PERFORMASI KALKULASI HASH SHA-1 PADA SISTEM EMBBEDED ARDUINO

PERFORMANCE CALCULATION OF HASH SHA-1 IN EMBEDDED SYSTEM USING ARDUINO

Gembong Edhi Setyawan[1], Aryo Pinandito[2], Fajar Pradana[3]

Program Teknologi Informasi dan Ilmu Komputer (PTIIK), Universitas Brawijaya
Malang gembong@ub.ac.id[1],aryo@ub.ac.id[2], fajar.p@ub.ac.id[3]
Naskah diterima 16 Februari 2015, direvisi 2 Maret 2015, diterima 25 Maret 2015

Abstract

The development of digital electronic devices that can communicate with each other causing the need for data security or data protection. However, in the many digital electronic devices are not equipped with security or protection of the data. In this study has the main objective to design an embedded system that can be added to the digital electronic devices to provide security or protection of the data. As the initial phase of the study, in this paper have measured performance data security in embedded systems with Arduino using a cryptographic algorithm SHA-1 hash function. Performance of SHA-1 hash calculation using linear regression approach of measurement results show for 1 byte of data takes time 2,505 ms. Each additional 1 byte of data calculation time hash function SHA-1 increased 0.0715 ms.

Keywords: *arduino, cryptography, data security, embedded system, hash function, SHA-1*

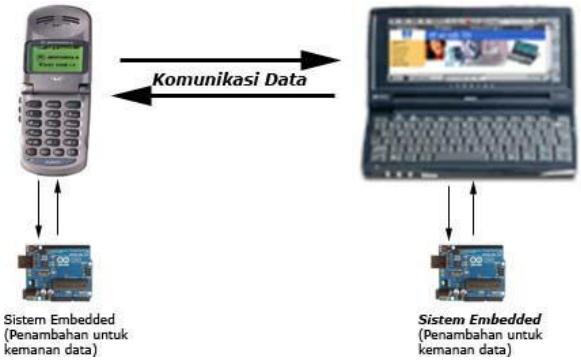
Abstrak

Perkembangan perangkat elektronik digital yang bisa berkomunikasi satu sama lain menyebabkan adanya kebutuhan terhadap keamanan atau perlindungan data. Akan tetapi di perangkat elektronik tersebut belum banyak dilengkapi dengan keamanan atau perlindungan terhadap data. Pada penelitian ini mempunyai tujuan utama untuk merancang suatu sistem embedded yang dapat ditambahkan ke dalam perangkat elektronik tersebut untuk memberikan keamanan atau melindungi terhadap data yang akan dikomunikasikan. Sebagai tahap awal dari penelitian, di makalah ini telah mengukur performansi keamanan data di sistem embedded arduino menggunakan algoritma kriptografi dengan fungsi hash SHA-1. Performansi kalkulasi hash SHA-1 menggunakan pendekatan regresi linear dari hasil pengukuran menunjukkan untuk 1 byte data membutuhkan waktu 2,505 ms. Setiap penambahan 1 byte data waktu kalkukasi fungsi hash SHA-1 bertambah 0,0715 ms.

Kata Kunci: arduino, fungsi hash, keamanan data, kriptografi, SHA-1, sistem embedded

