



UNIVERSITAS
MERCU BUANA

**PERBANDINGAN TINGKAT KEAMANAN MD5
DENGAN SHA512 UNTUK MENGATASI SERANGAN
MITM PADA PRIVACY DATA *E-HEALTH***

TESIS

**Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan
Program Pascasarjana Magister Teknik Elektro**

UNIVERSITAS

MERCU BUANA

Oleh :

Sirep Purwanti

55414120023

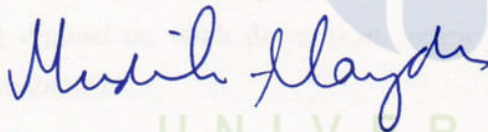
**UNIVERSITAS MERCU BUANA
PROGRAM PASCASARJANA**

PENGESAHAN TESIS

Judul : Perbandingan Tingkat Keamanan MD5 dengan SHA512 Untuk
Mengatasi Serangan MITM Pada *Privacy Data E-Health*
Nama : Sirep Purwanti
NIM : 55414120023
Program : Pascasarjana Program Magister Teknik Elektro
Konsentrasi : *Network Security ICT*
Tanggal :

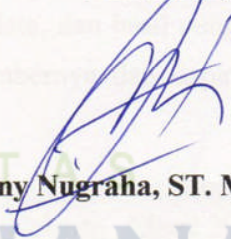
Mengesahkan

Pembimbing 1



(Prof. Dr. -Ing. Mudrik Alaydrus)

Pembimbing 2



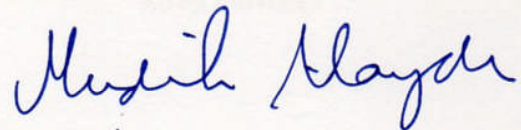
(Beny Nugraha, ST. MT. M.Sc)

Direktur Pascasarjana

Ketua Program Studi



(Prof. Dr. Didik J. Rachbini)



(Prof. Dr. -Ing. Mudrik Alaydrus)

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam Tesis ini :

Judul : Perbandingan Tingkat Keamanan MD5 dengan SHA512 Untuk Mengatasi Serangan MITM Pada *Privacy Data E-Health*
Nama : Sirep Purwanti
N I M : 55414120023
Program : Pascasarjana Program Magister Teknik Elektro
Kosentrasi : *Network Security ICT*

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, Maret 2017



Sirep Purwanti

KATA PENGANTAR

Segala puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena berkat rahmat-Nya, tesis dengan judul “**Perbandingan Tingkat Keamanan MD5 dengan SHA512 Untuk Mengatasi Serangan MITM Pada Privacy Data E-Health**” ini dapat diselesaikan.

Tesis ini disusun untuk memenuhi salah satu syarat menyelesaikan Program Pascasarjana Magister Teknik (M.T.) dalam bidang keahlian Teknik Elektro pada program studi *Network Security* ICT di Universitas Mercubuana.

Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa hormat dan ucapan terima kasih yang sebesar besarnya kepada:

1. Bapak Prof. Dr. –Ing. Mudrik Alaydrus atas arahan dan waktu yang telah diluangkan kepada penulis untuk berdiskusi selama menjadi dosen pembimbing, dan perkuliahan.
2. Bapak Beny Nugraha, ST. MT. M.Sc. atas arahan dan waktu yang telah diberikan kepada penulis untuk berdiskusi selama menjadi dosen pembimbing, dan perkuliahan.
3. Bapak Dr. Andi Adriansyah, M.Eng. dan Bapak Dr. Denny Setiawan, MT. sebagai dosen penguji
4. Bapak, Ibu, Suami dan Kakak atas support dan doanya.
5. Semua dosen program Pascasarja Magister Teknik Elektro di Universitas Mercubuana.
6. Rekan-rekan program S2 Magister Teknik Elektro angkatan 16.
7. Kepada semua pihak yang telah membantu, yang namanya tidak dapat penulis sebutkan satu persatu.

Dengan keterbatasan pengalaman, pengetahuan maupun pustaka yang ditinjau, penulis menyadari bahwa tesis ini masih banyak kekurangan dan perlu pengembangan lebih lanjut agar benar-benar bermanfaat. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran agar tesis ini lebih sempurna, dan dapat penulis gunakan dalam penelitian dan penulisan karya ilmiah di masa yang akan datang.

