SECURE DATA TRANSFER USING GENERIC DATA LINEAGE FRAMEWORK & ACCOUNTABILITY MECHANISM

[1]T.Sathya , [2]K.Sudhadevi

[1] PG Student, Department of Computer Science& Engineering Vivekanandha Institute of Engineering & Technology for Women, Elayampalayam

[2]Assistant Professor, Department of Computer Science& Engineering Vivekanandha Institute of Engineering & Technology for Women, Elayampalayam

[1]tejusap1112@gmail.com

Abstract: Deliberate or Non deliberate leakage of the secret data information is a certainly one of the most severe security problems in the organization nowadays .Not only in the organization, it should be stretch to personal lives. The plenty of information are updated in smart phones and socialnetworks, this was the reason that mistakes was happened by humans. This information is obliquely transferred to third party and fourth party applications. For this introduce the Generic framework model (i.e.) Data lineage of LIME framework. By using this model, it consists of two roles: owner and consumer data flow across multiple entities. And also perform an additional role called auditor. Build and combine a new method of Accountable data transfer protocol with the framework. Finally applying the LIME framework and accountability mechanism to the data leakage scenarios.

Keywords: LIME framework, Accountable data transfer mechanism, robust watermarking, oblivious transfer.

1. INTRODUCTION

In the digital era, the Information is leaked through accidentally exposures by critical employees. The malicious external entities are the one of the most severe security threats to the organization. The individual person is also affected by data leakage due to social networks and smart phones.

For example, according to chronology of data leakage or breaches are governed by PRC (Privacy Rights Clearing house) in US suggested that 2008, 913, 049,623 records or documents have been breached. The problems that are explained here for the leakage in the environment.

- **Social Network:** The third party application widely used the online social websites or application such as the twitter,face book. Etc... By these the private details about the users can be leaked within advertise companies. It is not possible to analyze a particular application that should be a responsible for leakages.
- **Outsourcing**: The personal information is stored in Four smart phones that also breached. And the personal information has been threatened due to improper outsourcing. For these above problems there is no accountability mechanism are associated during data transfer.By introducing accountability data transfer protocol mechanism they detect the history of transmission data across multiple entities. These are also mentioned as data lineage or provenance. It is a framework model for securing the data from the leakage.

2. RELATED WORK

Michael Backes [1] et al., describe the problem of data leakage. The personal information is available in smart phones and social networks. By these the un-

authentication person can threaten theinformation & it should be leaked. For avoiding these he introduces the lime framework model for the data leakage.

P.Papadimitriou and H.Garcia- Molina [2] et al., suggest the model to define the data distributor has passed the data to the trusted agents (third parties). Sometimes the data are leaked unfortunately and it should be found in unauthorized place (somebody'slaptop).

F.Kelbert and A.Pretschner [3] et al., introduce the data usage control enforcement through the distributed system. And it requires the controlling & preserving the data while transfer. Protecting the intellectual property of multimedia authors & insiders. It describes the weakness of proofof ownership approaches [4]. Fingerprinting scheme identify the people from illegal redistributed copy of data [5]. J.J. Cox et al., proposed the method of multimedia data by Gaussian random vector & Geometric Transformation of watermarking technique that the originalimage areavailable and it can be watermarked before the transferring.

3. PROPOSED WORK

In the proposed work, formalize the problem of provable associating of theguilty party to the leakages and apply the methodology to solve the informationleakagesproblem.By demonstrating the LIMEframework knownthe details about that & how theyperform the operation in avoiding the data leakage.

3.1 LIME Framework:

LIME stands for the Lineage in Malicious Environment. It is a Generic Data lineage framework and they used for the data flow across multiple entities in the malicious environment.There are the three different principle roles that can be allocated to involved parties in time.

a) Data Owner

b) Data consumer

c) Data Auditor

These are the three main roles involved in the LIME framework model.

- **Data Owner**

Data Owner defines the responsibility for the management of documents. He transfers the documents to the authorizedconsumer.

- **Data Consumer**

It means receives the document & can carry out some task or operation.