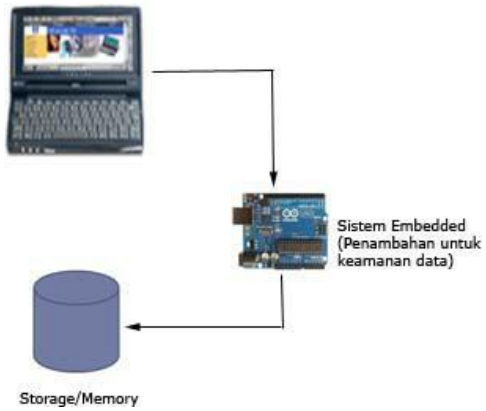
PENDAHULUAN

Pertumbuhan perangkat elektronik digital dari tahun ke tahun sangatlah pesat. Perkembangan teknologi komunikasi menyebabkan banyak perangkat elektronik digital ini bisa saling berkomunikasi satu sama lain. Akan tetapi, banyak dari perangkat elektronik digital ini yang belum menerapkan sistem keamanan data. Penelitian ini mempunyai tujuan utama, yaitu merancang suatu sistem embedded yang dapat ditambahkan ke perangkat elektronik digital untuk memberikan keamanan atau perlindungan pada data. Ada dua hal yang bisa diterapkan dengan penambahan sistem embedded diperangkat elektronik digital ini, yaitu menjamin perlindungan data pada saat komunikasi antara dua perangkat dan menjamin keamanan data di memory perangkat tersebut. Secara garis besar tujuan utama dari penelitian ini dapat dilihat pada Gambar 1 dan Gambar 2. Sistem embedded merupakan suatu sistem komputer yang dirancang untuk melakukan fungsi khusus dan terdiri dari perangkat keras serta perangkat lunak yang dituntut untuk bekerja secara real time (Bourahla, 2009). Selain itu, sistem embedded adalah suatu sistem yang tertanam dan sebagai bagian dari suatu sistem komputer yang lengkap. Namun jika dibandingkan dengan komputer PC pada umumnya, sistem embedded memiliki kemampuan pengolahan data dan memori yang lebih kecil.



Gambar 1. Penambahan sistem embedded untuk memberikan keamanan data pada perangkat elektronik yang berkomunikasi

Pada tahun 2001, Peter Shipley dan Simson L Garfinkel mempublikasikan analisisnya bahwa modem ketika terhubung dengan jaringan internet tidaklah aman (Shipley, 2001). Modem merupakan salah satu perangkat elektronik digital yang dapat berkomunikasi dengan perangkat lain melalui jaringan internet,sehinggadapat dikatakan bahwa suatu perangkat elektronik digital tingkat tidak amannya terhadap data yang dikirimkan atau diterima akan meningkat tajam jika terhubung dengan jaringan internet (Koopman, 2009).



Gambar 2. Penambahan sistem embedded untuk memberikan keamanan pada data yang disimpan di memori

Beberapa perangkat aplikasi elektronik sekarang ini dapat berkomunikasi dengan perangkat elektronik lainnya atau dengan komputer (Jyostna, 2011), misalnya dari mobil ke handphone dan peralatan video ke MP3 player (Koopman, 2009). Akan tetapi, keamanan data untuk perangkat-perangkat ini masih banyak yang belum menerapkan dan dalam jangka waktu ke depan akan jadi suatu permasalah tersendiri (Koopman, 2009). Perkembangan dari perangkat elektronik yang dapat berkomunikasi melakukan transfer data melalui jaringan komunikasi dibutuhkan perlindungan atau keamanan data di perangkat elektronik tersebut. Dikarenakan jarangnya perangkat elektronik yang menerapkan keamanan data, maka pada penelitian ini timbul suatu ide untuk menambahkan suatu sistem embedded yang dapat memberikan perlindungan terhadap data tersebut, seperti terlihat pada Gambar 1 dan Gambar 2.

Salah satu metode untuk memberikan keamanan pada data yaitu dengan menggunakan metode kriptografi. Jenis algoritma metode kriptografi yang sering digunakan adalah algoritma simetri, asimetri dan fungsi hash. Pada penelitian ini akan menggunakan fungsi hash untuk diterapkan dalam sistem embedded arduino. Fungsi hash adalah suatu teknik klasik yang paling banyak digunakan dalam praktek secara mendalam. Untuk memenuhi persyaratan dalam aplikasi, beberapa metode standard untuk fungsi hash telah dikembangkan di antaranya yaitu MD4 (Rivest, 1992), MD5 (Rivest, 1992), SHA-1 (____, 2008) dan SHA-2 (____, 2008). Fungsi hash cenderung sangat cepat untuk diterapkan pada arsitektur mikroprosesor modern (Osvik, 2012), sehingga sangat cocok untuk diterapkan pada sistem embedded. Salah satu arsitektur mikroprosesor yang banyak digunakan dalam sistem embedded adalah arduino. Arduino menggunakan mikrokontroler AVR ATMega yang memungkinkan sebuah program dijalankan didalamnya. Saat ini sistem embedded berbasis arduino dapat digunakan untuk aplikasi transmisi data. Untuk menjamin keamanan data yang ditransmisikan maka data yang ditransmisikan perlu dikalkulasikan nilai hash-nya. Pada penelitian ini diimplementasikan salah satu metode enkripsi hash SHA-

