A SECURITY MECHANISM IN SOCIAL NETWORKS BY GUILTY LEAKAGE DETECTION

[1]REKHA V R, [2]REMYA G NAIR

[1] Assistant Professor, Department of IT, College Of Engineering Kidangoor(Under CUSAT & KTU), Kottayam
[2] M.Tech Student , Department of Computer Science, College Of Engineering Kidangoor(under CUSAT & KTU)
E-mail: [1]rekhavr@gmail.com, [2]nair0869@gmail.com

Abstract— This paper aims to find the guilty of leakage of information in social networks. Here watermarking and lineage mechanism are used for security and thus to find the guilty of private information leakages in social networks. Here three entities are important. That are Owner, Consumer and Auditor. Owner can give documents to consumers. Owner can manage documents. Consumer can share documents to other consumer. Thus Owner can make lineage. Auditor will invoke only when a leakage will happen. Auditor can challenge each consumer to prove their genuinity. If any consumer cannot prove their genuinity that consumer will be the guilty one. We are using watermarks using text files. We can use video , audio or image files in the place of text files.

Keywords— Watermark, Data provenance, Digital watermark, Lineage mechanism.

I. INTRODUCTION

The increase in the use of smart phones and laptops has increased the use of social networks like facebook[6]. By using the social network such as facebook, a third party can get the users private data and can give it to advertisement companies. Then we can say that leakage[2] of private data happened. In this project 3 entities are important. That are Auditor,Owner,and Consumer. Owner will give documents to Consumers. Consumer can manage documents. Auditor will invoke only when one leakage will happen[1]. If leakage will happen Owner can give complaint to Auditor. The Auditor can challenge each consumers to prove their genuinity. If any consumer cannot prove genuinity that consumer will be the guilty one. Here watermarking method is used for security and to find the guilty of private data leakage in networks when one leakage will happen. Watermarking is an embedding method in image,text,video or audio files. It is used for proving ownership. Watermark embedding and watermark detection methods are used here.AES encryption method is used here. When auditor challenge consumer,consumer has to prove their genuinity. Watermark is embedded as an ID value. Here visible watermark is used. Lineage mechanism is used here. Lineage mechanism is the phenomenon of giving datas to consumer and from this consumer to another consumer,likewise. And in this lineage the last one will be the guilty one. This is one assumption taking here. This lineage can also embedded in watermark. Here multiple rewatermarking[9] method is used. That is for each consumer different watermark is used. Filename is also passing with the lineage in watermark. Digital watermarking is the process by which identifying data is woven into media content such as images, movies, music or programming, giving those objects a unique, digital identity that can be used for a variety of valuable applications. Imperceptible to the human senses yet easily recognized by special software detectors, a digital watermark remains constant even through recording, manipulation and editing, compression and decompression, encryption, decryption and broadcast without affecting the quality of the content. Digital watermarks are covert digital security features that transform multiple, previously passive elements of driver licenses, such as photo and artwork, into machine-readable security tokens. When applied as a covert layer of security to driver licenses, digital watermarks enable fast, machine-readable authentication of IDs. The features are imperceptible to humans, but read by computers or other devices enabled with special secure software.

II. DETAILS EXPERIMENTAL SET UP

2.1. Data Lineage Generation

[4]Auditor is invoked by the owner of the document and is provided with the leaked document. In order to find the guilty party, the auditor proceeds in the following way:

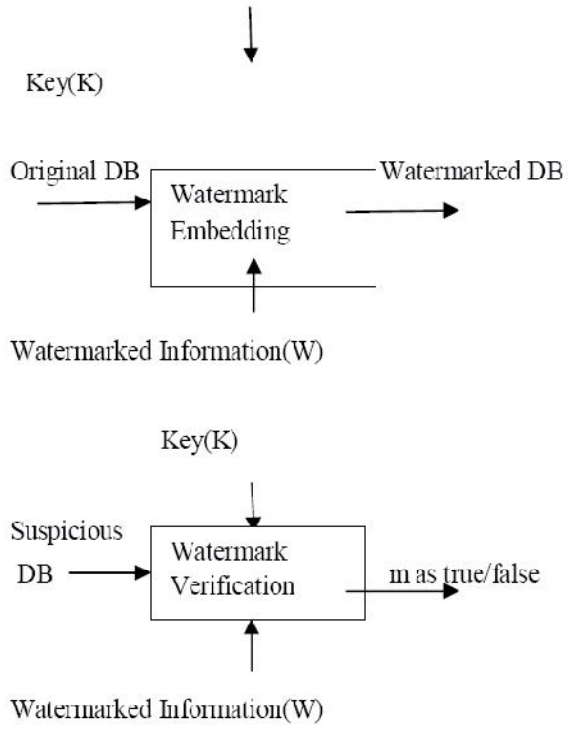
The auditor initially takes the owner as the current suspect. The auditor appends the current suspect to the lineage. The auditor sends the leaked document to the current suspect and asks him to provide the detection keys k1 and k2 for the watermarks in this document as well as the watermark σ. If a non-blind watermarking scheme is used, the auditor additionally requests the unmarked version of the document. If, with key k1,σ cannot be detected, the auditor outputs the lineage . If the current suspect is trusted, the auditor checks that σ is of the form(CS, CR, τ)where Cs is the identifier of the current suspect, takes CR as current suspect and auditor appends current suspect to the lineage. The auditor verifies that σ is of the form[CS, CR, τ]skCR where CS is the identifier of the current suspect. He also verifies the validity of the signature. The auditor outputs the lineage[4]. The last entry is responsible for the leakage.

In our paper we are using text files for watermarking. Here AES Encryption method is used for encrypting file content. A key or ID value is used for watermarking. Here multiple re watermarking method is used. That is for every consumer the watermark will be different. Here we are using visible watermarking method. The Dot Net platform and sql server database is used for implementation. Encryption and watermarking codes are available in Google search.

This project is best suitable for a company to find the leaker of their private information when outsourcing also. We can use different datatypes in the place of text files like image,video or audio files. But depend on the datatypes the method or algorithm for watermarking will be different.

Sender holding D recipient requesting D_w

$K=GenKey^{WM}(1^K)$
Б=(CS, CR, r)
$D_w=W(D, Б,K)\rightarrow\downarrow D_w$



Owner can form lineage that is owner can give documents to one consumer and from this consumer,he/she can share documents to another consumer .In this way owner can form a chain of consumers. This is called data lineage or data provenance[5] mechanism.

In this paper, we formalize this problem of provably associating the guilty party to the leakages, and work on the data lineage methodologies to solve information leakage in various leakage scenarios. At the design stage itself we can add accountability constraints as .It enforces accountability by design mechanism.

We can take non repudiation assumptions;that is if leakage will happen consumers must take the responsibility of that leakage.

Here embedding identifiers of the document so as to identify the leaker of information leakage.

Furthermore, it should not be possible for a malicious consumer to remove the embedded information without rendering the document useless. A technique that can offer these properties is robust watermarking[12].

We formed one website for this using above given languages.

III. RESULTS & DISCUSSIONS

Here when auditor will invoke to find the guilty of leakage ,auditor can challenge each consumer to prove their genuinity. For this purpose here digital watermarking is used. When auditor challenge each consumer consumers should give details of document that owner gave. Then auditor detect the documents with the leaked document. Then detect watermarks[10]. If the leaked document and the document that consumer gave are same ,then that consumer will be the guilty one. Thus we can say in that lineage the last one will be the guilty one after checking.

Digital watermarking

Digital watermarking is the process by which identifying data is woven into media content such as images, movies, music or programming, giving those objects a unique, digital identity that can be used for a variety of valuable applications. In this paper watermarking is done using one ID value. This is used as key. Visible watermark is used with the lineage. Encryption is similar to locking the content in a safe and typically protects content from high-speed digital copying. Digital watermarking is similar to persistently labeling (i.e. searing) invisible identification, copy protection or security information onto the content.