- **Data Auditor**

It defines that they not involved in transfer of documents & he is only invoked, when a leakage occur and it perform steps to identify the leaker in the transferring process. The auditor just verify the link while leakage in the data transact

Transfer of data

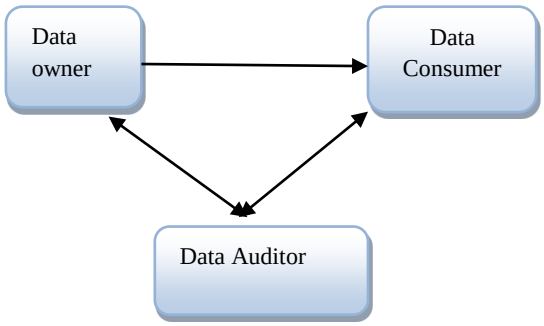

Figure 1: Roles of Framework

3.2 Framework Model:

- **Non – Repudiation**: The sending owner trust the receiving owner. He should take responsibilities if the data are leaked.

- **Fingerprinting:** When a document or record is transfer to the consumer then the sender embedded the information that is uniquely identifying a recipient.

4. WATERMARKING CONCEPT

It is a technique that is used to hide a small amount of digital data in a digital signal way. It also a logo or text on images should be help to prevent images from being copied or allow others to know where it was copied and who knows the rights. In nowdays it can be used in webpages also. Watermarking can be classified into many ways. That is digital watermarking; robust watermarking etc…it not only an images audio, video, film to show it is a copyrighted one by the owner of the object. The below diagram shows the transfer of document between owner and consumer. The auditor is an entity which only required when a leakage occurs. The auditor then constructs the data lineage by communicating with the involved parties. They can also use the fingerprinting between owner and consumer.

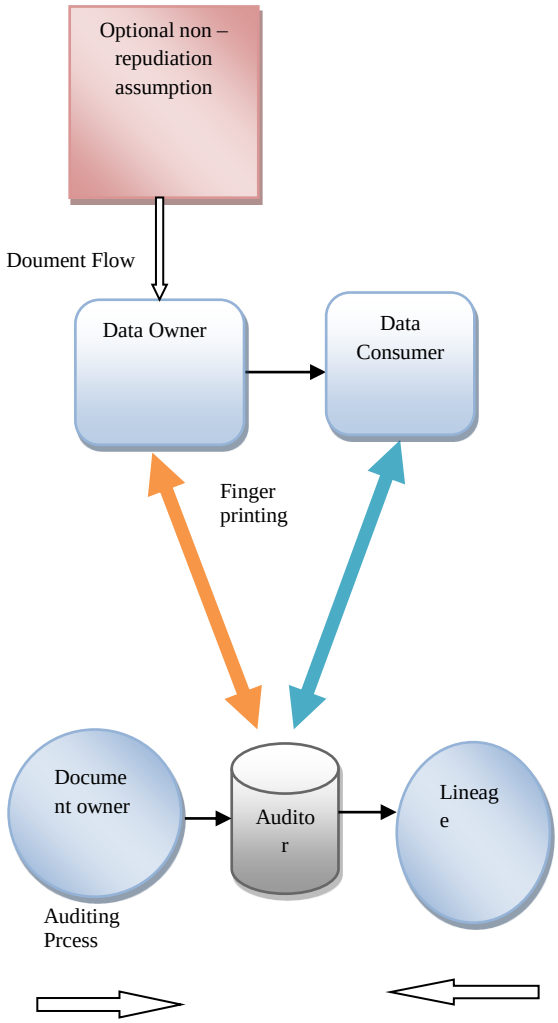

Figure 2: Framework of LIME

4.1 Objectives of Watermarking

- **Robust Watermarking:**

In a framework, the information should be embedded and it converts the identifiers to the document and it provides the consumers for data leakage. The embedding information does not affect the documents. This is called robust watermarking.

For example,

Two images consider as similar

P - Set of all possible documents.

WM_1 is corresponds to {0, 2} – is a set of watermarking.

K – Set of keys&S- Security parameter of watermarking.

- **Polynomial Algorithm of Symmetric Detecting Watermarking Scheme:**
  - A) P^1 = W(p,w,s) – Input of the o Probabilistic key Generation Algorithm:
    $GenKey^{WH1}$ (1^S) Outputs a key S belongs to K
  - B) Probabilistic Embedding Algorithm
    Original Documents p belongs to P^1

- **Oblivious Transfer:**

IntheObliviousTransfer, it candivide into two parties they are: Sender and Receiver.

They used for send message, and sender can encrypt the message & converts into ciphertext. So the receiver performs the function of decryption and allocates the fixed message size.