1 untuk melindungi data yang ditransmisikan pada sistem embedded yang menggunakan arduino. Sehingga nantinya data yang telah melewati proses hashing akan lebih aman dari interupsi. Selain untuk melindungi data, proses hash juga bisa dilakukan untuk menjamin bahwa data yang dikirimkan adalah benar. Teknik ini biasa digunakan dalam enkripsi data, misalnya untuk menyimpan password agar tidak ada yang dapat mengetahuinya meskipun dia dapat melihat hash dari password itu. Hash atau hashing sendiri adalah proses perubahan suatu data menjadi data lain dengan panjang tertentu, sedemikian sehingga data itu tidak dapat dipulihkan kembali.

Sebagai tahap awal penelitian, untuk menerapkan keamanan data di sistem embedded maka perlu diketahui terlebih dulu kinerja dari metode kriptografi di sistem embeded. Oleh sebab itu pada makalah ini masih dibatasi pada tahap awal penelitian yang membahas performansi salah satu metode kriptografi pada sistem embedded. Berdasarkan penelitian Osvik (2012), Sklavos (2012) dan Jarvinen (2004) metode kriptografi yang digunakan adalah kalkulasi fungsi hash SHA-1, dan berdasarkan Javale (2013) sistem embedded yang digunakan adalah arduino. Pengukuran performansi kalkulasi hash SHA-1 pada sistem embedded arduino di makalah ini, disusun sebagai berikut. Pada bagian II dibahas tentang tinjauan pustaka yang mengulas tentang implementasi metode kriptografi di sistem embedded yang telah dilakukan sebelumnya. Kemudian, pada bagian III dibahas tentang metodologi penelitian yang diantaranya menjelaskan implementasi metode kriptografi hash SHA-1 dan perancangan program untuk menguji kinerja implementasi hash SHA-1 pada sistem embedded arduino. Selanjutnya dibagian IV tentang hasil dan pembahasan. Dibagian V merupakan kesimpulan dari makalah ini. Selanjutnya dituliskan daftar pustaka serta lampiran yang berupa hasil pengukuran performansi kalkulasi hash SHA-1 pada sistem embedded arduino.

Tinjauan Pustaka

Algoritma hash yang umum digunakan pada aplikasi yang menggunakan teknik kriptografi adalah SHA-1 dan MD5. Umumnya teknik kriptografi dengan menggunakan hash ini digunakan untuk menyimpan password karena sifatnya yang satu arah. Kebanyakan sistem elektronik modern, seperti PC, PDA, telephone seluler, *network router* dan *smart card* memerlukan kemampuan akses, menyimpan, memanipulasi, atau mengkomunikasikan informasi yang bersifat sensitif. Sehingga keamanan menjadi hal yang serius untuk diterapkan dalam desain sistem tersebut. Sistem-sistem embedded yang terkait dengan berbagai macam produk elektronik, telekomunikasi dan jaringan komputer menghadapi kebutuhan akan keamanan informasi. Di satu sisi sumber daya yang dimiliki sistem embedded sangat terbatas, di sisi lainnya sistem embedded tersebut sering dioperasikan dalam lingkungan yang tidak aman secara fisik (Ravi, 2004).

