ENHANCING TIME-STAMPING TECHNIQUE

BY IMPLEMENTING MEDIA ACCESS CONTROL ADDRESS

PACU PUTRA SUARLI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems

Universiti Teknologi Malaysia

JANUARY 2013

This thesis I dedicated to my lovely parents (***Suwarly Mangun & Siti Romlah***) with their encouragement from I was child until now…

And then, for my Big Bro (***Suhendro S. Pd.***), thanks for your support and your encouragement to teach your naughty brother (me) become like what you see right now.

And my late Brother (***Giri Handika***), I am sure you always smile Beside Our GOD'S Hand, we always pray for you dude…

My chubby funny nephew (***Muhammad Rakan Mahardika***), I miss you nduuut…

And to My12 (***Rizki Lia Ismawati***), thanks for your spirit and teach me about LOVING to each other…

ACKNOWLEDGEMENT

Alhamdulillahirabbil ‘alamin, I would like to deeply praise to the **ALLAH SWT** for allowing me to pass all of this moment. I also would like to take this opportunity to express my sincere gratitude to all those who have contributed in completing this thesis

First, I wish to express my sincere appreciation my main thesis supervisor, Associate Professor DR. Mazleena Salleh, for the encouragement, guidance, critics and friendship. I am also very thankful to DR. Siti Hajar Othman for guidance, advice, and motivation. Without their continued support and interest, this thesis would not have been the same as presented here.

Next, I wish to express my sincere gratitude to my beloved family, my brother for their support, encouragement, and kindness. I have nothing without them.

Not forgetting, I would like to express my sincere gratitude to my evaluator, coordinator for project I and II, for the guidance to complete this report. And I very thankful to all Indonesian student in UTM (Persatuan Pelajar Indonesia UTM), whether far from my hometown, because of them I feel stay in my hometown. Unfortunately, it is not possible to list all of them in this limited space.

ABSTRACT

There are many ways to prevent the sensitive information from unauthorized manipulation. Time stamping is one of the ways to prevent the information by keep tracking time creation of the document. Based on the existing research, there are several techniques that implemented time stamping method for a document. In this study, implementing time stamping method for medical record system is the main objective. The integrity of patient medical data is important and therefore the medical record need a mechanism that can verify the record from unauthorized manipulation. The components that included in this proposed time stamping method are MAC (Media Access Control) Address and hash function (SHA512). Besides that, this proposed method also provides a link between a record to another record. That link is produced by including hash value of previous record to the time stamp. This proposed method introduced several functionalities for the medical record. The first functionality is to trace creation time of each record, by recording of the time when the document was time-stamped. The second functionality is to trace who is the creator of the record. The third functionality is to trace which computing device that has been used to create the record by examining the MAC Address. And the last functionality is to prevent the possibility of unauthorized document was put between the documents that already stored in the database by implementing linking hash value. Thus by implement this proposed method, the sensitive information of medical record can be prevented from updated and manipulation by unauthorized people.

