Secure and Reliable Data Transfer across Multiple Entities by Using LIME

B. Sneha
M.Tech
CSE Department
Anurag Group of Institutions
Village Venkatapur
Mandal Ghatkesar
Dist Medchal, Telangana, India.
bsnehareddy888@gmail.com

N. Swapna Goud
Assistant Professor
CSE Department
Anurag Group of Institutions
Village Venkatapur
Mandal Ghatkesar
Dist Medchal, Telangana, India.
swapnagoudcse@cvsr.ac.in

G. Vishnu Murthy
Professor and HOD
CSE Department
Anurag Group of Institutions
Village Venkatapur
Mandal Ghatkesar
Dist Medchal, Telangana, India.
hodcse@cvsr.ac.in

Abstract— A data distributor has given precise data to a set of evidently trusted agents. Some of the data are leaked and found in an unjustified place. The distributor must assess the probability that the splitted data came from one or more agents, as opposed to having been individually collected by others. We suggest data allocation techniques which can enhance the chance of identifying split. These strategies do not build on changes of the outsourced data. While sending data through the network there is a lot of dishonest user looking to hack useful data. A proper security should be provided to data which is send to network. To avoid this data leakage, we used the data lineage mechanism. We develop and analyze novel accountable data transfer protocol between two entities within a malicious environment by building upon oblivious transfer and robust Watermarking.

Keywords: *Oblivious Transfer, Watermarking, Data Lineage*

*****

1. INTRODUCTION

Data Lineage gives a visible representation to decide the records go with the flow/movement from its origin to destination through specific changes and lops on its manner inside the organization history. Data lineage represents: how the records lops among special data factors, how the data gets converted along the way, how the illustration and parameters alternate, and the way the data splits or converges after every hop. Easier representation of the Data Lineage can be proven with dots and features, in which dot represents a data box for data point and a line connecting them represents the transformation the data factor under goes, between the data containers. Representation of data lineage extensively relies upon on scope of the Metadata Management and reference point of hobby. Data Lineage gives basis of the data in addition to intermediate data glide hops from the reference point with diffident records lineage, ends in the final destination information factors and its intermediate information flows with Forward information lineage. These views may be merged with end-to-end Lineage for a reference factor that gives whole audit trail of that records factor of interest from source to its destination. As the information factors or hops will increase, the complexity of such representation turns into incomprehensible. Thus, the quality function of the information lineage view would be able to simplify the view by way of briefly masking undesirable peripheral data points. A device that has asking characteristic enables scalability of the view and complements analysis with satisfactory consumer enjoy for each technical and enterprise users alike. Scope of the data lineage determines the quantity of metadata required to symbolize its data lineage. Usually, Data Governance, and Data Management determines the scope of the information lineage based on their regulations, employer records control approach, information impact, reporting attributes, and critical records factors of the agency. Data Lineage affords the audit path of the records factors at the bottom granular stage, but presentation of the lineage may be finished at various burn stages to simplify the enormous data, much like the analytic web maps. Data Lineage may be visualized at various ranges based on the granularity of the view. At a very high level data lineage provides what systems the data interacts before it reaches vacation spot. As the granularity increases it goes as much as the data point degree wherein it can provide the info of the records point and its ancient conduct, attribute homes, and tendencies and Data Quality of the records passed through that precise information point within the data lineage. Data Governance plays a key function in metadata management for guidelines, strategies, regulations, implementations. Data Quality and Master Data Management helps in enriching the data lineage with more business cost. Even though the very last illustration of Data lineage is provided in a single interface however the manner the metadata is harvested and uncovered to the data lineage User Interface (UI) can be absolutely specific. Thus, Data lineage is categorized into 3 classes based on the way of metadata is gathered: Data lineage regarding software applications for based records, Programming Languages, and Big Data. Data lineage expects to view as a minimum the technical metadata involving the records points and its various differences. Along with technical information, Data Lineage can also improve the metadata with their corresponding Data Quality results, Reference Data values, Data Models, Business Vocabulary, People, Programs, & Systems related to the records factors and improvements. Masking feature within the records lineage visualization lets in the equipment to contain all the enrichments that rely for the precise use case.

