UNIVERSITI TEKNOLOGI MARA

Healthcare Data Integrity Using Hash Function

WAN MADIHAH BINTI WAN HARRUM

Dissertation submitted in partial fulfillment
of the requirements for the degree of
Master of Science (Computer Networking)

Faculty of Computer and Mathematical Sciences

January 2016

ABSTRACT

Healthcare fields are currently evolving around the digital world, and it is a must for security analyst to ensure it is safe and secure to store data in digital form or even to be uploading into clouds. Digital world today offer ways to ensure data security and integrity called encryption. Encryption converts data into forms that cannot be read by normal people. In order to preserve data security, there is a type of encryption form being introduced, Hash function. Hash function however, has an open flaw for data integrity. This research aim to analyse real health data integrity using new version of hash function and its performance against collision resistance. This will benefit others by listing the pros and cons of applying hash function in medical field. Real healthcare data are being hash with three different version of hash function, MD5, SHA-1, SHA-2. Message digest outputs are tested for collision resistance to ensure data integrity. The result from this findings will leads to better solution and allow better enhancement for hash function problem.

ACKNOWLEDGEMENT

Alhamdulillah, thanks you Allah for the Grace and Blessing, I am able to finish this dissertation. I would like to thank my supportive supervisor Dr. Fakariah Hani Binti Mohd Ali for her supports, help, comments, suggestions and ideas to solve related problem during my dissertation completion.

I would like to thank my parents, En. Wan Harrum Bin Wan Nawang and Pn. Noraini Binti Awang, for their supportive attitude and strong words of encouragement that help me throughout dissertation completion. Thanks to my friends for the help with providing ideas, support and suggestions.

Thank you and may ALLAH bless all of you.

TABLE OF CONTENTS

Page

CHAPTER ONE: INTRODUCTION

CHAPTER TWO: LITERATURE REVIEW

CHAPTER 1

INTRODUCTION

This chapter describes the overview of this whole report including problem statements, objectives, research questions, scope and significance of the dissertation.

1.1 RESEARCH BACKGROUND

Data security becomes highly topic to be concern in this rapidly evolving technology era. World today are attempt to convert a physical to a virtual data, this changes and shifting regulations require user to reanalyze on data protection techniques. Digital world today offer ways to ensure data security called encryption. Encryption converts real message or data into a type of form that cannot be known by normal people. Implementing encryption also one of the best choices to increase data security but it has open flaws for integrity. One of the alternatives to preserve integrity of documents, files or data is through fingerprint (Forouzan, 2008). There are several types of encryption that was introduced, such as, symmetric encryption, asymmetric encryption and hashing. Today, hashing encryption are widely being used and the algorithm is currently developing. Figure 1.1 illustrates the simple idea of hashing encryption.

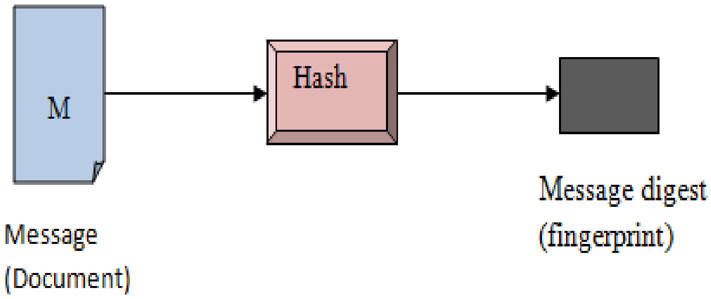

Figure1.1 Message and message digest