, stealth backdoors, root kits and spyware. Benefits of scene, yields few wrong negative and very less wrong positives. Good analysis is survived from particular performance down grading.

In [3], authors introduced a new mode called as Storages Capsules for protecting secret files on a PC. By encrypted file containers which allow an incorporated machine to safely analyze, revise perceptive records without being able to steal secret data by this idea of new system in motivated. By proposed scheme by separating the client's primary OS in a virtual system protection is provided. While it is getting to private information or documents, the Capsule framework turns off the primary OS's device output, and when it is finished revert its state. Primary point of preference of proposed systemis that they work with current application srunning on thing working operating system.

In [4], authors invented a new security framework called Aquifer used to avoid by mistake data exposure in latest OS by recognize ing the information mediatory issue as a growing burden for latest OSs and Application designers in Aquifer characterize protection margins that defend the whole user interface system explaining the user work. If a processis not part of the current UI workflow, Aquiferterminates the process. At the last author provide implementation of Aquifer concept and consolidate using Android operating system.

In [5], Privacy Oracle is utilized over an extensive variety of applications and information leaks. To discovering data releases new methodis proposed called Privacy Oracle system. System uses black-box fluff testing strategy and improvement is analysis of leaks of privatedata and search three various kinds of dataleaks these two fold contributions proposed by authors. Author discovers similar leaks basedon the various testing strategies in that changein the application inputs are outlined to changein the application outcomes.

In [6], author proposed the new framework Gyrus which monitors the user communications for general work like sending email, instant messaging, online social networking and online financial services. Gyrus uses propernature of applications by analyzing user intentionand meaning is that the Gyrusdeploysa "What You Send" (WYSIWYS) policy. Thisoffering comprise of two fold approach, firstthey capture the clients communications withan application and second they validate derived system outcome may be outlined back tothe users communications. Gyrus system is implementedon virtualization environment and efficiently prevents malware from forwarding unintentional data on the network. Advantages of proposed system are prevents malware from forwarding unexpected content on the network, problematic for further attack, extremely proficient and no postponement to the users.

In [7], author proposed novel tool named DeWare that is detection of malware. DeWare forces the dependencies among client actions and system work. This tool is used for detecting nfection carried by susceptible applications. Proposed system is utilized to give security for a PC, as well as for analyzing and calculating untrusted websites for forensicgoals. DeWare can be easy to install and use in Windows.

Data leak prevention (DLP) [13], is a suite of methodologies proposed for the loss of delicate data that happens in ventures over the globe.By concentrating on the area, classification and checking of data very still, being used and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

inmovement, this solution can go far in offering an enterprise getting an idea about what datait has, and in halting the various leaks of data that happen every day.

Possibilities of recognizing guilty agents is improved by the algorithms [14] deployed with false objects. Authors experimental results are said that the mitigating the sum objective will improve in guilty agents. Author has created anew system that creates false objects.

This paper [15] contains short concept behind the data leakage detection as well as technique to recognize person that leaks data. Infield of data extraction main issue is the dataleakage. In the past watermark technique is helpful to find out the data leakage with modification of data.

III. PROBLEM STATEMENT

A privacy preserving data-leak detection (DLD) solution to solve the issue where a special set of sensitive data digests is used in detection.

IV. PROPOSED ALGORITHM

A System Architecture

Data owner sends information to the clientsystem. While sending the data to client overthe network traffic attacker may attack theperceptive data surfing on the network to avoidthis type of leakage of sensitive data we areusing the Data Leak Detection system"(DLD).The exactly work of system is as follow:

Working:

1) User login to the system with proper user name, password and read input file. The input file can be in .txt, .pdf or can be of any format.
2) Apply bloom filter to given input file.
3) Encrypt data key using AES algorithm, also system will encrypt generated Hash using SHA as well as key using ECC algorithm.
4) After all the encryption sender forwards the encrypted data to the receiver system where receiver will display received files
5) On the receivers side receiver of the file decrypt the received file and generate it on hash using SHA algorithm and send the hash to DLD System for comparison
6) At DLD system it receive both sender and receiver hash. And compare both hash of sender and receiver if both hashes are matched then there is no leakage in data otherwise data leakage is there and the file is rejected.

