Enhanced Data Protection Scheme For Web Services

D.Arun[1], S.Arun Raj[2] , S.Aarokyaraj[3]
Department Of Cse, Arasu Engineering College,
Kumbakonam.

Abstract*Intentional or unintentional leakage of confidential data is undoubtedly one of the most severe security threats that organizations face in the digital era. The threat now extends to our personal lives: a plethora of personal information is available to social networks and smart phone providers and is indirectly transferred to untrustworthy third party and fourth party applications. We present a generic data lineage framework LIME for data flow across multiple entities that take two characteristic, principal roles (i.e., owner and consumer). We define the exact security guarantees required by such a data lineage mechanism toward identification of a guilty entity, and identify the simplifying non-repudiation and honesty assumptions. We then develop and analyze a novel accountable data transfer protocol between two entities within a malicious environment by building upon oblivious transfer, robust watermarking, and signature primitives. Finally, we perform an experimental evaluation to demonstrate the practicality of our protocol and apply our framework to the important data leakage scenarios of data outsourcing and social networks. In general, we consider, our lineage framework for data transfer, to be an key step towards achieving accountability by design.*

Keyword: *Data Leakage Prevention, Data Privacy Leakage Model Watermarking, Data Leakage Protection, Data Loss Prevention.*

INTRODUCTION

Data Lineage provides a visual representation to discover the data flow/movement from its source to destination via various changes and hops on its way in the enterprise environment. Data lineage represents: how the data hops between various data points, how the data gets transformed along the way, how the representation and parameters change, and how the data splits or converges after each hop. Easier representation of the Data Lineage can be shown with dots and lines, where dot represents a data container for data point(s) and lines connecting them represents the transformation(s) the data point under goes, between the data containers.

Representation of Data Lineage broadly depends on scope of the Metadata Management and reference point of interest. Data Lineage provides sources of the data and intermediate data flow hops from the reference point with backward data lineage, leads to the final destination's data points and its intermediate data flows with Forward data lineage. These views can be combined with End to End Lineage for a reference point that provides complete audit trail of that data point of interest from source(s) to its final destination(s).

EXISTING SYSTEM

In the digital era, information leakage through unintentional exposures, or intentional sabotage by disgruntled employees and malicious external entities, present one of the most serious threats to organizations. Confidential data is undoubtedly one of the most severe security threats that organizations face in the digital era. The threat now extends to our personal lives: a plethora of personal information is available to social networks and smart phone providers and is indirectly transferred to untrustworthy third party and fourth party applications.

DISADVAN
TAGES:

1. Duplicate data increased.

2. Data leakage is more.

3.ccess to sensitive Data is Limited.

4.t only allow identification of leaker in a non-

provable manner.

PROPOSED
SYSTEM:

Identification of the leaker is made possible by forensic techniques, but these are usually expensive and don’t always generate the desired results. Therefore, we point out the need for a general accountability mechanism in data transfers. This accountability can be directly

associated with provably detecting a transmission history of data across multiple entities starting from its origin. This is known as data provenance, data lineage or source tracing. The data provenance methodology, in the form of robust watermarking techniques or adding fake data, has already been suggested in the literature and employed by some industries.

Additionally, most of these approaches only allow identification of the leaker in a non-provable manner, which is not sufficient in many cases. We present a generic data lineage framework LIME for data flow across multiple entities that take two characteristic, principal roles (i.e., owner and consumer). We define the exact security guarantees required by such a data lineage mechanism toward identification of a guilty entity, and identify the simplifying non-repudiation and honesty assumptions. We then developandanalyze a novel accountable data transfer protocol between two entities within a malicious environment by building upon oblivious transfer, robust watermarking, and signature primitives.

ADVANTAGES:

1.We can detect the data leakages.
2.t uses oblivious transfer with a two-lock cryptosystem.
3.Prove its correctness by giving micro benchmarking results.

MODULES:

1. Lime

2. Dataowner

3. Consumer

4. Auditor

MODULE DESCRIPTION: LIME:

A generic data lineage framework for data flow across multiple entities in themalicious environment. we identify an optional non-repudiation assumption made between two owners,and an optional trust (honesty) assumption made by the auditor about the owners.The key advantage of our model is that it enforces accountability by design.

