Cipher text multi level encryption using cloud computing

Vidya.G,
mathu2607@gmail.com
Guided by
Ms.G.Saradhambal

Abstract: In this paper, we are discussed about the fulfilment of Data Leakage in Malicious Environment. A data distributor has given the actual data to a set of allegedly trusted agents. Some of the data are leaked. The distributor must evaluate the possibility of the crevice data and should identify data should came from one or more agents, as opposed to having been individually gathered by other means.so, we proposed a data collection strategies to improve the probability of identifying crevices. These method do not built on alterations of the released data. In some cases, we can use some "realistic but fake" data records to improve the detecting crevices and identifying the guilty party. While sending data through the network, some illegal users access the data. The proper security should be provided while sending the useful data over the network. Now a days, the usage of smartphones has been increased. Using some applications in smartphones, the third party can access the data easily, due to this the confidentiality must be affected.to avoid this kind of data leakage we propose the data lineage mechanism. We give fake information to the guilty agent. We develop and analyse the novel accountable data transfer protocol between two entities within a maliciousenvironment by building upon oblivious transfer, robust watermarking and signature primitives. Finally, we apply our framework in the important data leakage scenario and social network, to evaluate the practicality. In general, our lineage framework for data transfer, to be a key step towards achieving accountability by design.

Keywords: Data leakage, lineage framework, secured data.

I.INTRODUCTION

Data leakage is an important matter for business organizations in this networking world. Illegal disclosure may have serious consequences for an organization in both long term and short term. Risks include losing clients and stakeholder confidence, spoil brand name, landing in undesirable lawsuits and overall losing good name and market share in the industry. To prevent from all these unwanted issues from happening, an organized effort is needed to control the information leakage inside and outside the organization. Here is our attempt to demystify the jargon surrounding the data leakage prevention procedures which will help to choose and apply the best suitable options for the business. Leakage refers to an unwanted loss of something which escapes from its proper location and lineage refers to the 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 towards identifying the guilty entity and identify the simplifying disapproved and honesty assumptions.

In the business, sometimes some sensitive data must be handed over to the trusted third parties. For example, in medical field, the patients record will be given to the researchers to find the treatment methodology to cure the diseases. Likewise, a company may have partnerships with other companies which require sharing of customer data. Another enterprise may outsource its data processing, so data must be given to many other companies. The owner of the data are called as distributor and the allegedly trusted third parties are the agents. The aim is to detect if the distributors sensitive data is leaked by agents, atleast we have to find the agent who crevice the data.

II.OVERVIEW OF DATA LINEAGE

Data Leakage Prevention is the kind of solutions which help an organization to make controls to prevent unwanted accidental or malicious leakage of actual information to illegal entities in and outside organization. Here, sensitive information may refer as organization's internal process documents, strategic business plans, intellectual property, financial statements, security policies, network diagrams, blueprints, etc.

2.1 Need Data Lineage

There are such fields where data leakage may occur, so it is very essential to detect such kind of detection, following users may lead to data leakage,

1. The security illiterate
   - The employees with lack of knowledge about security

- Corporate risk because of accidental breaches

2. The gadget needs
    - Introduce a variety of devices to their work PCs
    - Download software
3. The unlawful residents
    - Usage the company's resources unwantedly like by storing music,movies or playing games.
4. The malicious/disgruntled employees
    - Typically minority of employees.
    - Send data access to the third parties. For example, customer lists, RD, etc.

2.2 Generic Data Leakage Prevention

- Usage of security mechanisms
- Firewalls,IDS's & Antivirus software
- Thin-Client architecture
- Advanced security measures.
- Use of pattern based security tools.
- Use of reasoning algorithms.
- Access control & Encryption.
- Access control & Device Control.
- Storage of encryption keys.

III. RELATED WORK CREATIONG ENCRYPTED DIGITAL WATERMARK

Our approach and watermarking are similar in the sense of providing agents with some kind of identifying receiver's information. However, because of its nature, a watermark modifies the item being watermarked. If the object to be watermarked cannot be modified, then a watermark cannot be inserted. . In such cases, methods that attach watermarks to the distributed data are not applicable. Finally, there are also lots of other works on mechanisms that allow only authorized users to access sensitive data through access control policies. Such approaches prevent in some sense data leakage by sharing information only with trusted parties. However, these policies are restrictive and may make it impossible to satisfy agent's requests.

