

Analisis Pengamanan IoT Pada Surveillance Camera

by Rauf Endro Widagdo

Submission date: 20-Nov-2019 12:37PM (UTC+0700)

Submission ID: 1217155223

File name: Rauf_Endro_Widagdo-16523057.pdf (286.49K)

Word count: 1215

Character count: 7681

Analisis Pengamanan IoT Pada Surveillance Camera

Jurusan Informatika Fakultas Teknologi Industri
Universitas Islam Indonesia
Jl. Kaliurang km 14 Yogyakarta 55510

Abstrak—Internet of Things (IoT) merupakan teknologi baru yang menghubungkan mesin atau perangkat dengan jaringan internet agar dapat saling bertukar informasi sehingga dapat berjalan sesuai fungsinya. Adanya IoT dapat membantu aktivitas dalam berbagai bidang seperti bidang pertanian, energi, kesehatan, transportasi, dan lain lain. Karena IoT banyak digunakan di berbagai bidang, diperlukannya perhatian pada pengamanan perangkat IoT. Perangkat IoT yang ada saat ini memiliki sistem keamanan yang berbeda sesuai dengan jenis dan fungsinya. Contohnya Surveillance Camera yang memiliki sistem keamanan yang beragam. Lebih tepatnya sistem keamanan dengan menggunakan Secure Hash Algorithm pada sistem login dan enkripsi pada file. Pada artikel ini akan dilakukan analisis sistem keamanan login pada Surveillance Camera dengan melakukan tes performa untuk setiap Secure Hash Algorithm. Dengan menganalisis pengamanan pada sistem keamanan perangkat IoT yang ada, akan didapatkan sistem keamanan yang lebih efisien.

Kata Kunci — Internet of Things, Sistem Keamanan, Perangkat IoT, Surveillance Camera

I. PENDAHULUAN

Internet of Things (IoT) merupakan suatu hal yang baru untuk zaman sekarang. Berbagai macam perangkat sekarang telah menerapkan teknologi IoT, contohnya kamera pengawas (Surveillance Camera) yang sudah menerapkannya yang dapat mempermudah aktivitas dengan internet agar dapat berbagi data, pengendalian jarak jauh, monitoring, dan berbagai hal yang tentunya dengan hal tersebut dapat membuat pekerjaan lebih fleksibel. Selain sisi positif dari IoT terdapat juga sisi negatifnya. Seperti penyalahgunaan untuk melakukan tindak kejahatan. Maka dari itu keamanan sangat perlu diperhatikan demi mencegahnya tindakan-tindakan *cybercrime*.

Surveillance Camera memiliki berbagai macam sistem keamanan contohnya sistem login dengan menggunakan beberapa enkripsi pada password. Surveillance Camera yang ada saat ini menggunakan enkripsi password dan pengenkripsian file dengan algoritma yang berbeda-beda. Surveillance Camera bisa menggunakan algoritma-algoritma yang ada dan belum ada kepastian untuk menentukan

algoritma yang cocok. Sebagai sampe penulis menggunakan Secure Hash Algorithm (SHA) SHA-256 dan SHA-512 untuk dilakukan analisis. Setiap hash memiliki perhitungan rumus yang berbeda yang akan mempengaruhi keamanan dan performa pada perangkat IoT.

Dalam kasus ini, perangkat Surveillance Camera menggunakan raspberry pi dan modul kamera. Raspberry pi akan menjalankan program untuk menjadi Surveillance Camera

Dari penjelasan tersebut, dapat disimpulkan beberapa permasalahan yaitu pada sistem keamanan yang ada beragam dan belum ada kepastian untuk menentukan algoritma yang cocok.

Dengan permasalahan yang telah dijelaskan, penulis berkesimpulan bahwa perlu adanya analisis pada sistem keamanan yang ada agar dapat menentukan sistem keamanan yang tepat dan sesuai untuk perangkat Surveillance Camera tersebut.

