PERANCANGAN SISTEM PEMINDAIAN DAN AUTENTIKASI PERANGKAT PENGGUNA FOG COMPUTING PADA JARINGAN WIFI

DESIGN OF SCANNING AND AUTHENTICATION SYSTEM FOR FOG COMPUTING DEVICES ON WIFI NETWORK

[1]Andri Rifky Aditama, [2]Favian Dewanta, [3]Ratna Mayasari

[1,2,3] Universitas Telkom, Bandung

[1] andririfkya@student.telkomuniversity.ac.id, [2]favian@telkomuniversity.ac.id, [3]ratnamayasari@telkomuniversity.ac.id

Abstrak

Fog computing **adalah komputasi desentralisasi di mana data, perhitungan, data penyimpanan berada di antara** *end-user* **dan** *cloud***. Yang membedakan** *Fog computing* **dengan** *cloud* **adalah kedekatannya dengan pengguna akhir dan mendukung mobilitas layanan, dan host di** *edge network* **atau** *end device* **seperti set-top-box atau jalur akses. Dengan demikian, Fog dapat mengurangi latensi layanan, meningkatkan QoS, serta menghasilkan pengalaman pengguna yang superior. Pada tugas akhir ini dibuat sebuah aplikasi pemindaian dan autentikasi perangkat pengguna pada** *fog computing***. Pembuatan aplikasi ini memanfaatkan aplikasi berbasis Android sebagai aplikasi bergerak (mobile application) dan *WiFi* sebagai jaringan pendukung dalam pembuatan aplikasi pemindaian dan autentikasi fog computing server. Dalam pengujian, penulis menganalisis delay dan besar paket pada dua protokol keamanan yaitu J-PAKE dan** *xor and hash***. Hasil eksperimen pada tugas akhir ini memperlihatkan bahwa delay protokol** *xor and hash* **lebih besar dibanding J-PAKE tetapi besar paket yang dikirim lebih kecil. Kemudian penulis mendapatkan kesimpulan tambahan bahwa spesifikasi perangkat mempengaruhi delay proses autentikasi.**

Kata kunci : *Fog computing*, Autentikasi, Protokol, J-PAKE, *xor and hash*, Pemindaian

Abstract

***Fog computing* is decentralized computing where data, computation, storage data are located between the *end-user* and the *cloud*. What distinguishes *Fog computing* from the *cloud* is its proximity to end users and support for mobility services, and hosts on the network *edge* or**

end devices such as set-top-boxes or access points. Thus, Fog reduces service latency, and improves QoS, resulting in a superior user experience. In this final project, an application for scanning and authenticating user devices in fog computing is developed. The development of this application utilizes an Android-based application as a mobile application and a *Wi-Fi* as a support network in making fog computing server authentication and scanning applications. During the test, the authors analyzed the delay and packet size in two security protocols, namely J-PAKE and *xor and hash*. The experimental results in this final project show that the *xor and hash* protocol delay is greater than J-PAKE but the packet size sent during transaction is smaller, furthermore, the authors get an additional conclusion that device specifications affect the delay in the authentication process.

Keyword: ***Fog computing, Authentication, Protocol, J-PAKE, xor and hash, Scanning***

---

1. Pendahuluan

Kemajuan ilmu pengetahuan dan teknologi saat ini berkontribusi besar bagi kehidupan manusia terutama di bidang elektronika dan telekomunikasi, mengakibatkan menusia dapat terhubung ke internet setiap saat. Teknologi *fog computing* yang dapat membantu dalam melakukan pengolahan data sebelum dikirim ke *cloud*. Efeknya dapat mempercepat waktu yang dibutuhkan untuk komputasi secara *real time*. Perangkat user akan melakukan autentikasi terhadap *fog computing server*. Lalu server akan mengecek dan memberikan layanan jika pemindaian dan autentikasi berhasil[1]. Namun karena perangkat yang terhubung ke wifi itu banyak, maka untuk bisa terhubung kepada fog computing perangkat harus terautentikasi. Pada beberapa penelitian sebelumnya, semua *client* yang terhubung di satu jaringan WiFi harus terautentikasi pada fog server walaupun hanya beberapa yang akan dihubungkan ke fog computing server[2]. Oleh karena itu, Dalam penelitian ini penulis membuat sistem untuk meningkatkan kemanan konektivitas user yang berada di jaringan WiFi dengan mengautentikasi user yang ingin terhubung ke fog computing *server* saja. Hasil yang diharapkan penulis pada penelitian ini meminimalisir sumber daya yang dibutuhkan untuk proses autentikasi.