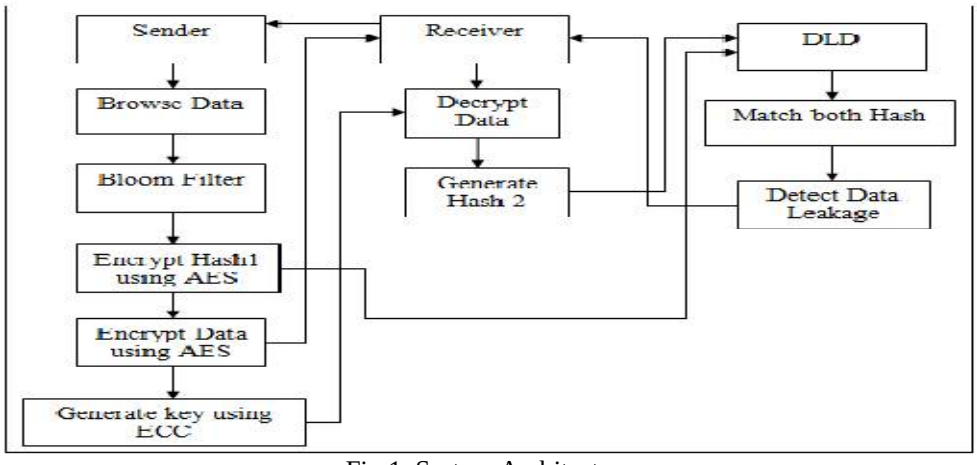


Fig.1. System Architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

B. Algorithms

Algorithm 1: AES Algorithm

1. Key Expansion: - Using Rijndael's key schedule Round keys are derived from the cipher key.
2. If DistanceToTree(u)> DistanceToTree(DCM) and First-Sending(u) then
3. Initial Round :- AddRoundKey where Each byte of the state is combined with the round key using bitwise xor.
4. Rounds

SubBytes : non-linear substitution step
ShiftRows : transposition step
MixColumns : mixing operation of each column. AddRoundKey
5. Final Round: It contain SubBytes, ShiftRows and AddRoundKey

Algorithm 2: ECC Algorithm

Key Generation
Key generation is a vital portion.In that both public key and private key generated. The sender encrypts the text with receiver's public key and the receiver decrypts its private key.
Now, select a number 'd' within the range of 'n'.

Following equation can develop the public key
Q=d*P
d = the random number which chose from the numbers (1 to n-1). P is the point on the curve. 'Q' is the public key and'd' is the private key.

Encryption
Let 'm' be the message that are forwarding. Demonstrates message on the curve by 'm'.
Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 - (n-1)].
Two cipher texts will be generated let it be C1 and C2.
C1 = k* P
C2 = m+k*QC1 and C2 will be sent.

Decryption
Have to get back the message 'm' that was send to us,
M=C2-d*C1
M is the original message that has sent.

Algorithm 3: SHA-256 Algorithm

Step 1: Append Padding Bits Message is "padded" with a 1 and as many 0's as necessary tobring the message length to 64 bits fewer than an even multiple of 512.

Step 2: Append Length 64 bits are appended to the end of the padded message. These bitshold the binary format of 64 bits indicating the length of the original message.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

C. Mathematical Model

At Data Owner:

1. Registration of Users (Data Owner/Receiver)

DO= {do1, do2, ... , don}
Where, DO is the set registered users. Sender is data owner who want to send thedata or receiver who want to receive original data.

At Sender:

Input

P1: Input Files

IF= {if1, if2,.... , ifn}
Where, IF is the set of all file, which are transmitted through network.

Process

P2: User Defined Key Generation

UK= {uk1, uk2,...., ukn}
Where, UK is the key generated by owner to encrypt the file

P3. File Encryption

EF= {ef1, ef2,...., efn}
After getting UK, the file to be send is encrypted. UK is used to encrypt the file.

P4. Hash Generation

H= {h1, h2,...., hn}
Where, H is the set of hash. For each file hash is generated.

P5. Hash Encryption

EH= {eh1, eh2,...., ehn}
Where, EH is the encrypted form of hash.Generated Hash is encrypted by using AES Algorithm.

P6. User Defined Key Encryption

EUK= {euk1, euk2,...., eukn}
Where, EUK is the encrypted form of user defined key.To increase the security, the key used for file encryption is also encrypted.For this purpose ECC algorithm is used.

P7. Send Encrypted Fingerprint to Receiver

EF= {ef1, ef2,...., efn}
Where, Encrypted fingerprint efn is sending to receiver Rn.Fingerprint contain the hash of original file.This will be used by DLD server to detect the data leakage in file.

P8. Send Encrypted File to receiver.