ABSTRAK

Terdapat banyak cara untuk mengelakkan maklumat sensitif daripada manipulasi yang tidak dibenarkan. Setem Masa adalah salah satu cara untuk mengelakkan maklumat dengan menyimpan masa pembuatan dokumen itu. Berdasarkan penyelidikan yang sedia ada, terdapat beberapa teknik yang dilaksanakan kaedah setem masa untuk dokumen. Dalam kajian ini, melaksanakan kaedah setem masa untuk sistem rekod perubatan adalah objektif utama. Integriti data perubatan pesakit adalah penting dan oleh itu rekod perubatan memerlukan mekanisme yang boleh mengesahkan rekod dari manipulasi tidak dibenarkan. Komponen yang termasuk dalam kaedah setem masa yang dicadangkan ini adalah MAC (Media Access Control) Alamat dan fungsi hash (SHA512). Selain itu, kaedah yang dicadangkan ini juga menyediakan pautan antara rekod satu dan rekod lain. Pautan ini dihasilkan dengan memasukkan nilai hash setem masa rekod sebelumnya. Kaedah yang dicadangkan ini memperkenalkan beberapa fungsi kepada rekod perubatan. Fungsi pertama adalah untuk mengesan masa penciptaan setiap rekod, dengan rakaman masa apabila dokumen itu ditanda masa. Fungsi kedua ialah untuk mengesan siapa pencipta rekod. Fungsi ketiga adalah untuk mengesan mana peranti pengkomputeran yang telah digunakan untuk mencipta rekod dengan memeriksa Alamat MAC. Dan fungsi terakhir adalah untuk mengelakkan kemungkinan dokumen yang tidak dibenarkan telah dimasukkan antara dokumen yang telah disimpan dalam pangkalan data dengan melaksanakan hubungan nilai hash. Oleh itu, dengan melaksanakan cadangan kaedah ini, maklumat sensitif rekod perubatan boleh dihalang daripada dikemaskini dan manipulasi oleh pihak yang tidak dibenarkan.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	**ii**
	DEDICATION	**iii**
	ACKNOWLEDGEMENT	**iv**
	ABSTRACT	**v**
	ABSTRAK	**vi**
	TABLE OF CONTENT	**vii**
	LIST OF TABLES	**xi**
	LIST OF FIGURES	**xii**
	LIST OF ABBREVIATION	**xiv**
1	**INTRODUCTION**	**1**
	1.1 Overview	1
	1.2 Problem Background	2
	1.3 Problem Statement	3
	1.4 Objectives	4
	1.5 Scope	5
	1.6 Significance of Study	5
	1.7 Aim of study	6
	1.8 Organization of Thesis	6

2	**LITERATURE REVIEW**	**7**
	2.1 Overview	7
	2.2 Document Integrity	9
	2.3 Electronic Medical Record	10
	2.4 Definition of Time-stamping	11
	2.5 Method of Time-stamping	14
	2.5.1 Hash Function	14
	2.5.1.1 One Way Function	14
	2.5.1.2 Collision Resistance	15
	2.5.1.3 Message Digest	17
	2.6 Time-Stamping Scheme	17
	2.6.1 Trust Third Party	18
	2.6.1.1 Simple Scheme	19
	2.6.1.2 Linking Scheme	20
	2.6.2 Distributed Scheme	22
	2.7 Protocol of Time-stamping	23
	2.7.1 Ticket and stub time-stamping protocol	23
	2.7.1.1 Advantages and disadvantages of ticket and stub time stamping protocol	26
	2.7.2 Nonce-Based Time-stamping Protocol	26
	2.7.2.1 Advantages and disadvantages of ticket and stub time stamping protocol	27
	2.7.3 Originator-Generated Timestamp Receipt Protocol	28
	2.7.3.1 Advantages and disadvantages of originator-generated timestamp receipt protocol	29
	2.7.4 Augmented Originator-Generated Timestamp Receipt Protocol	29
	2.7.4.1 Advantages and disadvantages of Augmented Originator-Generated Timestamp Receipt Protocol	30
	2.7.5 Public Key Certificate-Based Protocol	31
	2.7.5.1 Advantages and disadvantages of Public Key Certificate-Based Protocol	32
	2.7.6 Time-Based Signing Key Protocol	32