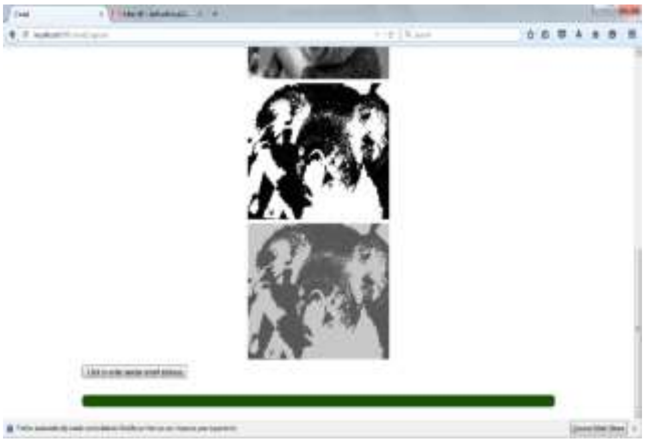

Fig: Encrypted Image using LIME

LIME (Lineage In the Malicious Environment) can be used with any type of data for which watermarking schemes exist. Therefore, we briefly describe different watermarking techniques for different data types. Most watermarking schemes are designed for multimedia files such as images, videos, and audio files. In these multimedia files, watermarks are usually embedded by using a transformed representation (e.g. discrete cosine, wavelet or Fourier transform) and modifying transform domain coefficients. Watermarking techniques have also been developed for other data types such as relational databases, text files and even Android apps. The first two are especially interesting, as they allow us to apply LIME to user databases or medical records. Watermarking relational databases can be done in different ways. The most common solutions are to embed information in noise-tolerant attributes of the entries or to create fake database entries. For watermarking of texts, there are two main approaches. The first one embeds information by changing the text's appearance (e.g. changing distance between words and lines) in a way that is imperceptible to humans. The second approach is also referred to as language watermarking and works on the semantic level of the text rather than on its appearance. A mechanism also has been proposed to insert watermarks to Android apps.

This mechanism encodes a watermark in a permutation graph and hides the graph as a linked list in the application. Due to the list representation, watermarks are encoded in the execution state of the application rather than in its syntax, which makes it robust against attacks. In this approach the authors propose to rather remove existing information than adding new information or modifying existing information. Thereby the watermarking scheme guarantees that no false entries are introduced. The above schemes can be employed in our framework to create data lineage for documents of the respective formats. The only modification that might be necessary when applying our scheme to a different document type is the splitting algorithm. For example for images it makes more sense to take small rectangles of the original image instead of simply taking the consecutive bytes from the pixel array. Embedding multiple watermarks into a single document has been discussed in literature and there are different techniques available. In they discuss multiple rewatermarking and in the focus is on segmented watermarking. Both papers show in experimental results that multiple watermarking is possible which is very important for our scheme, as it allows us to create a lineage over multiple levels. It would be desirable not to reveal the private watermarking key to the auditor during the auditor's investigation, so that it can be safely reused, but as discussed in current public key watermarking schemes are not secure and it is doubtful if it is possible to design one that is secure. In Sadeghi presents approaches to zero-knowledge watermark detection. With this technology it is possible to convince another party of the presence of a watermark in a document without giving any information about the detection key or the watermark itself. However, the scheme discussed in also hides the content of the watermark itself and are therefore unfit for our case, as the auditor has to know the watermark to identify the guilty person. Furthermore, using a technology like this would come with additional constraints for the chosen watermarking scheme.

IV. APPLICATION

It involves study of unobtrusive techniques for detecting leakage in a set of objects or records. Specifically, study the given scenario: After giving the set of objects to the agents, the distributor finds some of the objects may be in the unauthorized place. The distributor must evaluate the possibility of the crevice data and should identify data should came from one or more agents, as opposed to having been individually gathered by other means.in the proposed work, a model is developed to determine the guilt of agents. The algorithms distribute objects to agents, in a way that improves the chances of identifying the leaker. Finally, the option of adding fake objects to the distributed set is also considered. Such objects does not compare with real entities but appear realistic to the agents. In the sense, fake objects acts as a type of watermark for the entire set, without modify 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 the Proposed System, the hackers can be traced with good amount of evidence**.**

V. CONCLUSION & FUTURE WORK

We proposed LIME, a model for accountable data transfer across multiple entities. We defined participating parties, their interrelationships and give a detailed instantiation foe a data transfer protocol using novel combination of oblivious transfer robust watermarking and digital signatures. Although LIME does not actively prevent data leakage 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. 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] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Ktaz, A. Konwin-ski, G. Lee, D. Patterson, A. Rabkin, I. Stoics, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, Vol. 53, No. 4, 2010, pp. 50-58.