At DLD Server

P9. Receive Fingerprint from both sender and receiver

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

RF= {rf1, rf2,...., rfn}

P10. Data leakage detection

Compare generated hash with received hash of file.If Hash at receiver == Hash from senderData is not leaked
Else
Data is leaked

P11. Notify about status of file to actual receiver

Output O = {P1 ∪ P2 ∪ P3 ∪ P4 ∪ P5 ∪ P6 ∪ P7 ∪ P8 ∪ P9 ∪ P10 ∪ P11 }

D. Experimental Setup

Proposed system is built by using Java (VersionJDK 8) to implement the efficiency and effectiveness. The development tool kit used is Netbeans(Version 8). System minimum required is2GB RAM,Windows XP above. Minimum three systems are required for setup. One acts assender and another as a receiver and third is DLD System. DLD system canbe implemented on receiver side or separately on third system. DLD machine checks if data issecurely transferred or not. For secure transfer of data system uses ECC encryption technique.

V. RESULTS AND DISCUSSION

A. Dataset

All kind of files used as data set.

B. Result Set

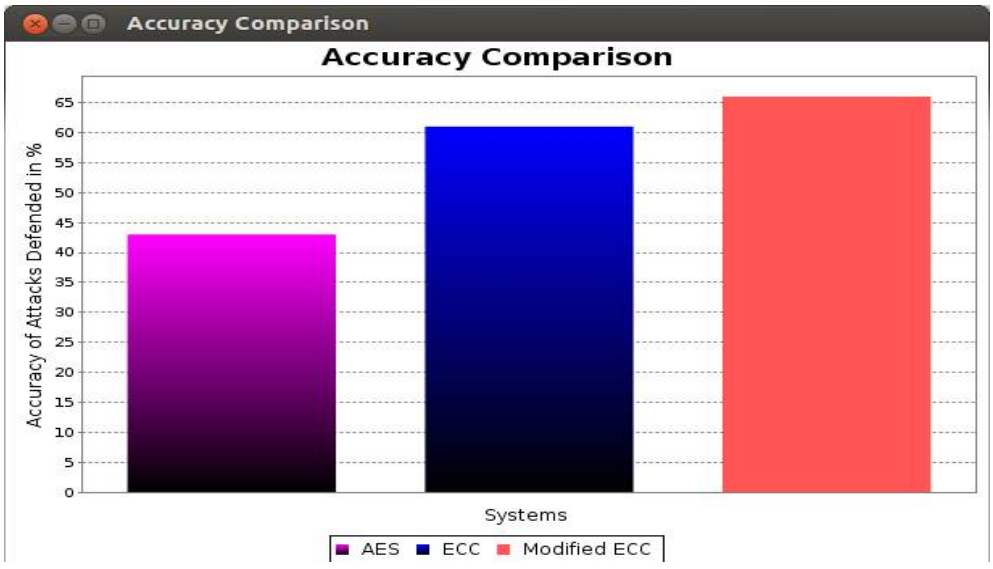


Fig.2..Accuracy Comparison Graph

Figure 2 show the accuracy comparison graph in which the accuracy of three methods are given i.e. using AES, ECC and modified ECC. From figure we can clearly see that using Modified ECC we can get a higher accuracy.

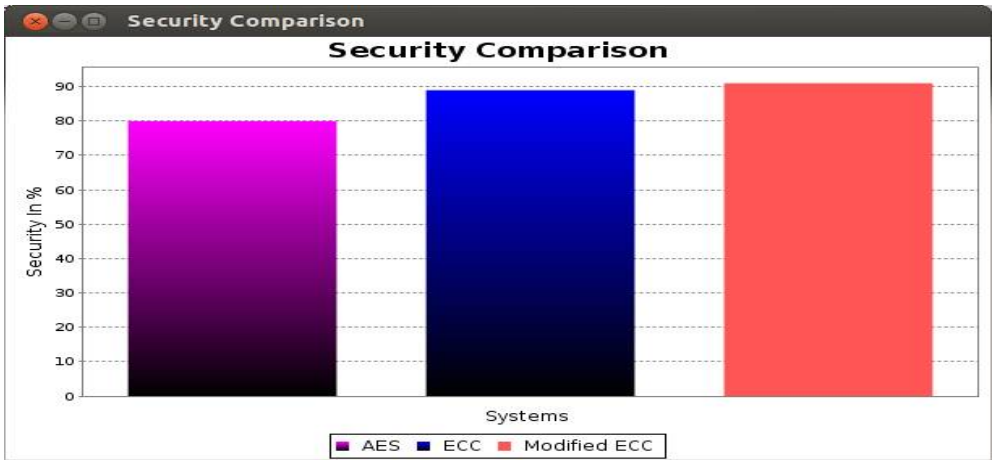
.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016



. Fig.3. Security Comparison Graph

Figure 3 shows the Security comparison graph for three different techniques those are AES, ECC, and Modified ECC from which we can clearly see that we will get higher security by using modified ECC.

C. Algorithmic Complexity

The algorithmic complexity will be the number of iterations that are required to classify an in-complete pattern object properly to the specific class.