2. RELATED WORK

Ana Charpentier, Caroline Fontaine, Teddy Furon, Ingemar Cox proposed the first asymmetric fingerprinting protocol dedicated to Tardos codes. The construction of the fingerprints and their embedding with in pieces of Work do not need a trusted third party. In particular, they anticipate that some form of secure multi-party computation can be applied. The authors considered two forms of oblivious transfer protocols, the first based on traditional cryptographic techniques and the second based on less well known Commutative Encryption or Two-Lock crypto-systems. These later techniques are less mature than traditional Oblivious Transfer protocols in terms of security, but offers interesting properties that are convenient to our application. Further work is needed to improve their semantic security, so that their advantages do not come at the cost of decreased security.

Munkhbaatar Doyoddorj and Kyung-Hyune Rhee introduced design and analysis of a fragile watermarking scheme with tampering localization and recovery mechanism. The focus of their analysis is on characteristics of watermark detector as well as distinguishes its property such as fragility against robustness measure. In order to design effective watermarking scheme, authors analyzed the characteristics of our scheme by defining the characterization mode. This proposed scheme utilized the block-mapping strategy to identify the tampered region by generating the random indexing block sequence. By using this technique, we can detect any modifications made to the image and indicate the specific locations where the modification was made.

JosepDomingo-Ferrer presented the first construction for anonymous fingerprinting which is completely specified from a computational point of view and it is readily implementable. Unlike previous proposals, the proposed construction relies only on computationally well-defined primitives. By properly tuning its security parameters, good consumer and producer protection can be attained. In addition, if combined with smart cards for fingerprinting on the consumer's side, the construction also provides protection against collusions.

3. FRAMEWORK

A. Proposed System Framework

While transferring the data, the data leakage may occurred then to overcome this data leakage problem in this paper we propose a simplified model named as LIME (Lineage in the Malicious Environment) framework. This proposed LIME framework allows us to define the exact properties that our transfer protocol has to fulfill in order to allow a provable identification of the guilty party in case of data leakage.

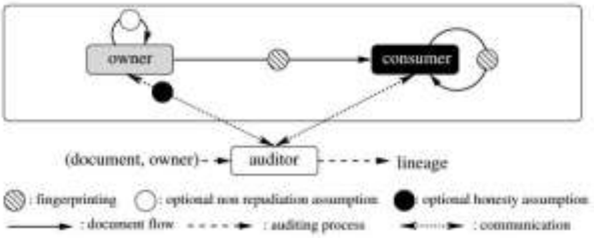


Fig1. LIME Framework

In this LIME framework we are using two techniques such as;

1. Watermarking
2. Oblivious Transfer

Watermarking

A watermarking scheme can be defined with two functions, the embedding or marking function and the extraction or verification function. Roughly speaking, the marking function takes an image as an input together with the mark to be embedded and produces the marked image. On the other side, the verification function takes the marked image and gives the mark embedded in the image.

Oblivious Transfer:

In cryptography, an oblivious transfer (OT) protocol is a type of protocol in which a sender transfers one of potentially many parts of data to a receiver, but remainder insensible as to what piece (if any) has been moved.

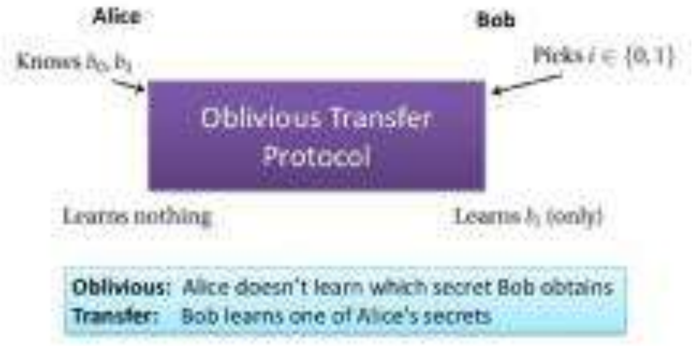

Alice
Bob
Knows b_0, b_1
Picks $i \in \{0,1\}$
Oblivious Transfer Protocol
Learns nothing
Learns b_i (only)
Oblivious: Alice doesn't learn which secret Bob obtains
Transfer: Bob learns one of Alice's secrets

Fig2. Example for Oblivious Transfer

B. Implementation Modules for Lime Framework In this LIME framework we have 3 main modules;

1. Data Owner Module
2. Data User/Consumer Module
3. Auditor Module

Data owner:

The data owner is responsible for the management of documents and the consumer receives documents and can carry out some task using them.