Arduino adalah papan rangkaian elektronik *open source* yang didalamnya terdapat komponen utama, yaitu sebuah mikrokontroler dengan jenis AVR dari perusahaan Atmel. Karena sifatnya yang *open source* banyak suatu sistem aplikasi yang berbasis pada arduino, misalkan pengendali otomatis perangkat rumah / *home automation* (Javale, 2013). Didalam aplikasi *home automation* (Javale, 2013) tersebut, terdapat komunikasi antara telephone seluler yang berbasis android, sistem embedded arduino dan perangkat elektronik rumah. Didalam aplikasi tersebut, terjadi komunikasi data antara perangkat, akan tetapi data yang ditransfer sama sekali tidak diamankan, sehingga sangat rentan sistem *home automation* tersebut dapat dikendalikan oleh orang lain.(Sklavos, 2012) dalam penelitiannya mengatakan bahwa kriptografi untuk arduino, yang mempunyai komputasi perhitungan terbatas, saat ini hanya ada dua alternatif metode enkripsi yang cocok, yaitu MD5 dan *cryptography suite* untuk arduino. Cryptography suite mendukung hashing menggunakan SHA-1, SHA-2, HMAC-SHA-1 dan HMAC-SHA-2. Implementasi kriptografi pada sistem embedded sebelumnya pernah dilakukan oleh Jarvinen (2004). Di dalam penelitiannya, diimplementasikan metode enkripsi SHA-1 pada sistem embedded FPGA. Selain dari pada itu juga jelaskan perbandingan implementasi SHA-1 dan MD5 pada sistem embedded FPGA. Didalam kesimpulannya dijelaskan bahwa SHA-1 merupakan metode yang tercepat dan paling ringkas untuk diterapkan pada FPGA.

Selain itu, SHA-1 juga memberikan kinerja yang stabil. Berdasarkan penelitian terdahulu (Javale, 2013; Sklavos, 2012 dan Jarvinen, 2004), maka dalam penelitian ini metode hash SHA-1 untuk diimplementasikan dalam sistem embedded arduino.

Metode Penelitian

a) Implementasi Hash SHA-1 pada Sistem Embedded Arduino

Implementasi hash SHA-1 pada sistem embedded arduino adalah dengan membuat library SHA-1, pembuatan program kalkulasi SHA-1 dan pengujian hasil dari kalukulasi hash SHA-1. SHA-1 termasuk ke dalam *one way hash function*. Algoritma SHA-1 mengambil *input* dengan panjang sembarang, dan sebagai *output*-nya adalah suatu *fingerprint* atau *digest* sepanjang 160 *bit* (_____, 2008). SHA dibuat oleh NIST dan digunakan bersama DSS (*Digital Signature Standard)*. Oleh NSA, SHA dinyatakan sebagai standar fungsi hash satu-arah. SHA didasarkan pada MD 4 yang dibuat oleh Rivest dari MIT. Algoritma ini menerima masukan berupa pesan dengan ukuran maksimum 264 bit dan menghasilkan digest yang panjangnya 160 bit yang lebih panjang dari MD5. SHA-1 adalah algoritma yang dipakai untuk mengenkripsi data, biasanya algoritma ini digunakan untuk mengacak password menjadi barisan code-code acak yang tidak dapat dibaca. SHA-1 menawarkan alternatif lain dalam algoritma enkripsi informasi. SHA-1 menghasilkan 40bit karakter enkripsi, Sehingga SHA-1 memberikan

pengacakan lebih banyak, dan peluang untuk meng-deskripsi lebih besar.

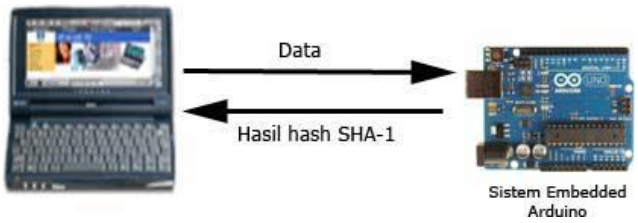
Langkah-langkah pembuatan *message digest* dengan SHA-1 adalah sebagai berikut:

1) Ubah pesan *m* menjadi *message digest* dengan fungsi hash SHA-1
2) Tentukan bilangan acak k<q
3) Tanda tangan dari pesan *m* adalah bilangan *r* dan *s*