Akhir kata, penulis berharap agar tesis ini memberikan manfaat bagi kita semua, terutama untuk pengembangan ilmu pengetahuan di bidang keamanan jaringan ICT.

Jakarta, Maret 2017

Sirep Purwanti

DAFTAR ISI

Cover.....	i
Lembar Pengesahan.....	ii
Pernyataan.....	iii
Abstrak.....	iv
Kata Pengantar.....	vi
Daftar Isi.....	vii
Daftar Gambar.....	x
Daftar Tabel.....	xii
Bab I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
Bab II KAJIAN PUSTAKA.....	5
2.1 Jurnal Pendukung/ Penelitian Terkait.....	5
2.2 E-health.....	8
2.2.1 EHR.....	10
2.2.2 <i>Standart Communication Protokol</i> dengan HL 7 <i>(Health Level 7)</i>	12

2.3	Serangan.....	14
2.3.1	Jenis – jenis serangan.....	14
2.3.1.1	Tantangan <i>Security</i>	16
2.3.1.1.1	Data <i>confidentiality</i>	16
2.3.1.1.2	Data <i>Integrity</i>	16
2.3.1.1.3	Data <i>authentication</i>	17
2.3.1.1.4	Data <i>availability</i>	17
2.3.2	Serangan MITM.....	17
2.3.2.1	<i>Phishing attack</i>	19
2.3.2.2	<i>Modification attack</i>	21
2.4	Keamanan dengan metode kriptografi.....	23
2.4.1	Pengertian Kriptografi.....	23
2.4.2	Kriptografi dengan MD5.....	25
2.4.3	Kriptografi dengan Hash SHA512.....	27
2.5	Kali Linux.....	29
2.6	Virtual Box.....	29
2.7	Hashcat.....	31
Bab III	METODOLOGI PENELITIAN.....	34
3.1	<i>Testbed</i> Setup.....	34
3.1.1	Spesifikasi <i>Hardwar</i>	34
3.1.2	<i>Software</i> Pendukung.....	35
3.1.2.1	Kali Linux 2.0.....	35

3.1.2.2	Hashcat <i>for</i> windows.....	36
3.1.2.3	BeEF Kali linux.....	36
3.1.2.4	Hash <i>Identifier</i>	37
3.2	Metode Pengujian.....	38
3.3	Topologi Jaringan.....	39
3.4	Skenario Pengujian.....	39
3.4.1	Membandingkan Tingkat Keamanan Antara Data yang tidak terlindungi dengan data yang terlindungi MD5.....	40
3.4.2	Membandingkan Tingkat Keamanan Antara MD5 dan SHA512	40
3.5	Lokasi Penelitian.....	40
3.6	Metode Pengambilan Data.....	40
Bab IV	DATA DAN ANALISA.....	41
4.1	Data Hasil Penelitian.....	41
4.1.1	Perbandingan mekanisme keamanan antara data yang tidak terlindungi dengan data yang terlindungi MD5.....	43
4.1.1.1	Hasil percobaan <i>phising</i> website https dan modifikasi data.....	43
4.1.1.2	Waktu <i>generate</i> data MD5 dengan hashcat 3.30	45

4.1.1.3	Perbandingan Jumlah bytes data	46
4.1.1.4	Kesimpulan.....	47
4.1.2	Perbandingan Mekanisme Keamanan Antara MD5 dan SHA512.....	47
4.1.2.1	Perbandingan Jumlah bytes data.....	47
4.1.2.2	Waktu <i>generate hash</i>	48
4.1.2.3	<i>Range</i> karakter MD5 dan SHA512 yang bisa <i>dicracked</i>	52
4.1.2.4	Hasil percobaan modifikasi data	56
4.1.2.5	Kesimpulan	56
Bab V	KESIMPULAN DAN PENELITIAN LANJUTAN.....	58
5.1	Kesimpulan.....	58
5.2	Penelitian Lanjutan.....	58
	DAFTAR PUSTAKA.....	59