	2.7.6.1 Advantages and disadvantages of Time-Based Signing Key Protocol	33
	2.7.7 Bounded storage model	34
	2.7.7.1 Advantages and disadvantages of Bounded storage model	34
	2.8 MAC Address	35
	2.9 Chapter Summary	35
3	**RESEARCH METHODOLOGY**	38
	3.1 Overview	38
	3.2 Research Procedure	39
	3.2.1 Phase I: Literature Review	40
	3.2.2 Phase II: Design and Implementation	42
	3.2.3 Phase III: Validation and Testing	42
	3.2.4 Tools and software needs	44
	3.3 Chapter Summary	44
4	**INITIAL DESIGN**	**45**
	4.1 Overview	45
	4.2 Propose Technique	45
	4.2.1 Media Access Control Address	47
	4.2.2 Hash Function SHA 512	48
	4.2.3 Generating Current Time	50
	4.3 Design of Application Flowchart	51
	4.4 Database Design	52
	4.5 Preliminary Analysis	56
	4.5.1 Single Character Change	58
	4.5.2 Single Character Delete	58
	4.5.3 Single Character Add	59
	4.6 Chapter Summary	69
5	**IMPLEMENTATION AND DESIGN**	**70**
	5.1 Overview	70
	5.2 Medical Record System	70

5.2.1 Login Use Case 71
5.2.2 Register Patient Use Case 73
5.2.3 Consultation Use Case 74
5.2.4 View Medical Record Use Case 78
5.2.5 View Log of Printed Document Use Case 79
5.3 Black Box Testing 81
5.3.1 Test Case 81
5.3.2 Testing Result 83
5.4 Security and the Strengthens of the Proposed Method 85
5.5 Chapter Summary 88

6 DISCUSSION AND CONCLUSION 89
6.1 Overview 89
6.2 Achievement and Solution 89
6.3 Problem and Challenges 91
6.4 Future Work 91
6.5 Closing Note 92

REFERENCE 93

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Comparison of hash function algorithms	15
2.2	Comparison Existing Time-Stamping Protocol	36
4.1	LoginTable Table Design	53
4.2	PatientInfo Table Design	54
4.3	Record Table Design	54
4.4	MedicalLog Table Design	55
4.5	Sample of Medical Record Details	57
4.6	Preliminary Analysis Case 1	60
4.7	Preliminary Analysis Case 2	63
4.8	Preliminary Analysis Case 3	66
5.1	Patient Test Case Information	82
5.2	Consultation Details	82
5.3	Test Case Details	83
5.4	Result of Functionality Testing	84
5.5	Comparison table between system with and without proposed method	84
5.6	Comparison of Time Stamping Method	87

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Structure of secure document (Jian-hua *et al.*, 2008)	9
2.2	Condition of digital time-stamping	12
2.3	Pre-image collision resistance	16
2.4	Second pre-image collision resistance	16
2.5	Classification time-stamping scheme	18
2.6	Simple schema model	19
2.7	Linking scheme	21
2.8	Model linking scheme	21
2.9	Main Ticket and Stub time-stamping protocol (Peyravian *et al.*, 2000)	24
2.10	Alternative Ticket and Stub protocol (Peyravian *et al.*, 2000)	26
2.11	Nonce-based time-stamping protocol (Peyravian *et al.*, 2000)	27
2.12	Originator generated time-stamping receipt (Peyravian *et al.*, 2001)	28
2.13	Augmented Originator-Generated Timestamp Receipt Protocol (Peyravian *et al.*, 2001)	30
2.14	Public Key Certificate-Based Protocol (Peyravian *et al.*, 2001)	31
2.15	Time-Based Signing Key Protocol (Peyravian *et al.*, 2001)	33
3.1	Research Framework	40
4.1	Proposed time-stamping technique	47
4.2	Generating time proposed method	50

4.3	Flowchart Medical Record System	52
5.1	Login Page	72
5.2	VB Source Code for Login Case	72
5.3	Register Patient Page	73
5.4	VB Source Code for Register Patient Case	74
5.5	Consultation Page	75
5.6	VB Source Code for Validation Patient	76
5.7	VB Source Code for Get MAC Address	76
5.8	VB Source Code for Get Time	77
5.9	View Medical Record Page	79
5.10	View PrintLog Page	80
5.11	Source Code of Validation Record	80

LIST OF ABBREVIATION

BBC	-	British Broadcasting Corporation
EMRS	-	Electronic Medical Record System
MAC	-	Media Access Control
PKI	-	Public Key Infrastructure
TSA	-	Time Stamping Authority
TTP	-	Trust Third Party

CHAPTER 1

INTRODUCTION

1.1 Overview

Nowadays, data or information becomes very important thing that should have more integrity. Data has strong relation with someone privacy, such as medical record, identity record, etc. Data itself should construct of three elements of information security, they are confidentiality, integrity, and availability. In information security aspect it called as data investigation. There is an evidence which published by BBC(2012), "*Verizon found that 58% of all the data stolen during breaches in 2011, hacktivists stole more data from large corporations than cybercriminals in 2011*". That statement shows how the data is very important.