   $r=(g^k \bmod p) \bmod q$

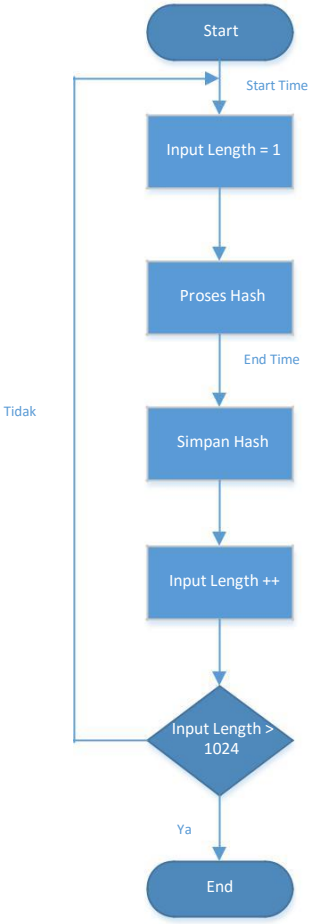
   $s = (k^{-1} (H(m) + x*r)) \bmod q$
4) Kirim pesan *m* beserta tanda-tangan *r* dan *s*

Gambar implementasi program SHA-1 dapat dilihat pada Gambar 3.



Gambar 3. Implementasi program SHA-1 pada arduino

Flowchart untuk implementasi program SHA-1 dapat dilihat pada Gambar 4.

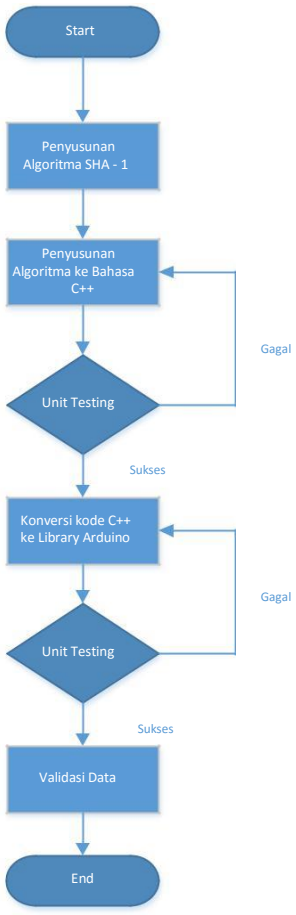


Gambar 4. Flowchart untuk implementasi program SHA-1 pada arduino

b) Pengukuran Performansi Hash SHA-1 pada Sistem Embedded Arduino

Pengukuran performansi hash SHA-1 dilakukan dengan menghitung waktu kalkulasi SHA-1 pada sistem embedded arduino. Pengujian dilakukan dengan mengirimkan data dari komputer dari 1 karakter (1 byte) sampai dengan 1024 karakter (1 MB), kemudian data tersebut diproses di sistem embedded arduino dan menghasilkan hash untuk dikirimkan kembali hasilnya dikomputer. Pada saat proses kalkulasi hash di arduino inilah, waktu kalkulasi akan dihitung di setiap data yang dikirim.

Waktu kalkulasi ini dibutuhkan untuk mengukur kinerja atau kecepatan arduino dalam melakukan pengubahan data menjadi fungsi hash SHA-1. Flowchart untuk menghitung waktu kalkulasi SHA-1 di sistem embedded arduino ini dapat dilihat pada Gambar 5.



Gambar 5. Flowchart pengukuran performansi kalkulasi Hash SHA-1 pada arduino

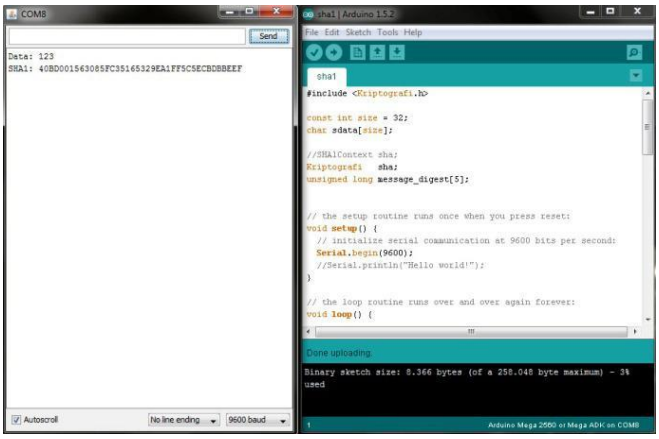
HASIL PENELITIAN DAN PEMBAHASAN

Berangkat dari penyajian di bagian latar belakang, tinjauan teoritis dan metode penelitian dapat dilakukan penyajian data penelitian yang kemudian dilakukan pembahasan untuk menjelaskan berbagai hal yang berkaitan dengan hasil temuan.