2. Dasar Teori /Material dan Metodologi/perancangan

2.1 Fog Computing

Fog Computing yang juga dapat diartikan sebagai Edge Computing Dalam beberapa tahun belakangan ini penggunaan *Fog Computing* mengalami peningkatan dalam pembuatan aplikasi dalam range kecil sampai menengah, Dibandingkan dengan cloud, fog memiliki *latency* yang lebih rendah, dukungan mobilitas yang tinggi, dan interaksi secara *real-time*[3]. Fog memiliki tiga layer utama yaitu cloud, fog, dan perangkat dengan cara kerja yaitu data yang kecil akan diproses pada fog lalu diteruskan menuju cloud, sedangkan *big data* akan tetap diproses di cloud, dengan

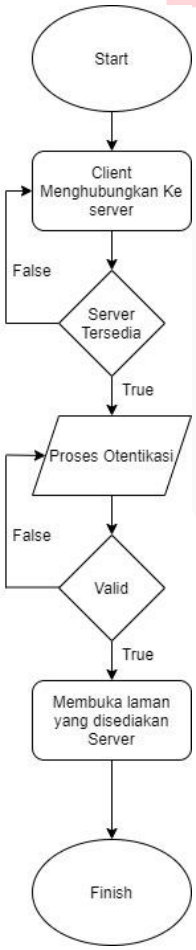
proses tersebut akan meringankan peran cloud dalam mengolah data[4].

2.2 Autentikasi

Autentikasi adalah suatu proses untuk memeriksa atau memverifikasi perangkat komputasi pengguna seperti ponsel atau layanan daring seperti email. Mekanisme autentikasi yang tepat sangat berpengaruh bagi pengguna sehingga dapat mencegah akses illegal ke perangkat komputasi[5].

3. Pembahasan

3.1 Desain Sistem



Gambar 1 Diagram Alir *Proses scanning and authenticating*

Penjelasan proses sistem *Proses scanning and authenticating* yang dibuat dalam bentuk diagram alir adalah pada gambar 1 adalah sebagai berikut.

1. *Client* menghubungkan ke *server*

Client akan menginput IP dan Port yang sudah dipindai sebelumnya. Jika IP dan Port yang dimasukan benar maka proses autentikasi akan dimulai.

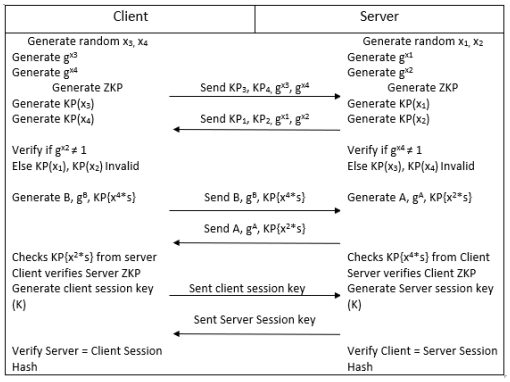
2. Proses autentikasi

Pada tahap berikutnya, setelah *client* terhubung ke IP dan Port yang benar maka autentikasi akan dilakukan. Pada pengujian penulis menggunakan dua protokol keamanan yang berbeda, yaitu protokol J-PAKE dan protokol *xor and hash*.

3. Membuka halaman yang disediakan *server*

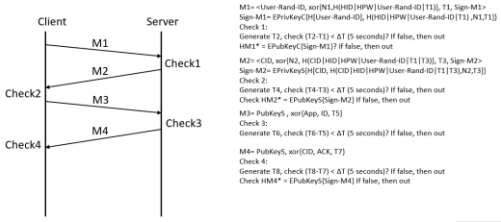
Jika autentikasi berhasil dilakukan, maka user akan dapat membuka halaman web yang disediakan oleh *server*. Halaman web yang disediakan pada sistem adalah Halaman Login sederhana yang usernya sudah ditentukan oleh web admin.

3.2 Protokol Keamanan



Gambar 2 Diagram J-PAKE

Gambar 2 adalah model diagram protokol pertama, yaitu protokol J-PAKE. J-PAKE merupakan pengembangan dari protokol Diffie-Hellman. Perbedaan J-PAKE dengan Diffie-Hellman adalah J-PAKE tidak membutuhkan kunci publik sebagaimana Diffie-Hellman. Walaupun begitu, kedua algoritma tersebut sama-sama bisa digunakan untuk bertukar kunci dan membentuk session key.[6].