The awareness of security data or information should be increased in developing country. Because, most of the systems that have been released are electronic system based, such as paying the tax, medical system, etc. If most of the system using electronic base system, it means the threat of the data increased. By that reason, the data become more important, confidential, and cannot access or updated by unauthorized user. There are so many ways can be implemented to prevent the data stolen and data updating without authority from the authorized user, such as time-stamping and digital signature.

Time-stamping is a method that make document more secure from updating by unauthorized people with certain time. The difference between time-stamping and digital signature is in time-stamping does not only add a digital signature by the author, but, it also adds the data with certain time when the author creates the data or document. It means the creation and modification of a document can be traced in this method.

1.2 Problem Background

Recently, there are so many crime cases that related to the document stolen and updated by unauthorized writer. For example, if a patient from medical center did a check-up for their health. Then, the doctor creates and records their medical record into the medical center system. The medical record system will show the updated medical record of that patient. So, if the medical record was updated by unauthorized user, the doctor cannot recognize that the doctor did not create that medical record. Because, in that record there is no information about when the creation or update date and also there is no information about who is the last person who update that medical record. In this case, securing or tracking our document or data is very important to prevent our data from ignorance of unauthorized people.

In computer science there are some of recognized techniques that make our data or information more secure, one of them is time-stamping. Time-stamping is a method to keep track time of creation and modification date of a document does prevent the copyright stolen. As (Schneier, 1996) state "*It must be impossible to timestamp a document with a date and time different from the present one"*. From that statement explains that the time-stamping technique will be secure if the document that already time-stamping cannot be changed.

There are some methods that already implemented in existing research, first ticket and stub time-stamping protocol algorithm and second nonce based time-stamping protocol algorithm as described by (Peyravian *et al.*, 2000). Another recent method for time-stamping electronic documents using certificates and user specified times, they are originator generated time-stamp receipt protocol, augmented originator generated time-stamp receipt protocol, public key certificate based protocol, and time based signing key protocol as described by (Peyravian *et al.*, 2001).

Besides that, there are some methods also implement time-stamping algorithm with hash function. Hash function means any algorithm or subroutine that maps large data sets of variable length, called keys, to smaller data sets of a fixed length. There are some hash function techniques to hash the message or data in cryptography, such as MD2, MD5, SHA 0, SHA 1, SHA 2 (256, 512), whirlpool, etc. Some technique of time-stamping already combined between time-stamping methods with hash function to make the integrity of document become more secure. But, in one of hash function method (MD5 and MD4), there was collision-finder that can make client-side hash function in time-stamping insecure (Buldas and Laur, 2006). Besides that, (Wang and Yu, 2005) described it also happen in another hash function, such as HAVAL-128, MD4, RIPEMD, and SHA-0. Then, in hash function also there is pre-image attack. Therefore, this study proposes a new method of time stamping that implemented to the medical record system.

1.3 Problem Statement

Combining time-stamping with hash function is one of implementation of time-stamping method. In those methods the researcher combining time-stamping with any of hash functions algorithm like SHA-1, SHA-0, and MD5. But, as described by (Buldas and Laur, 2006), combining between time-stamping with hash function (MD5) is not secure as client-side, because there is attack that called as

collision finder. This collision finder means that function can produce the same value when two different messages hashed with one hash function.