Owner can complaint auditor if the owners private data is leaked.

CONCLUSION

We present this 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 benchmarking results. By presenting a general applicable framework, we introduce accountability as early as in the design phase of a data transfer

infrastructure. Although this paper 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. This system 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 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.

ACKNOWLEDGEMENT

I would like to express my sincere thanks to my project guide Mrs. Rekha V.R from Information Technology Department. I would like to express my sincere thanks to all other faculty members of the Department of Computer Science and Engineering and the Department of Information Technology for their support. I would like to express my sincere thanks to my parents and friends for their valuable support and contribution to my project. Last and foremost, I bow my head in reverence to the Almighty God for providing me the strength and energy to work on this project and enabling me to achieve one of my goals

REFERENCES

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

[2] DataBreachcost ,”http://www.symantec.com/about/news/release/article.jsp?prid=20110308_01

[3] “Privacy rights clearinghouse ”http://www.privacyrights.org//”..

[4] M.Backes, N.Grimm, and A.Kate, ”Lime:Data lineage in the malicious environment,” in Security and Trust Management-10th Interntional Workshop, STM2014, Wroclaw, Poland, September10-11,2014,Proceedings,2014,pp.183-187.

[5] Hasan, R. Sion, and M. Winslett, The case of the fake picasso:Preventing history forgery with secure provenance, in FAST, 2009.

[6] ”Facebook in Privacy Breach,” http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

[7] Pretschner, M. Hilty, F. Schutz, C. Schaefer, and T. Walter, "Usage Control Enforcement: Present and Future,"IEEE Security \& Privacy, vol. 6, no. 4, pp. 44-53, 2008.

[8] Kelbert and A. Pretschner, Data usage control enforcement in distributed systems, in CODASPY, 2013.

[9] A. Mascher-Kampfer, H. St¨ogner, and A. Uhl, “Multiplere-watermarking scenarios,” in Proceedings of the 13th International Conference on Systems, Signals, and Image Processing (IWSSIP 2006).Citeseer, 2006, pp. 53–56.

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

[11] “Pairing-Based Cryptography Library (PBC),”http://crypto.stanford.edu/pbc.

[12] A. Adelsbach, S. Katzenbeisser, and A.-R. Sadeghi, “A computational model for watermark robustness,” in Information Hiding. Springer,

[13] “GNU Multiple Precision Arithmetic Library (GMP),”http://gmplib.org/.

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

[15] A.-R. Sadeghi, “The Marriage of Cryptography and Watermarking .

[16] Beneficial and Challenging for Secure Watermarking and Detection,” in Proceedings of the 6th International Workshop on Digital Watermarking, ser. IWDW ’07, 2008, pp. 2–18.

[17] P. Meerwald, “Watermarking toolbox, ”http://www.cosy.sbg.ac.at/pmeerw/Watermarking/source ”

[18] J. Kilian, F. T. Leighton, L. R. Matheson, T. G. Shamoon, R. E. Tarjan,and F. Zane, “Resistance of digital watermarks to collusive attacks,” in IEEE International Symposium on Information Theory, 1998, pp.271–271.2007, pp. 145–160.

[19] Watermarking Electronic Text DocumentsContaining Justified Paragraphs and Irregular Line Spacing Adnan M. Alattar and Osama M. Alattar Digimarc Corporation, Tualatin, OR 97062 .

[20] Watermarks hide in plain text,”http://www.trnmag.com/Stories/060601/Watermarks_hide_in_plain_text_060601.html”.

[21] Content based Zero-Watermarking Algorithm for Authentication of Text Documents Zunera Jalil, Anwar M. Mirza1and Maria Sabir FAST National University of Computer and Emerging Sciences, Islamabad, Pakistan Air University, Islamabad, Pakistan.

★★★