[2] M. S. Blumenthal, "Is Security Lost in the Clouds?"*Communica-tions and Strategies*, No. 81, 2011, pp. 69-86.

[3] C.CachinandM.Schunter, "A cloud you can trust,"*IEEESpectrum*,Vol. 48, No. 12,2011,pp. 28-51.

[4] C. Cremers, "The Scyther Tool: Verification, falsification, and analysis of security protocols." *In Computer Aided Verification, Springer Berlin Heidelberg*, 2008, pp. 414-418.

[5]Cloud Security Alliance https://downloads.cloudsecurityalliance.org/initiatives/cdg/CSA_CCAQIS_Survey.pdf (accessed March 24, 2013).

[6] W. Diffie, P. C. V. Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges,"*Designs, Codes and Cryptography*,Vol. 2, No. 2, 1992, pp. 107-125.

[7]M. Ali, K. Bilal, S. U. Khan, B. Veeravalli, K. Li, and A. Y. Zomaya, "DROPS: Division and Replication of Data in the Cloud for Opti-mal Performance and Security," *IEEE Transactions on Cloud Computing*, 2015, DOI: 10.1109/TCC.2015.2400460.

[8] N. En and N. Srensson, "An extensible SAT-solver," *Lecture Notes in Computer Science*, vol. 2919, Springer, 2003, pp. 502-518.

[9] C P. Gomes, H. Kautz, A. Sabharwal, and B. Selman, “Satisfia-bility solvers,” *In Handbook of Knowledge Representation, Elsevier*, 2007.

[10] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud compu-ting: Opportunities and challenges,”*InformationSciences*,Vol. 305, 2015, pp. 357-383.

[11] A. Juels and A. Opera, “New approaches to security and availabil-ity for cloud data,” *Communications of the ACM*,Vol. 56, No. 2, 2013, pp. 64-73.

[12] S. Kamara and K. Lauter, “Cryptographic cloud storage,” *Financial Cryptography and Data Security*,Springer Berlin Heidelberg, 2010, pp. 136-149.

[13]M. Kaufman,”Data security in the world of cloud compu-ting,”*IEEE Security andPrivacy*,Vol. 7, No. 4, 2009, pp. 61-64.

[14] H. Lin and W. Tzeng, “A secure decentralized erasure code for distributed network storage,” *IEEE Transactions on Parallel and Dis-tributed Systems*, vol. 21, no. 11, Nov. 2010, pp. 1586-1594.

[15] H. Lin and W. Tzeng, “A secure erasure code-based cloud storage system with secure data forwarding,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, June 2012, pp. 995-1003.

[16] S. U. R. Malik, S. K. Srinivasan, S. U. Khan, and L. Wang, “A Methodology for OSPF Routing Protocol Verification,” *12th Inter-national Conference on Scalable Computing and Communications (ScalCom)*, Changzhou, China, Dec. 2012.

[17] L. Moura and N. Bjrner, “Satisfiability Modulo Theories: An appetizer,” *Lecture Notes in Computer Science*, Vol. 5902, Springer, 2009, pp. 23-36.

[18] T. Murata, “Petri Nets: Properties, Analysis and Applications,” *Proc. IEEE*, Vol. 77, No. 4, pp. 541-580, Apr. 1989.

[19] A. Shamir, “How to Share a Secret,” *Comm. ACM*, Vol. 22, No. 11, Nov. 1979, pp. 612-613.

[20]H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments,"*IEEE Security andPrivacy*, Vol. 8, No. 6, 2010,pp. 24-31.

[21] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, “Secure Overlay Cloud Storage with Access Control and Assured Deletion,” *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 6, Nov. 2012, pp. 903-916.

[22]A. Yun, C. Shi, and Y. Kim, “On protecting integrity and confiden-tiality of cryptographic file system for outscored storage,” *Proceed-ings of 2009 ACM workshop on cloud computing security CCSA’09*, pp. 67-76, 2009.

[23] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, “SeDaSC: Secure Data Sharing in Clouds,” *IEEE Systems Journal*,2015,http:// dx.doi.org/10.1109/JSYST.2014.2379646.

[24] A. R.Khan, M. Othman, S. A. Madani, and S. U. Khan, “A survey of mobile cloud computing application models,”*IEEECommunica-tions Surveys and Tutorials*,2013,1-21.