Gambar 3 Diagram *xor and hash*

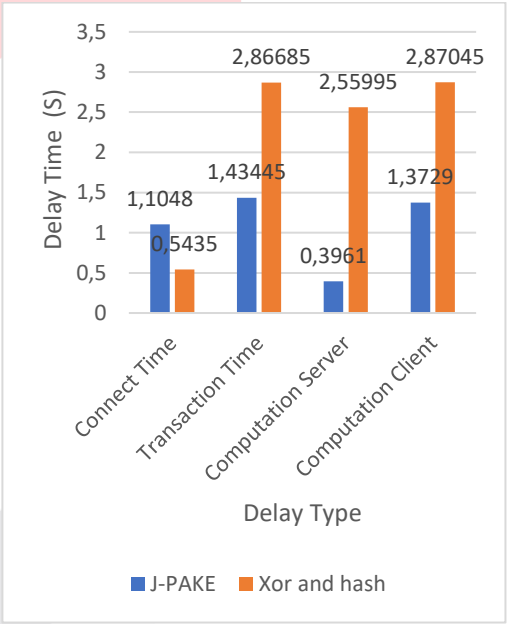
Gambar 3 adalah model diagram Protokol *xor and hash*. Cara kerja protokol ini dengan menggabungkan beberapa nilai yang sudah di-*hash* untuk mendapatkan nilai baru, Selanjutnya nilai tersebut akan di-xor-kan lalu akan dikirim. Protokol ini memiliki beberapa tahap *check*, yang pertama *check* waktu, jika pengiriman lebih dari 5 detik maka transaksi dibatalkan, yang kedua adalah *check* ID pada *server*, jika ID tidak terdaftar pada *server*, maka transaksi dibatalkan[6][7].

3.3 Perancangan Aplikasi Android

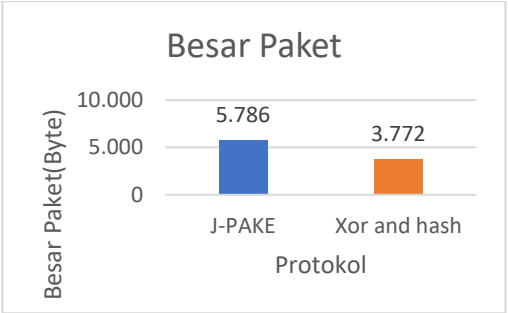
Penulis menggunakan Bahasa pemograman Dart dalam pembuatan aplikasi menggunakan Flutter. Aplikasi berisi Autentikasi J-PAKE dan membuka halaman web jika autentikasi berhasil

4. Hasil dan analisis

4.1 Pengujian Delay pada nilai password benar

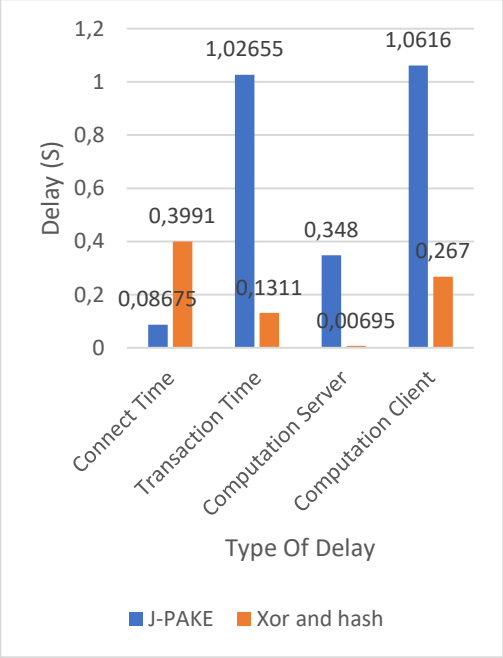


Gambar 4 Delay pada proses autentikasi password bernilai benar

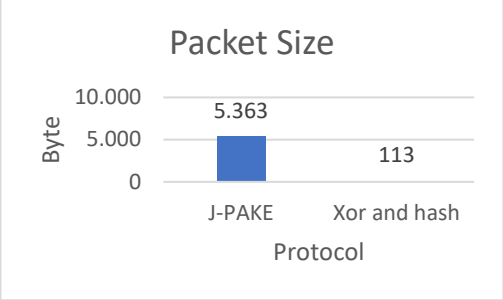


Gambar 5 Besar Paket proses autentikasi password bernilai benar

Gambar 4 merupakan perbandingan hasil dua protokol dari pengambilan dua puluh sampel rata – rata antara autentikasi protokol J-PAKE dan protokol *xor and hash* pada kondisi input password bernilai benar dan kondisi perangkat normal. Gambar 5 Merupakan perbandingan rata – rata besar paket dalam satu kali transaksi. Hasil menunjukkan Protokol *xor and hash* memiliki delay rata – rata lebih besar tinggi dibanding J-PAKE tetapi besar paket yang dikirimkan lebih rendah.