For Example,

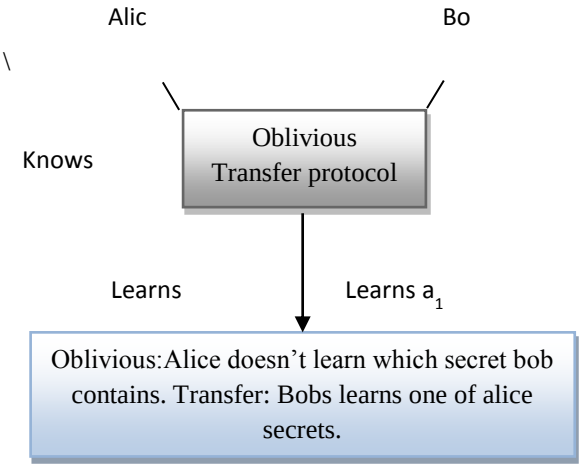

Figure 3: Oblivious Transfer

5. ACCOUNTABLE DATA TRANSFER PROTOCOL

Shanmugapriyan [6] et al., proposed the Accountable Data Transfer is the protocol used for the verifying the data transfer between two entities. It contain trusted sender & untrusted sender and they used for the embedding the information and it takes the role of auditor in the case of data leakage to perform the steps.

5.1 Trusted Sender:

In Trusted Sender of accountable data transfer the sender should be trusted so there is no need to necessary for any security mechanism.

Sender hold P, Recipient request P_w

$K = Gen\ Key^{WM}(1^K)$

$\sigma = (C_S, C_{R,}T)$

$P_W = W(P, \sigma, K)$ $\rightarrow$ $_P{}^W$ is an document of watermarking

5.2 Untrusted Sender:

The Untrusted sender means the prevention of sender documents from decoy or attack for that the document should be splited into n parts and each contain different watermarking versions. And the sender transfer by using oblivious transfer mechanism by the combination of result the recipient received it by probability method.

5.3 Generation of Data Lineage:

The following steps are to find the guiltyparty that the auditor precedes in the given way.

- **Step1**: The auditor takes the owner as the current suspect & he appends the current suspect to the lineage.
- **Step 2:** The auditor sends the leaked document to the owner and to provide the keys k1, K2 for the watermark scheme. If non blind watermarking scheme used the auditor additionally provides the unmarked version of document.
- **Step 3:** If suppose the keys k1, σ cannot be detected, it goes with step 8.
- **Step 4:**If the current suspect is trusted, the auditor checks the form σ ($Cs,C_{R,}$and T) where Cs is the identifier of current suspect. Takes the CRis current suspect.
- **Step 5**: The auditor verifies the form & and also verify the validity of signature.
- **Step 6:** The auditor splits the document into n parts for each one assign keys 0 & 1 .if none of these are detectable he allocates the detectable bit of itbit.
- **Step 7:** The auditor Cr to prove if suppose he produces the wrong form or signature he must be a current suspect. Then the auditor outputs the lineage.

6. CONCLUSION & FUTURE WORK

Eventually, a framework model of lime is applicable and it does not perfectly prevent the data leakage of the network. For that only the accountable data transfer should be introduced it will find the malicious entities occur in the transfer of data from sender to the receiver. It provides the various requirements such as oblivious transfer for documents privacy and it perform the honesty assumption methods for data transfer. In future research, motivate the technique based on encryption and the decryption algorithm for the data leakage problemin various documents and also they approaches for derived data. And it produces the key generation method for the secret key for sender andreceiver.

\

REFERENCES

[1] Michael Backs ,Data lineage in Malicious Environment in preceding of IEEE Transaction on secure Computing in CISPA Starland University.

[2] P. Papadimitriou and H. Garcia-Molina, "Data leakage detection," Knowledge and Data Engineering, IEEE Transactions on, vol. 23, no. 1, pp. 51–63, 2011.

[3] F. Kelbert and A. Pretschner, "Data usage control enforcement in distributed systems," in CODASPY, 2013, pp. 71–82.

[4] N. P. Sheppard, R. Safavi-Naini, and P. Ogunbona, "Secure multimedia authoring with dishonest collaborators," EURASIP J. Appl. SignalProcess., vol. 2004, pp. 2214–2223, 2004.

[5] B. Pfitzmann and M. Waidner, "Asymmetric fingerprinting for larger collusions," in Proceedings of the 4th ACM conference on Computerand communications security, ser. CCS '97, 1997, pp. 151–160.

[6] D. Shanmugapriyan and Murugaanandam, "Secured and Highly Reliable Data Transfer in MANET Using Position-Based Opportunistic Routing Protocol" International Journal of Innovations in Scientific and Engineering Research(IJISER) vol. 2014, pp. 1-5.

