**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 5.258**

***IJCSMC, Vol. 5, Issue. 3, March 2016, pg.216 – 222***

# A Digital Signature Scheme Secure Against Adaptive Attack

**S.G.Sandhya[1], R.Uma Maheswari[2]**
Department of Computer Science and Engineering, IFET College of Engineering, Villupuram -605602, India
sgsandhyadhas@gmail.com
umamaheswariramamoorthy@gmail.com

***Abstract- Intentional or unintentional leakage of confidential data is undoubtedly one of the most severe security threats that organizations face in the digital era. Most of the advertisements are posted from any consumers that are displayed in social network profiles. If user clicks on the advertisements, it will redirect to another page. That page may be original or fake. If it is a fake advertisement, it automatically get your profile information and back send to hacker. So we are using two roles. That is consumer and user. If the login user name and password of the user is hacked it is easy for the hackers to get the details of user's friend and share all their details. Consumers also register and upload your advertisements with URL. Once consumers post advertisements to particular profile that advertisements display even in user side and admin side. Admin verify that advertisements, if it verified, verified symbol displayed on image in user side. If advertisements are fake means admin not verify and block the advertisements. If same advertisements posted from same account, it automatically blocks the particular system using IP and MAC.***

***Keywords: Data Leakage Prevention, data leakage protections, Digital Signature.***

## *I. INTRODUCTION*

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. Not only companies are affected by data leakage, it is also a concern to individuals. The rise of social networks and smart phones has made the situation worse. In these environments, individuals disclose their personal information to

various service providers, commonly known as third party applications, in return for some possibly free services. In the absence of proper regulations and accountability mechanisms, many of these applications share individuals' identifying information with dozens of advertising and Internet tracking companies. Even with access control mechanisms, where access to sensitive data is limited, a malicious authorized user can publish sensitive data as soon as he receives it. Primitives like encryption offer protection only as long as the information of interest is encrypted, but once the recipient decrypts a message, nothing can prevent him from publishing the decrypted content. Thus it seems impossible to prevent data leakage proactively. Privacy, consumer rights, and advocacy organizations try to address the problem of information leakages through policies and awareness.

Data Leakage is an important concern for the business organizations in this increasingly networked world these days. Illegitimate disclosure may have serious consequences for an organization in both long term and short term. Risks include losing clients and stakeholder confidence, tarnishing of brand image, landing in undesirable lawsuits, and overall losing goodwill and market share in the industry. To prevent from all these unwanted and nasty activities from happening, an organized effort is needed to control the information flow inside and outside the organization. Here is our attempt to demystify the jargon surrounding the data leakage prevention procedures which will help you to choose and apply the best suitable option for your own business. Leakage describes an unwanted loss of something which escapes from its proper location and Lineage describes as 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.

In the course of doing business, sometimes sensitive data must be handed over to supposedly trusted third parties. For example, a hospital may give patient records to researchers who will devise new treatments. Similarly, a company may have partnerships with other companies that require sharing customer data. Another enterprise may outsource its data processing, so data must be given to various other companies. The owner of the data can be called as distributor and the supposedly trusted third parties the agents. The goal is to detect when the distributors sensitive data have been leaked by agents, and if possible to identify the agent that crevice the data.

## *II. RELATED WORK*

Our approach and watermarking are similar in the sense of providing agents with some kind of receiver identifying information. However, by its very 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 request.

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.

## *III. PROPOSED WORK*

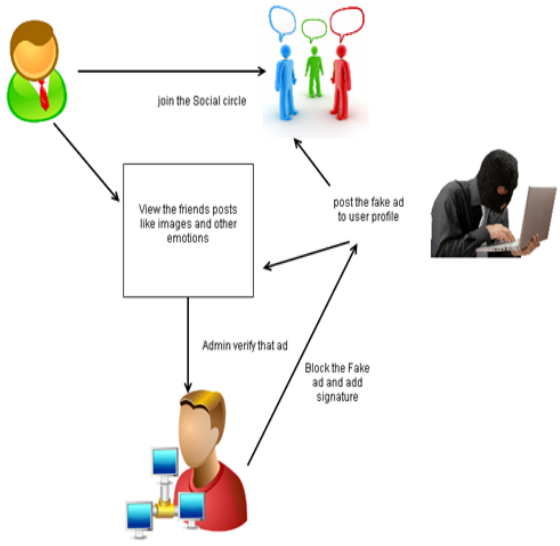
A model is developed for assessing the guilt of agents. The algorithms are also presented for distributing objects to agents, in a way that improves the chances of identifying a leaker. Finally, the option of adding fake objects to the distributed set is also considered. Such objects do not correspond to real entities but appear realistic to the agents. In a sense, the fake objects act as a type of watermark for the entire set, without modifying 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.

- Register identity Information
- Upload files with Signature
- Posting Ads
- Find the fake ad
- Block the fake ad user

### *1. REGISTER IDENTITY INFORMATION*

User Register the webpage before login. In Register page there are two types. One is consumer registration and another one is consumer registration. If any advertisement are posted in user profile to register as a consumer. While Register process user profile is also upload along with signature for users to share the image.




### *2. UPLOAD FILES WITH SIGNATURE*

Users search the friend and send request. And the request is another friend accepted. Upload image with the signature to avoid the unwanted posts from unauthorized users. Signature means a small type of keyword. If any other user tries to tag any photo the user's needs the signature to tag.