DAFTAR GAMBAR

Gambar 1.1 Poin serangan pada keamanan jaringan mHealth	2
Gambar 2.1 Jurnal Pendukung	5
Gambar 2.2 Hubungan antara beberapa paradigma e-health	9
Gambar 2.3. e-health memberikan perubahan dibidang pengobatan	10
Gambar 2.4. Struktur EHR	10
Gambar 2.5 Gambaran tentang hubungan antara standar eHealth yang berbeda	12
Gambar 2.6 Contoh data klinis pasien dengan format data HL7	13
Gambar 2.7 Deskripsi data klinis pasien dengan format data HL7	14
Gambar 2. 8. Man In The Middle	18
Gambar 2.9 Ilustrasi dari MITM Attack	19
Gambar 2.10 Phising attack	20
Gambar 2.11 Contoh Phising attack pada personal informasi bank	21
Gambar 2.12 Ilustrasi dari modification attack	22
Gambar 2.13 skema modification attack	22
Gambar 2.14 contoh input dan output hash	25
Gambar 2.15 Pengolahan pesan blok 512	27
Gambar 2.16 Dekstop Kali linux	29
Gambar 2.17 Oracle Virtual Box	30
Gambar 2.18 tampilan hashcat di cmd windows	31
Gambar 3.1 Testbed pengujian	34
Gambar 3.2 Dekstop Kali linux	35
Gambar 3.3 contoh perintah serangan dan urutan pada hashcat	36
Gambar 3.4 Tampilan beef	36
Gambar 3.5 Tampilan hash identifier	37
Gambar 3.6 Flowchart metode pengujian	38
Gambar 3.7 Topologi fisik jaringan	39
Gambar 4.1 Duplikat/ tiruan dari login https	43

Gambar 4.2 Password login tercatat dalam database tools beef	44
Gambar 4.3 Waktu modifikasi data	44
Gambar 4.4 Data yang dimodifikasi	45
Gambar 4.5 Waktu generate data total MD5	46
Gambar 4.6 Hasil cracked satu baris pesan MD5	49
Gambar 4.7 Hasil cracked satu baris pesan SHA512	49
Gambar 4.8 Hasil cracked MD5 pesan MHS	50
Gambar 4.9 Hasil cracked SHA512 pesan MHS	51
Gambar 4.10 Data percobaan MD 5 dengan 9 karakter	52
Gambar 4.11 Data percobaan MD 5 dengan 10 karakter	53
Gambar 4.12 data percobaan MD 5 dengan 14 karakter	53
Gambar 4.13 data percobaan SHA512 dengan 3 karakter	54
Gambar 4.14 data percobaan SHA512 dengan 2 karakter	55
Gambar 4.15 data percobaan SHA512 dengan 1 karakter	55

DAFTAR TABEL

Tabel 1.1 Kategori security service pada jaringan mHealth	3
Tabel 2.1 Perbandingan Jurnal	8
Tabel 2.2 Security Threat Taxonomy	15
Tabel 2.3 Perbedaan Variasi Algoritma SHA	28
Tabel 2.2 deskripsi perintah pada hashcat	32
Tabel 2.3 deskripsi mode hash pada hashcat	32
Tabel 2.4 Deskripsi output format file pada hashcat	33
Tabel 2.5 Deskripsi jenis serangan dan kode pada hashcat	33
Tabel 2.6 Contoh serintah serangan dan urutan pada hashcat	33
Tabel 4.1 Jumlah bytes data lengkap	42
Tabel 4.2 Waktu generate data MD5	45
Tabel 4.3 Jumlah bytes data lengkap	46
Tabel 4.4 Jumlah bytes data baris 1	47
Tabel 4.5 Hasil kesimpulan perbandingan data yang tidak terlindungi dengan terlindungi MD5	47
Tabel 4.6 Perbandingan hasil hash MD5 dan SHA512 dengan data [MSH]	47
Tabel 4.7 Perbandingan hasil hash MD5 dan SHA512 dengan data	48
Tabel 4.8 Rata-rata waktu generate data MD5 baris pertama	49
Tabel 4.9 Rata-rata waktu generate data SHA512 baris pertama	50
Tabel 4.10 Rata-rata waktu generate MD5 data MHS	51
Tabel 4.11 Rata-rata waktu generate SHA512 data MHS	52
Tabel 4.12 Hasil kesimpulan perbandingan antara MD5 dan SHA512 pesan baris pertama	56
Tabel 4.13 Hasil kesimpulan perbandingan antara MD5 dan SHA512 dengan data MHS	56