DATA OWNER:

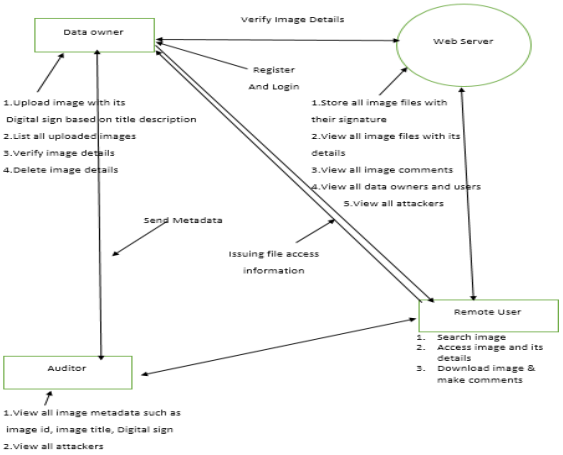
The data owner is responsible for the management of documents and the consumer receives documents and can carry out some task using them.

CONSUMER:

which receives the document. Consumers might transfer a document to another consumer, sowe 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:

which is is not involved in the transfer of documents, it is onlyinvoked when a leakage occurs and then performs all steps that are necessary to identify the leaker.



RELATED WORK:

1.ecure Spread Spectrum Watermarking for Multimedia- AUTHORS: I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon

This paper presents a secure (tamper-resistant) algorithm for watermarking images, and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data. We advocate that a watermark should be constructed as an independent and identically distributed (i.i.d.) Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data. We argue that insertion of a watermark under this regime makes the watermark robust to signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital conversion, requantization, etc.), and common geometric transformations (such as cropping, scaling, translation, and rotation) provided that the original image is available and that it can be successfully registered against the transformed watermarked image. In these cases, the watermark detector unambiguously identifies the owner. Further, the use of Gaussian noise, ensures strong resilience to multiple- document, or collusional, attacks. Experimental results are provided to support these claims, along with an exposition of pending open problems.

2. Digital Signature Scheme Secure Against

Adaptive chosen-

message attacks

AUTHORS: S. Goldwasser, S. Micali, and R. L. Rivest We present a digital signature scheme based on the computational difficulty of integer factorization. The scheme possesses the novel property of being robust against an adaptive chosen-message attack: an adversary who receives signatures for messages of his choice (where each message may be chosen in a way that depends on the signatures of previously chosen messages) cannot later forge the signature of even a single additional message. This may be somewhat surprising, since in the folklore the properties of having forgery being equivalent to factoring and being invulnerable to an adaptive chosen-message attack were considered to be contradictory. More generally, we show how to construct a signature scheme with such properties based on the existence of a "claw-free" pair of permutations--a potentially weaker assumption than the intractibility of integer factorization.The new scheme is potentially practical: signing and verifying signatures are reasonably fast, and signatures are compact.

CONCLUSION:

In this paper, we implement LIME, a model for accountable data transfer across multiple entities. We define participating parties, their interrelationships and give a concrete instantiation for a data transfer protocol using a novel combination of oblivious transfer, robust watermarking and digital signatures. We prove its correctness and show that it is realizable by giving micro bench marking results. By presenting a general applicable framework, we introduce accountability as early as in the design phase of a data transfer infrastructure. Although LIME does not actively prevent data leakage, it introduces reactive accountability.

Thus, it will deter malicious parties from leaking private documents and will encourage honest (but careless) parties to provide the required protection for sensitive data. LIME is flexible as we differentiate between trusted senders (usually owners) and untrusted senders (usually consumers). In the case of the trusted sender, a very simple protocol with little overhead is possible. The untrusted sender requires a more complicated protocol, but the results are not based on trust assumptions and therefore they should be able to convince a neutral entity (e.g. a judge). Our work also motivates further research on data leakage detection techniques for various document types and scenarios. For example, it will be an interesting future research direction to design a verifiable lineage protocol for derived data.

REFERENCES:

[1]. "Chronology of data breaches," http://www.privacyrights.org/data breach. [2]"Data breach cost", http//www.symantec.com/about/news/releas/ article .jsp? prid=20110308 01.

[2]. "Privacy rights clearinghouse," http://www.privacyrights.org.

[3]. "Electronic Privacy Information Center (EPIC),"http://epic.org, 1994.

[4]. "Facebook in Privacy Breach,"

http://online.wsj.com/article/

SB10001424052702304772804575558484075236968.

html. "Offshore outsourcing,"

http:/www.computerworld.com/article/

[5]. 100938/offshore outsourcing cited in Florida leak. A. Mascher-Kampfer, H. St ¨ogner, and A. Uhl, "Multiple re-watermarking scenarios," in Proceedings of the 13th International Conference on Systems, Signals, and Image Processing (IWSSIP 2006). Citeseer, 2006, pp. 53–56.

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

[7]. "Pairing- Based cryptography Library (PBC)"http://crypto.stanford.pbc

[8]. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Image Processing, IEEE Transactions on, vol. 6, no. 12, pp.1673–1687, 1997.