Besides that, based on some papers that related to this study, most of the time-stamping protocol did not focus on how the linking between one document with another document. Such as the protocol that was done by (Peyravian *et al.*, 2000, 2001), the protocol did not use any linking between one document with another document, except one protocol that called as originator generated time-stamp protocol. But, the linking number also did not compulsory to be included to time stamping.

1.4 Objective

From the problem statement above this study have some objective, they are:

i. Studying and implementing hash function especially SHA-2 (512) in hashing a document
ii. Analyzing the existing time-stamping method for a document
iii. Implementing and developing the prototype of proposed time-stamping method that will combine with hash function and Media Access Control (MAC) Address to make a document more secure for medical record.
iv. Testing and validating the prototype of time stamping method that will be implemented

1.5 Scope

This study will focus in time-stamping that combine with hash function especially SHA-2 (512) hash function method. A new proposed method of time-stamping implemented for medical record system. Because, based on the explanation before, the medical record is very important data that should keep about the privacy. Besides that, this proposed time-stamping technique uses MAC Address as a unique value. Then, XPS file becomes the output of this medical record. and also, this study does not analyze about the possibility of man in the middle attack.

1.6 Significance of study

Basically, this study helps to know and analyze the function of time-stamping in securing our data or document. By analyzing and knowing function of time stamping, how to make our document or data more secure can be understood. Combining time-stamping and hash function can help to make our data or document encryption become more complicated, so the unauthorized user cannot change, modified, or delete our data or document.

Then, based on (Williams and Boren, 2008), E-Medical record is one of ICT invention in developing country. Most of developing country use electronic medical record (EMR) in their hospital system. The medical record is very confidential, it means no one can see or update the medical record except the doctor and the authorized people.

By implementing the proposed method of time stamping in medical record system, it means the medical record can be traced who is the creator and when the document was made by the author. Besides of that, by adding the MAC address this proposed method also can trace where the document has been created.

1.7 Aim of study

This study proposes a method that designed by using hashing function (SHA 512), and then combining with other function, like reliability time in TSA, ID, Media Access Control (MAC) Address as a unique key, digital signature, etc. This proposed method implemented into medical record that will affect the confidentiality of medical record.

1.8 Organization of Thesis

This thesis is divided into six chapters, the first chapter is introduction, and the second is literature review, then research methodology, analysis design, implementation and testing, and the conclusion. Each of chapter will provide summary of the chapter and will be part of the last chapter as the conclusion.

Introduction is the first chapter of this thesis. In this chapter include the overview of the thesis, problem that become a background to do this study, the problem that find by the writer, the objectives of this thesis, scope, significance of study, and organization of thesis.

The second chapter of this thesis will be literature review. This chapter explain about the important research that always done before that help to finish this thesis in this chapter. Such as, what are the techniques that already done by the research before, what are the disadvantages and advantages of the existing technique that already implemented, etc.

The third chapter of this thesis is research methodology. In this chapter how to do this research will be explained in more details. Where each phase figures to complete the objective of the thesis that already explained in the first chapter.

The fourth chapter is the analysis design. In this chapter will explain about the proposed time stamping method that combined with Media Access Control Address and hash function. Besides that, in this chapter also explain the flow of medical report system that already implemented with new propose method of time stamping. At the end of this chapter, preliminary analysis shows how secure this proposed technique can be used, especially in hashing to count how many hamming weight of changes of each data.

The fifth chapter is the implementation and testing. In this chapter explain about how to implement the proposed method of time stamping to medical record system. Besides that, how the testing will be done to the proposed method that implemented with medical record will be more details in this chapter.

And the last chapter will be conclusion. The last chapter will include all the summaries of each chapter. From that summary, this study comes out with a conclusion and also the future work for further research.

REFERENCES

Abd Ghani, M. K., Bali, R. K., Naguib, R. N. G., Marshall, I. M., and Wickramasinghe, N. S. (2008). Electronic health records approaches and challenges: a comparison between Malaysia and four East Asian countries. *International Journal of Electronic Healthcare, 4*(1), 78-104.