### *3. POSTING ADVERTISEMENT*

It deals with the post advertisement to user profile. While consumer posts the advertisement that advertisement automatically view in user profile and admin side. In user profile that advertisement display with "ad not verify signature". That signature will display until admin verify the advertisement. Otherwise that signature will replace the signature "admin verified".

### *4. FIND THE FAKE ADVERTISEMENT*

Consumer while upload the advertisement that is automatically to view in admin side. When the admin clicks the advertisements and find it to be fake then that advertisement will be blocked.

### *5. BLOCK THE FAKE ADVERTISEMENT USER*

If consumer contiguously uploads fake advertisements, admin to track the user block. Some user to hack the social user profile from advertisement click. so fake consumer to upload the fake advertisement to user profiles. Admin to track the fake user and block them.

## *IV. EXPERIMENTAL RESULTS*

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, admin to generate the report for original advertisement and fake advertisement .To separate the report for the use of track the user information and advertisements information for future use. Admin also generate the report for total advertisements.

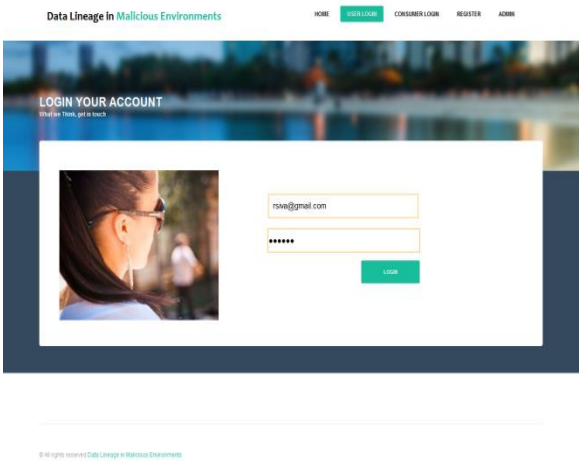



Fig 1: Login page

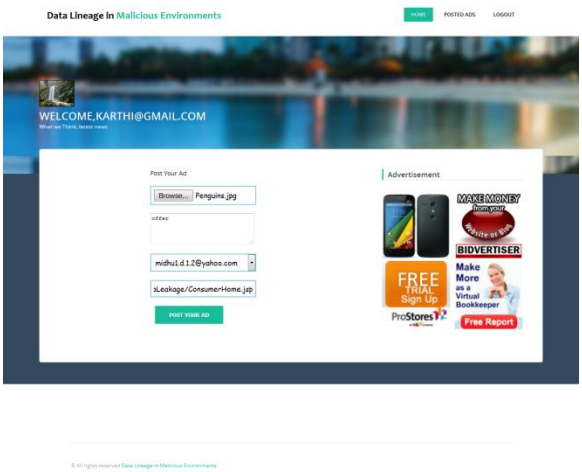



Fig 2: Post Advertisement

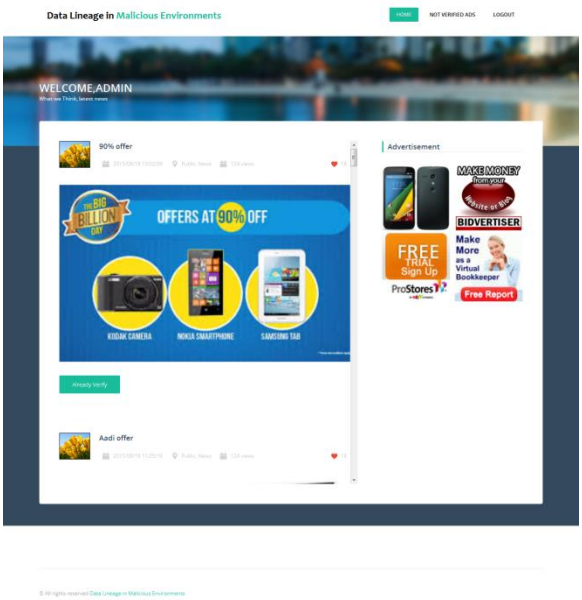



Fig 3: verify Advertisement

## *V. CONCLUSION*

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. To simulate longer data transfer chains, we also perform experiments with multiple iterations of our implementation and find it to be robust. Finally, we demonstrate usage of the protocol to real-life data transfer scenarios such as online social networks and outsourcing.

## *REFERENCES*

[1] Chronology of data breaches, http://www.privacyrights.org/data-breach.

[2] Data breach cost, http://www.symantec.com/about/news/release/article.jsp?prid=20110308 01.

[3] Privacy rights clearinghouse, http://www.privacyrigh ts.org.

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

[5] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in International Conference on Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE. IEEE, 2005, pp. 709–716.

[6] Offshore outsourcing, http://www.computerworld.com/s/article/109938/Offshore outsourcing cited in Florida data leak.

[7] A. Mascher-Kampfer, H. Stogner, and AUhl, "Multiplere-watermarking scenarios, in Proceedings of the 13th International Conference on Systems, Signals, and Image Processing (IWSSIP 2006).Citeseer, 2006, pp. 53–56.

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

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

[10] I. 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.

[11] M.Backes, N.Grimm, and A.Kate,"Lime: Data lineage in the malicious environment," in Security and Trust Management - 10th International Workshop, STM 2014, Wroclaw, Poland, September 10-11,2014. Proceedings, 2014, pp. 183–187.

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

[13] M. Naor and B. Pinkas, "Efficient oblivious transfer protocols," in Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms, 2001, pp. 448–457

[14] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in Advances in Cryptology-ASIACRYPT 2001. Springer,2001, pp. 514–532.

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

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