II. KAJIAN PUSTAKA

A. Raspberry Pi

Raspberry Pi adalah komputer *single board* yang dikembangkan oleh Raspberry Pi Fondation dan berukuran seperti kartu kredit.[1] Raspberry Pi dirancang sebagai pendidikan dan terinspirasi oleh keberhasilan BBC Micro untuk mengajar pemrograman komputer hingga satu generasi.[2]

B. Apache

Apache Server menyediakan fasilitas distribusi online layanan situs web menggunakan HTTP (Hyper Text Transfer Protocol). [3]

C. MySQL

MySQL adalah database yang pada awal kemunculannya hanya berjalan untuk Unix dan Linux. Karena semakin banyak yang menggunakan MySQL, Diluncurkanlah versi untuk beberapa platform termasuk Windows.[4]

D. *Secure Hashing Algorithm 256(SHA-256)*

Fungsi kompresi SHA-256 beroperasi pada blok pesan 512-bit dan 256-bit. SHA-256 adalah algoritma chipper block 256-bit yang mengenkripsi nilai hash antara menggunakan blok pesan sebagai kunci.[5]

E. *Secure Hashing Algorithm 512(SHA-512)*

Fungsi kompresi SHA-512 beroperasi pada blok pesan 1024-bit dan 512-bit. SHA-512 adalah algoritma chipper block 512-bit yang mengenkripsi nilai hash antara menggunakan blok pesan sebagai kunci.[5]

Berikut adalah tabel perbandingan antara algoritma SHA-256 dan SHA-512 yang ditampilkan pada Tabel 1

Tabel 1. Perbandingan algoritma SHA-256 dan SHA-512[6]

Algoritma	Message Length (bit)	Block Size (in bits)	Word Size (in bits)	The Size of the Message Digest (bit)
SHA 256	<2 ⁶⁴	512	32	256
SHA 512	<2 ¹²⁸	1024	64	512

III. METODOLOGI

Tahapan-tahapan yang dilakukan adalah:

A. Tahapan Penelitian

Terdapat beberapa langkah yang dilakukan dalam tahapan ini seperti :

1. Pengumpulan data : melakukan pengumpulan literatur dari artikel, buku, jurnal, dan lain-lain.
2. Penyiapan alat : menyiapkan alat-alat yang dibutuhkan untuk melakukan perancangan baik *hardware* maupun *software*.
3. Perancangan dan pemasangan software: membuat rancangan perangkat lalu kemudian memasang *software* yang ingin dijalankan.
4. Pengujian : sistem yang telah siap kemudian dilakukan pengujian untuk memastikan bahwa sistem berjalan normal.

B. Alat dan Bahan

1. *Hardware*

Berikut adalah tabel perangkat keras yang digunakan untuk membuat *Surveillance Camera* yang akan ditampilkan pada tabel 2.

Tabel 2. Perangkat keras untuk membuat *Surveillance Camera*

No	Alat
1	Raspberry Pi
2	Micro SD
3	Modul Kamera
4	Kabel Micro USB

2. *Software*

Berikut adalah tabel perangkat lunak yang digunakan untuk membuat *Surveillance Camera* yang akan ditampilkan pada tabel 3.

Tabel 3. Perangkat lunak untuk *Surveillance Camera*

No	Nama Software	Fungsi
1	Raspbian	Sistem Operasi Raspberry Pi
2	Apache	Sebagai <i>Web Server</i>
3	Mysql	Sebagai penyimpanan database
4	Python	Program pendukung modul kamera

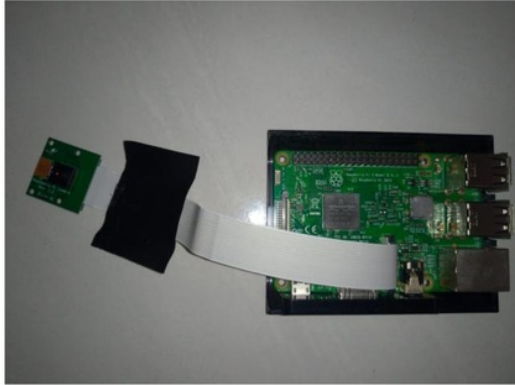
C. Perancangan dan Pemasangan Software

1. Perancangan Perangkat Keras

Pada tahapan ini akan dilakukan pemasangan Raspberry Pi dengan modul kamera.