A. Hasil Program Kalkulasi Hash SHA-1

Pembuatan program kalkulasi SHA-1, dilakukan di arduino. Untuk menguji apakah program tersebut berhasil atau tidak, input akan diberikan melalui komputer dan hasil hash akan dikirimkan kembali ke komputer. Hasil program dapat dilihat pada Gambar 6.

Pada Gambar 6 diuji dengan memasukkan data "123" dan hasil kalkulasi hash nya adalah "40BD001563 085FC35165329EA1FF5C5ECBDBBEEF".



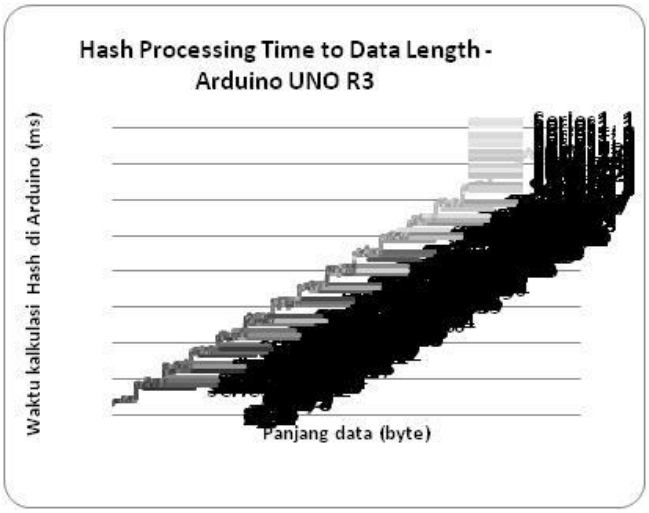
Gambar 6. Hasil program kalkulasi hash SHA-1

B. Hasil Pengukuran Performansi Kalkulasi Hash SHA-1 pada Sistem Embedded Arduino

Pengujian kinerja kalkulasi SHA-1 di arduino dilakukan dengan membuat program yang berfungsi untuk menghitung waktu pada pada proses kalkulasi SHA-1 di arduino. Pengujian dilakukan dengan memasukkan data dari 1 karakter (1 byte) sampai dengan 1024 karakter atau 1 MB. Tabel hasil pengujian dapat dilihat pada Tabel 1, sedangkan grafik hasil pengujian dapat dilihat pada Gambar 7.

Tabel 1.
Pengukuran kalkulasi hash SHA-1 pada arduino

Pjng Data	Waktu (ms)	SHA-1 Hash
0	3	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
1	4	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
2	4	FB96549631C835EB239CD614CC6B5CB7D295121A
3	4	8AEFB06C426E07A0A671A1E2488B4858D694A730
4	4	39DFA55283318D31AFE5A3FF4A0E3253E2045E43
5	4	6934105AD50010B814C933314B1DA6841431BC8B
6	4	C984AED014AEC7623A54F0591DA07A85FD4B762D
7	4	4E079D0555E5A2B460969C789D3AD968A795921F
8	4	70352F4161EDA4FF3C322094AF068BA70C3B38B
9	4	F58D5A5515F1A8A9D179AA58858B67B2F8A3388
10	4	8104BA1DC0409B259F487ED07DB477C38F205A30
. . .	. . .	. . .
1024	77	A0A32B159FECA49E7B13B9A49AE0127ADE587F8B



Gambar 7. Grafik performansi kalkulasi hash SHA-1 pada arduino

Berdasarkan tabel yang diperoleh pada Tabel 1 dan grafik pada Gambar 7, berapapun besarnya data yang akan dikalkulasi hash dapat diprediksi dengan menggunakan regresi linier. Misalkan panjang data adalah x, sedangkan waktu kalkulasi di arduino adalah y, gambar grafik dapat kita prediksi dengan persamaan regresi linear:

$$= + . \quad (1)$$

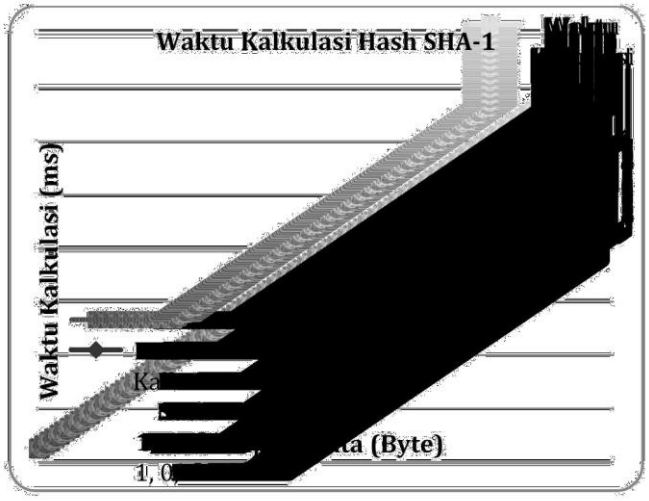
$$= \frac{\Sigma = \Sigma = \blacklozenge\blacklozenge \Sigma =}{\Sigma = ^2 - \Sigma = \blacklozenge^2} \quad (2)$$

$$= \frac{\Sigma =}{} - \frac{\Sigma =}{} \quad (3)$$

Berdasarkan persamaan (2) dan (3), persamaan regresi linear dapat diperoleh sebagai berikut:

$$= 2{,}43 + 0{,}0715 \quad (4)$$

Dari persamaan (4) dapat diperoleh grafik performansi kalkulasi hash SHA-1 dengan regresi linear pada Gambar 8.



Gambar 8. Grafik performansi kalkulasi hash SHA-1 pada arduino dengan regresi linear

Berdasarkan hasil dari regresi linear 1 byte data mempunyai waktu kalkulasi hash SHA-1 di arduino sebesar 2,5015 ms, sedangkan untuk 1 MB data mempunyai waktu kalkulasi sebesar 75,64 ms. Setiap penambahan 1 byte data, waktu kalkulasi akan bertambah sebesar 0,0715 ms.

PENUTUP

Pada makalah ini telah melakukan implementasi metode kriptografi hash SHA-1 di sistem embedded arduino. Performansi kalkulasi hash SHA-1 di sistem embedded arduino dihitung dengan mengukur waktu kalkulasi hash SHA-1 di sistem embedded arduino. Kalkukasi SHA-1 di sistem embedded arduino untuk data sebesar 1 byte membutuhkan waktu 2,50515 ms dan setiap penambahan data sebesar 1 byte dibutuhkan penambahan waktu sebesar 0,0715 ms.

DAFTAR PUSTAKA

_____, (2008), "Secure Hash Standard", National Institute of Standards and Technology, NIST FIPS PUB, 180-3, U.S. Department of Commerce

Baurahla, M., (2009), Modelling and Verification of Real-time Embedded System, Proceeding ISIICT'09 Proceedings of the Third international conference on Innovation and Information and Communication Technology, British Computer Society Swinton, UK.

Jarvinen, K., (2004), Design and Implementation of a SHA-1 Hash Module on FPGAs, Otakaari 5A, Espoo, FIN-02150, Finland.

Javale, D., Mohsin, M., Nandanwar, S., Shingate, M., (2013), Home Automation and Security System using Android ADK, International Journal of Electronics Communication and Computer Technology (IJECCT), Volume 3 Issue 2.

Jyostna, K., Padmaja, V., 2011, Secure Embedded System Netwroking: An Advance Security Perspective, International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, Vol 3 No.5

Koopman, P., 2004, Embedded System Security, IEEE Computer Society, Embedded Computing.

Ravi, S., Raghunathan, A., Kocher, P., Hatangady, S., 2004, Security in Embedded Systems: Design Challenges, ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, Pages 461–491, Broadway, New York.

Rivest, R., 1992, The MD4 Message-Digest Algorithm, RFC 1320 (Informational)

_____, 1992, The MD5 Message-Digest Algorithm, RFC 1321 (Informational)

Shipley, P., Garfinkel, S.L., 2001, An Analysis of Dial-Up Modems and Vulnerabilities, Copyright Spring.