Ansper, A., Buldas, A., Saarepera, M., and Willemson, J. (2001). *Improving the Availability of Time-Stamping Services*. Paper presented at the Proceedings of the 6th Australasian Conference on Information Security and Privacy.

Ben Shil, A., Blibech, K., and Robbana, R. (2008). A new timestamping schema in the Bounded Storage Model. *Risks and Security of Internet and Systems, 2008. CRiSIS '08. Third International Conference on*. 28-30 Oct. 2008. 199-205.

Bonnecaze, A., Liardet, P., Gabillon, A., and Blibech, K. (2006). Secure time-stamping schemes: a distributed point of view. *Annales des Télécommunications, 01*(61), 662-681.

Buldas, A., and Laur, S. (2006). *Do Broken Hash Functions Affect the Security of Time-Stamping Schemes? Applied Cryptography and Network Security*. In J. Zhou, M. Yung, and F. Bao (Eds.), (Vol. 3989, pp. 50-65): Springer Berlin / Heidelberg.

Cardenas, E. D. (2003). MAC Spoofing-An Introduction. *Global Information Assurance Certification*.

Cilardo, A., Mazzeo, A., Romano, L., Saggese, G. P., and Cattaneo, G. (2003). A web services based architecture for digital time stamping. *J. Web Eng., 2*(3), 148-175.

Haber, S., and Stornetta, W. S. (1991). *How to Time-Stamp a Digital Document*. Paper presented at the Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology.

Hu, P., Wei, C.-P., and Cheung, T.-H. (2002). *Investigating Telemedicine Developments in Taiwan: Implications for Telemedicine Program Management*. Paper presented at the Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 6 - Volume 6.

Jian-hua, Z., Nan, Z., Xianze, Y., and Chunyan, Y. (2008). Security Mechanism to Protect the Integrity of Web Documents. *Management of e-Commerce and e-Government, 2008. ICMECG '08. International Conference on*. 17-19 Oct. 2008. 395-398.

Moran, T., Shaltiel, R., and Ta-Shma, A. (2009). Non-interactive Timestamping in the Bounded-Storage Model. *J. Cryptol., 22*(2), 189-226.

NIST. (2002). Federal Information Processing Standards Publication 180-2, *Secure Hash Standard* (pp. 3-71). United States: National Institute of Standards and Technology.

Peyravian, M., Matyas, S. M., Roginsky, A., and Zunic, N. (2000). Ticket and Challenge-Based Protocols for Timestamping. *Computers & Security, 19*(6), 551-558.

Peyravian, M., Matyas, S. M., Roginsky, A., and Zunic, N. (2001). Methods for Timestamping Electronic Documents Using Certificates and User-Specified Times. *Computers & Security, 20*(3), 255-262.

Schneier, B. (1996). *Applied Cryptography* (2nd ed.). New York, USA: John Wiley & Sons.

Shaw, G. (2000). Digital document integrity. *Secure Images and Image Authentication (Ref. No. 2000/039), IEE Seminar on*. 2000. 12/11-12/14.

Som, M. H. M., Norali, A. N., and Ali, M. S. A. M. (2010). Telehealth in Malaysia - An overview. *Industrial Electronics & Applications (ISIEA), 2010 IEEE Symposium on*. 3-5 Oct. 2010. 660-664.

St Denis, T., and Johnson, S. (2006). *Chapter 5 - Hash Functions Cryptography for Developers* (pp. 203-250). Burlington: Syngress.

Toyoda, K. (1998). Standardization and security for the EMR. *International Journal of Medical Informatics, 48*(1–3), 57-60.

Wang, X., and Yu, H. (2005). *How to break MD5 and other hash functions*. Paper presented at the Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques.

Williams, F., and Boren, S. A. (2008). The role of electronic medical record in care delivery in developing countries. *International Journal of Information Management, 28*(6), 503-507.