Gambar 1. Modul Kamera



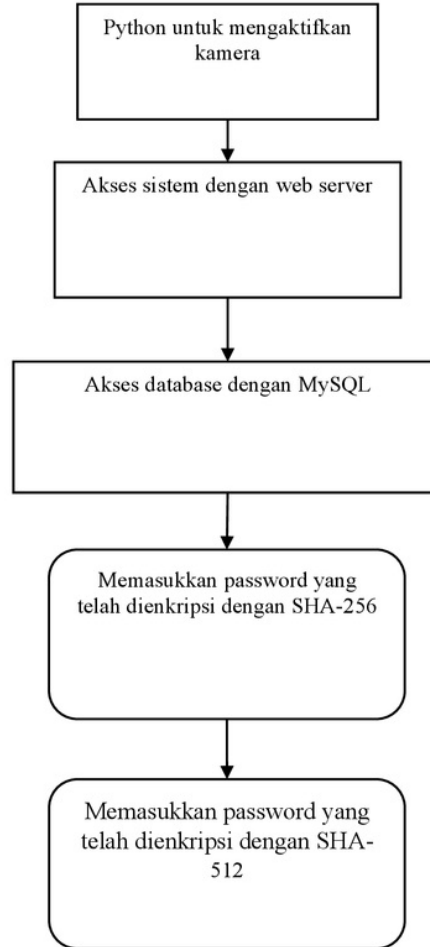
Gambar 2. Pemasangan modul kamera ke Raspberry Pi



Gambar 3. Perangkat yang telah siap digunakan

2. Pemasangan Software

Pada tahap ini akan dilakukan pemasangan software yang akan ditampilkan pada gambar berikut:



Gambar 4. Pemasangan Software

D. Pengujian

Pengujian dilakukan dengan menggunakan *function* php untuk mengukur *speed performance* dari setiap enkripsi password. Berikut adalah tabel *function* php dan tabel password yang telah di enkripsi pada yang akan ditampilkan pada tabel 4 dan tabel 4.

Tabel 4. *Function* php

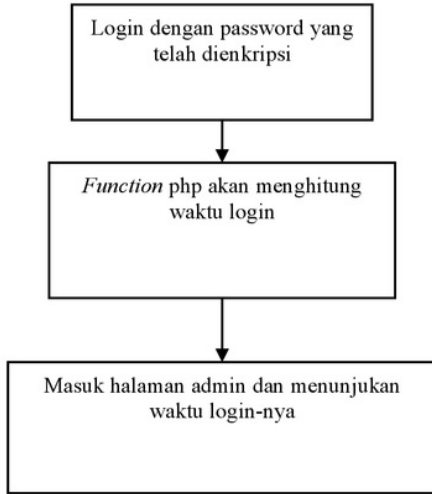
```

    $start = microtime(true);
    $finish = microtime(true);
    Print 'Page generated ini : ' round(($finish - $start)
    * 10000, 2) . ' <small>ms</small>'
  
```

Tabel 5. Password yang telah dienkripsi

No.	Nama	Password	Enkripsi
1	SHA-256	tes123	57776e8a41ff487b37a6b34186486b0e2f886e2cbf12a8e30d56dc67ea778193
2	SHA-512	tes123	f1cc9ea66b75fe623fd793c3e7df7910f8312a8827a17307be920584afcdb6c7dac2ced03c82715432fb958857cacc12a363ee253e9b8d2cad44d626d7129247

Skenario pengujian akan dilakukan seperti gambar berikut:



