INTISARI

INTEGRITAS DAN KEAMANAN PENGIRIMAN DATA DARI PERANGKAT IoT KE *CLOUD STORAGE* MENGGUNAKAN ALGORITME KECCAK DAN *DIGITAL SIGNATURE ALGORITHM (DSA)*

Oleh

Muhammad Asghar Nazal
16/403701/PPA/05218

Cloud computing merupakan teknologi yang menggunakan pusat server sebuah provider yang bersifat virtual dan dapat memberikan pelayanan terhadap penggunaan *software*, penyimpanan data, jaringan, serta komputasi data. Data security menjadi sangat penting ketika menggunakan *cloud computing*, salah satu penelitian yang sedang berjalan dan menggunakan teknologi *cloud* sebagai sarana penyimpanan adalah *G-Connect*. Salah satu pengembangan yang dilakukan projek *G-Connect* adalah mengenai keamanan pada data, terutama dalam masalah verifikasi data yang dikirim. Tanda tangan digital merupakan suatu cara yang dapat digunakan untuk memverifikasi data, salah satu algoritme untuk membuat tanda tangan digital adalah RSA. Pada penelitian sebelumnya, algoritme Keccak dan RSA telah diimplementasikan untuk kebutuhan verifikasi data. Namun setelah dilakukan studi literatur mengenai algoritme lainnya yang dapat membuat tanda tangan digital, ditemukan bahwa terdapat sebuah algoritme yang lebih baik dari RSA dalam segi kecepatan, yaitu *Digital Signature Algorithm* (DSA).

DSA merupakan salah satu algoritme kunci yang digunakan untuk tanda tangan digital, namun karena DSA masih menggunakan Secure Hash Algorithm (SHA-1) sebagai algoritme untuk hash maka DSA sudah jarang digunakan untuk keperluan keamanan data, sehingga dipilih dan digunakan algoritme Keccak sebagai pengganti algoritme hash pada DSA. Algoritme Keccak merupakan pemenang kompetisi yang diselenggarakan oleh NIST dan telah dijadikan standar untuk algoritme fungsi hash SHA-3 yang baru. Karena permasalahan di atas maka fokus penelitian ini adalah pada bidang keamanan khususnya pada data cloud dengan permasalahan pengamanan data menggunakan algoritme Keccak dan *Digital Signature Algorithm* (DSA). Hasil dari penelitian ialah terbukti bahwa algoritme Keccak dapat berjalan pada sistem kerja DSA, diperoleh perbandingan waktu eksekusi khususnya dalam segi kecepatan *Signing* dan *Verifying* antara DSA dan RSA di mana keduanya menggunakan algoritme Keccak.

Kata Kunci: ***Cloud Computing, Internet of Things*, *G-Connect Project*, Algoritme Keccak, *Digital Signature Standard*, *Digital Signature Algorithm***

ABSTRACT

INTEGRITY AND SECURITY OF DATA DELIVERY FROM IoT DEVICETO CLOUD STORAGE USING KECCAK ALGORITHM AND DIGITAL SIGNATURE ALGORITHM (DSA)

by

Muhammad Asghar Nazal
16/403701/PPA/05218

Cloud computing is a technology that uses a central service provider that acts virtual and can provide services to the use of software, data storage, networks, and computing data. Data security is a very important compilation using cloud computing; one of the research that is running and using cloud technology as a means of storage is G-Connect. One of the developments made by the G-Connect project is about data security; most of the problems verification of the data sent. A digital signature is a method that can be used to verify data; one of the algorithms for making digital signatures is RSA. In previous studies, the Keccak and RSA algorithms have implemented for data verification needs. But after a literature study of other algorithms that can make digital signatures, we found what is meant by an algorithm that is better than RSA in rectangular speeds, namely Digital Signature Algorithm (DSA).

DSA is one of the key algorithms used for digital signatures, but because DSA still uses Secure Hash Algorithm (SHA-1) as an algorithm for hashes, DSA rarely used for data security purposes, so the Keccak algorithm is used instead of the hash algorithm on DSA. The Keccak algorithm is the winner of the competition organized by NIST and has become the standard for the new SHA-3 hash function algorithm. Because of the above problems, the focus of this research is in the field of security, especially in cloud data with the problem of securing data using the Keccak algorithm and Digital Signature Algorithm (DSA). The results of the research are proven that the Keccak algorithm can run on the DSA work system, obtained a comparison of execution time especially in terms of the speed of Signing and Verifying between DSA and RSA where both use the Keccak algorithm..

Keywords: **Cloud Computing, Internet of Things, G-Connect Project, Keccak Algorithm, Digital Signature Standard, Digital Signature Algorithm.**