[7] I.J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Image Processing,

IEEETransactions on, vol. 6, no. 12, pp. 1673–1687, 1997.

[8] A.Mascher-Kampfer, H. Stogner, and A. Uhl, "Multiple re-watermarking scenarios," in Proceedings of the 13th InternationalConference on Systems, Signals, and Image Processing (IWSSIP 2006 Citeseer, 2006, pp. 53–56.

[9] G. S. Poh, "Design and Analysis of Fair Content Tracing Protocols," Ph.D. dissertation, 2009.

[10] R. Petrovic and B. Tehranchi, "Watermarking in an encrypted domain,"Jul. 7 2006, uS Patent App. 11/482,519.

[11] R. Anderson and C. Manifavas, "Chameleon - A new kind of stream cipher," in Fast Software Encryption. Springer, 1997, pp. 107–113.

[12] A.-R. Sadeghi, "Secure fingerprinting on sound foundations," Ph.D. dissertation, 2004.

[13] J. Domingo-Ferrer, "Anonymous fingerprinting based on committed oblivious transfer," in Public Key Cryptography. Springer, 1999, pp. 43–52.

[14] A.-R. Sadeghi, "How to break a semi-anonymous fingerprinting scheme," in Information Hiding. Springer, 2001, pp. 384–394.

[15] J. Domingo-Ferrer and J. Herrera-Joancomart´ı, "Efficient smart-card based anonymous fingerprinting," in Smart Card Research andApplications. Springer, 2000, pp. 221–228.

[16] D. Hu and Q. Li, "Asymmetric fingerprinting based on 1-out-of-n oblivious transfer," Communications Letters, IEEE, vol. 14, no. 5, pp. 453–455, 2010.

[17] R. Parviainen and P. Parnes, "Large scale distributed watermarking of multicast media through encryption," in Proceedings of the IFIPTC6/TC11 International Conference on Communications andMultimedia Security Issues of the New Century, vol. 192, 2001, pp. 149–158.

[18] A. Adelsbach, U. Huber, and A.-R.Sadeghi, "Fingercasting – Joint Fingerprinting and Decryption of Broadcast Messages," T. Data Hidingand Multimedia Security, vol. 2, pp. 1–34, 2007.

[19] S. Katzenbeisser, B. Skoric, M. U. Celik, and A.-R.Sadeghi, "Combining Tardos Fingerprinting Codes and Fingercasting," in Information Hiding, 2007, pp. 294–310

[20] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in International Conference on IndustrialInformatics, 2005. INDIN'05.2005 3rd IEEE. IEEE, 2005, pp. 709–716.

[21] G. Do¨err and J.-L.Dugelay, "A guide tour of video watermarking," Signal processing: Image communication, vol. 18, no. 4, pp. 263–282, 2003.

[22] M. A. Alsalami and M. M. Al-Akaidi, "Digital audio watermarking: survey," School of Engineering and Technology, De Montfort University,UK, 2003.

[23] R. Halder, S. Pal, and A. Cortesi, "Watermarking techniques for relational databases: Survey, classification and comparison," Journal ofUniversal Computer Science, vol. 16, no. 21, pp. 3164–3190, 2010.

[24] J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," Proceedings of the IEEE,vol. 87, no. 7, pp. 1181–1196, 1999.

[25] M. J. Atallah, V. Raskin, C. Hempelmann, M. Karahan, R. Sion,U. Topkara, and K. E. Triezenberg, "Natural Language Watermarking and Tamperproofing," in Information Hiding, 2002, pp. 196–212.

[26] J.-P. M. Linnartz and M. Van Dijk, "Analysis of the sensitivity attack against electronic

watermarks in images," in Information Hiding.Springer, 1998, pp. 258–272

[27] Y. Wu and R. H. Deng, "A Pollution Attack to Public-key WatermarkingSchemes," in Multimedia and Expo (ICME), 2012 IEEE InternationalConference on. IEEE, 2012, pp. 230–235.

[28] A.-R. Sadeghi, "The Marriage of Cryptography and Watermarking –Beneficial and Challenging for Secure Watermarking and Detection," in Proceedings of the 6th International Workshop on DigitalWatermarking, ser. IWDW '07, 2008, pp. 2–18.

[29] W. Zhou, X. Zhang, and X. Jiang, "Appink: watermarking android appsfor repackaging deterrence," in Proceedings of the 8th ACM SIGSACsymposium on Information, computer and communications security. ACM, 2013, pp. 1–12.