VI. CONCLUSION AND FUTURE SCOPE

System present fuzzy fingerprint, a privacy-preserving data-leak detection model and proposedits realization. Using special digests, the exposure of the confidential data is kept to aminimum during the detection. We have handled extensive experiments to validate the accuracy,privacy, and effectiveness of our solutions. For future work, we plan to concentrateson designing a host-assisted mechanism for the complete data-leak detection for large-scaleorganizations. In contribution we enhance bloom filter and encrypt data and hash usingECC. Also provide the Semihonest data and make system secure. Also focus on designinga host-assisted mechanism for the complete data-leak detection.We can conclude that we have proposed the system which we feel should provide bettersecurity than the Existing Framework. However this requires to be developing furtherdeploying the proposed system and verifying the result with existing system.In future this system can be implemented on large scale on big organization level andsecurity can be improved using more enhance algorithms.

As a future scope we can make use of different algorithms to improve the security.

REFERENCES

1. Uma Ashok Huljanti, Dr.Srinivasa Narasimha Kini, “Survey on Privacy Preservation of Sensitive Data”, pp.1303- 1306
2. XiaokuiShu, Danfeng Yao, Member, IEEE, and Elisa Bertino, Fellow, IEEE, ”Privacy-Preserving Detection of Sensitive Data Exposure”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 5, MAY 2015.
3. H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, Panorama: Capturing system-wide information flow for malware detection and analysis, in Proc. 14th ACM Conf. Comput. Commun.Secur., 2007, pp. 116127.
4. K. Borders, E. V. Weele, B. Lau, and A. Prakash, Protecting confidential data on personal computers with storage capsules, in Proc. 18th USENIX Secur. Symp., 2009, pp. 367382.
5. A. Nadkarni and W. Enck, “Preventing accidental data disclosure in modern operating systems,” in Proc. 20th ACM Conf. Comput.Commun. Secur., 2013, pp. 10291042.
6. J. Jung, A. Sheth, B. Greenstein, D. Wetherall, G. Maganis, and T. Kohno, “Privacy oracle: A system for finding application leaks with black box differential testing,” in Proc. 15th ACM Conf. Comput.Commun. Secur., 2008, pp. 279- 288..
7. Y. Jang, S. P. Chung, B. D. Payne, and W. Lee, “Gyrus: A framework for user-intent monitoring of text-based networked applications,” in Proc. 23rd USENIX Secur. Symp., 2014, pp. 79-93.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

8. K. Xu, D. Yao, Q. Ma, and A. Crowell, "Detecting infection onset with behavior-based policies," in Proc. 5th Int. Conf. Netw. Syst. Secur., Sep. 2011, pp. 57-64..
9. X. Shu and D. Yao, "Data leak detection as a service," in Proc. 8th Int. Conf. Secur. Privacy Commun.Netw., 2012, pp. 222-240.
10. M. O. Rabin, "Fingerprinting by random polynomials," Dept. Math., Hebrew Univ. Jerusalem, Jerusalem, Israel, Tech. Rep. TR-15-81, 1981.
11. K. Borders and A. Prakash, "Quantifying information leaks in outbound web traffic," in Proc. 30th IEEE Symp.Secur.Privacy, May 2009, pp. 129□140.
12. Panagiotis Papadimitriou, Hector Garcia-Molina, "Data Leakage Detection", KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 1, JANUARY 2011.
13. Anthony P. Noble, Reza Kopaee, Adel Melek, Nirvik Nandy, "Data Leak Prevention", 2010.
14. Archana Vaidya, Prakash Lahange, Kiran More, Shefali Kachroo and Nivedita Pandey, "DATA LEAKAGE DETECTION," Vol. 3, Issue 1, pp. 315-321
15. MAMTA SINGH, PRITI TRIPATHI, RENUKA SINGH, "DETECTION OF DATA LEAKAGE", International Journal of Computer and Communication Technology, ISSN (PRINT): 0975 - 7449, Volume-4, Issue-3, 2013

.

BIOGRAPHY

Ms.Uma Ashok Huljanti, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She received her B.E (Information Technology) Degree from BIGCE Solapur. Solapur University Solapur, Maharashtra, India -413003. Her area of interest is cloud computing, network security.

Prof. Dr. Srinivasa Narasimha Kini, received his PhD Degree from Cochin University of Science and Technology, Thrikkakara, South Kalamasserry, Cochin**.** He received his M.E (Computer) Degree from B.M.S. College of Engineering, Basavanagudi, Bangalore, India. He received his B.E (Computer) Degree from K L E Society's College of Engineering Udyambaug Belgaum, India. He is currently working as Asst Prof (Computer) at Department of Computer Engineering, JayawantraoSawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is network security,Data Mining etc.