Data User/Consumer:

The data user or consumer receives the document from data owner. Consumers might transfer a document to another consumer, so we also have to consider the case of an untrusted sender. Each consumer can reveal new embedded information to the auditor to point to the next consumer and to prove his own innocence.

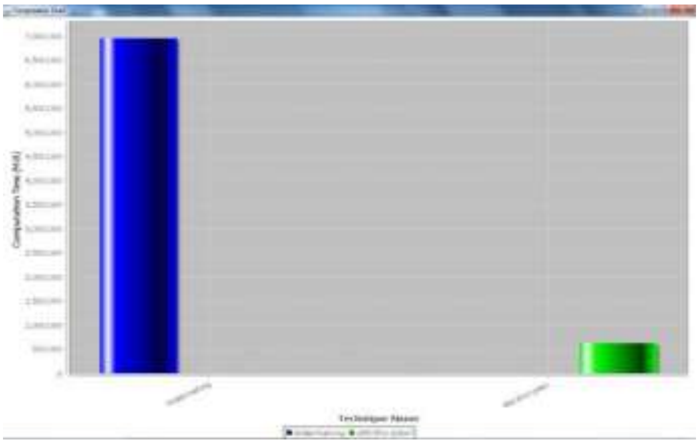
Auditor:

The auditor module is not involved in the transfer of documents, it is only invoked when a leakage occurs and then performs all steps that are necessary to identify the leaker.

4. EXPERIMENTAL RESULTS

In this experiment, we need to run auditor server then users can register as well as login into the application. After login, the user can upload an image into the application. After successfully uploading the image 2 keys will be generated for the given input file. One key is for the document and another key is assigned for each part of document.

Select a receiver and water mark and share the image. If the receiver wants to download then he can download and also re-share the image. After successfully re sharing the image detects the guilty for leak (like who is leaked the information at last) and finally, we can view the auditing details on auditor.



The computation time can be observed from the above graph.

5. CONCLUSION

In this paper we proposed a LIME framework to detect the data leakage and also we can detect the guilty users by re-sharing concept. We are applying the watermark technique to protect the images and also transferring the images. From the experimental results shown that the efficiency of the proposed LIME Framework.

REFERENCES

[1] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, “Extending oblivious transfers efficiently,” in Advances in Cryptology-CRYPTO 2003.Springer, 2003, pp. 145–161.

[2] M. Backes, N. Grimm, and A. Kate, “Lime: Data lineage in themalicious environment,” in Security and Trust Management - 10thInternational Workshop, STM 2014, Wroclaw, Poland, September 10-11,2014. Proceedings, 2014, pp. 183–187.

[3] R. Hasan, R. Sion, and M. Winslett, “The case of the fake picasso:Preventing history forgery with secure provenance,” in FAST, 2009, pp.1–14

[4] F. Kelbert and A. Pretschner, “Data usage control enforcement indistributed systems,” in CODASPY, 2013, pp. 71–82.[25] F. Salim, N. P. Sheppard, and R. Safavi-Naini, “A Rights Management Approach to Securing Data Distribution in Coalitions,” in NSS, 2010,pp. 560–567.

[5] 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.

[6] G. S. Poh, “Design and Analysis of Fair Content Tracing Protocols,”Ph.D. dissertation, 2009. [6] R. Petrovic and B. Tehranchi, “Watermarking in an encrypted domain,”Jul. 7 2006, uS Patent App. 11/482,519.

[7] R. Anderson and C. Manifavas, “Chameleon - A new kind of streamcipher,” in Fast Software Encryption. Springer, 1997, pp. 107–113.

[8] J. Domingo-Ferrer, “Anonymous fingerprinting based on committedoblivious transfer,” in Public Key Cryptography. Springer, 1999, pp.43–52.

[9] j-G. Choi, G. Hanaoka, K. H. Rhee, and H. Imai, “How to breakCOT-based fingerprinting schemes and design new one,” IEICE