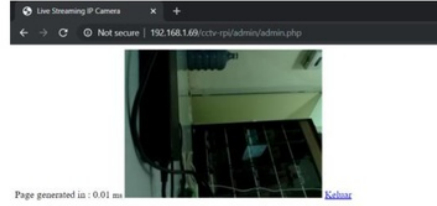
Gambar 5. Skenario Pengujian

IV. HASIL DAN PEMBAHASAN

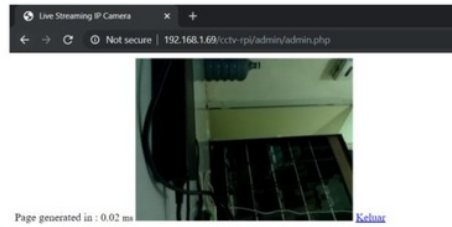
Setelah dilakukan pengujian didapat lah hasil seperti tabel 5 dan gambar berikut:

Tabel 5. Hasil pengujian

No	Nama	Waktu login
1	SHA-256	0.01 ms
2	SHA-512	0.02 ms



Gambar 6. Hasil SHA-256



Gambar 7. Hasil SHA-512

Sesuai pada hasil yang diperoleh, enkripsi SHA-256 lebih cepat dibandingkan dengan SHA-512. Itu dikarenakan jumlah karakter pada kedua enkripsi yang berbeda yaitu SHA-256 yang memiliki 64 karakter dan SHA-512 yang memiliki 128 karakter.

V. KESIMPULAN

Penulis menyimpulkan bahwa walaupun keduanya memiliki perbedaan waktu tetapi waktu tersebut tidak menjadi masalah karena perbedaan yang sangat kecil. Penulis menyarankan untuk memilih SHA-512 karena memiliki jumlah karakter yang lebih banyak yaitu 128 karakter daripada memilih SHA-256 yang hanya memiliki 64 karakter.

VI. REFERENSI

VII. REFERENCES

- [1] P. Bhaskar, "Raspberry Pi Home Automation With Wireless Sensors Using Smart Phone," *Int. J. Comput. Sci. Mob. Comput.*, vol. 45, no. 5, pp. 797–803, 2015.

- [2] ³ W. Harrington, *Learning Raspbian*. 2015.
- [3] T. Thaker, "ESP8266 based implementation of wireless sensor network with Linux based web-server," *2016 Symp. Colossal Data Anal. Networking, CDAN 2016*, 2016.
- [4] ⁵ Rini Sovia dan Jimmy Febio, "MEMBANGUN APLIKASI E-LIBRARY MENGGUNAKAN HTML, PHP SCRIPT, DAN MYSQL DATABASE Rini Sovia dan Jimmy Febio," *Processor*, vol. 6, no. 2, pp. 38–54, 2011.
- [5] ⁴ "Sha256-384-512."
- [6] M. Sumagita and I. Riadi, "Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application," vol. 7, no. September, pp. 373–381, 2018.

Analisis Pengamanan IoT Pada Surveillance Camera

ORIGINALITY REPORT

14%

SIMILARITY INDEX

8%

INTERNET SOURCES

5%

PUBLICATIONS

12%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universiti Teknikal Malaysia Melaka Student Paper	2%
2	Submitted to Universitas Brawijaya Student Paper	2%
3	Submitted to Universiti Malaysia Perlis Student Paper	2%
4	Submitted to University of Maryland, University College Student Paper	2%
5	180.242.78.39 Internet Source	1%
6	de.scribd.com Internet Source	1%
7	mafiadoc.com Internet Source	1%
8	hmte.ft.uns.ac.id Internet Source	1%

9

Submitted to Universitas Sebelas Maret

Student Paper

1%

10

Submitted to Unika Soegijapranata

Student Paper

1%

11

Submitted to Universiti Teknologi Malaysia

Student Paper

1%

Exclude quotes Off

Exclude matches Off

Exclude bibliography On