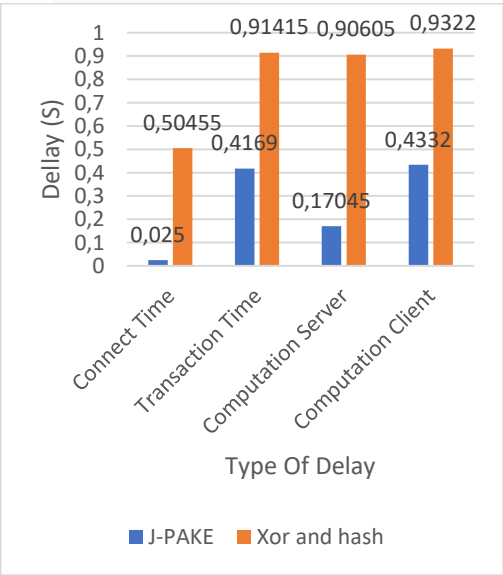


Gambar 6 Grafik rata - rata delay pada password salah

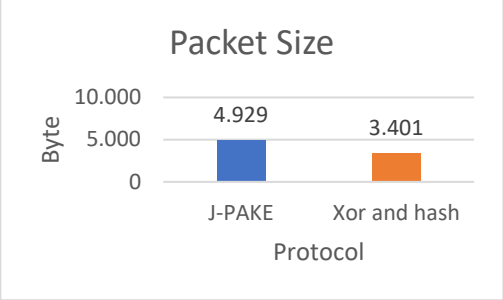


Gambar 7 Grafik Besar paket pada password salah

Gambar 6 adalah merupakan hasil rata – rata delay dan Gambar 7 merupakan rata – rata besar paket dalam satu kali transaksi dari 20 kali percobaan pada kedua protokol jika password yang dimasukkan salah. Hasil menunjukkan delay J-PAKE sekarang lebih tinggi dan sangat signifikan. Ini dikarenakan J-PAKE melakukan pengecekan pada tahap akhir sehingga tetap melakukan perhitungan walaupun input nya salah.



Gambar 8 Grafik rata - rata delay pada kinerja perangkat *client* maksimum



Gambar 9 Grafik rata - rata besar paket pada kinerja perangkat *client* maksimum

Gambar 8 merupakan perbandingan rata – rata delay yang terjadi sedangkan Gambar 9 merupakan rata – rata besar paket dalam satu kali transaksi dari 20 kali percobaan pada kedua protokol jika password yang dimasukkan benar dan kinerja perangkat *client* berjalan pada kondisi maksimum. Maksimum di sini berarti kondisi perangkat *client* berjalan pada mode *Best Performance* dan dialiri arus listrik. Hasilnya *xor and hash* memiliki delay lebih tinggi dan paket yang lebih kecil, Tetapi rata – rata waktu delay berkurang secara signifikan yang pada awalnya memiliki delay rata – rata 2 detik menjadi di bawah 1 detik.

5. Kesimpulan

Pada tugas akhir ini, penulis telah merancang sistem pemindaian dan autentikasi untuk menghubungkan *client* kepada *fog computing server*. Sistem ini dirancang untuk mengamankan *client* yang ingin terhubung kepada *fog computing server*. Proses pemindaian dibagi menjadi dua tahap yaitu pemindaian IP dan pemindaian Port. Sedangkan proses autentikasi menggunakan dua protokol keamanan yang berbeda, yaitu protokol J-PAKE dan protokol *xor and hash*. Masing – masing protokol memiliki kelebihan dan kekurangan masing – masing.

Hasil eksperimen pengukuran delay menunjukkan protokol *xor and hash* menghasilkan delay lebih besar, ini disebabkan karena *server* dan *client* melakukan komputasi lebih banyak dibanding protokol J-PAKE. Di sisi lain, protokol J-PAKE menghasilkan jumlah paket yang lebih besar dibandingkan *xor and hash*, ini dikarenakan protokol J-PAKE berbasis *Diffie-Hellman* di mana *client* dan *server* saling menukar hasil variabel. Jika penulis mendapat pertanyaan, “Protokol mana yang lebih dapat diandalkan?” Penulis akan menjawab untuk saat ini protokol J-PAKE lebih baik dari segi delay dan besarnya paket. Tidak menutup kemungkinan di waktu mendatang protokol *xor and hash* akan lebih baik karena model *xor and hash* masih dalam tahap pengembangan dan komputasi *xor and hash* lebih rumit sehingga akan lebih sulit untuk dipecahkan. Beberapa saran dari penulis untuk dijadikan pertimbangan pada penelitian selanjutnya yaitu menjadikan sistem menjadi satu aplikasi yang utuh dan mengubah nilai variabel yang statis menjadi dinamis.

REFERENSI

[1] S. B. Nath, H. Gupta, S. Chakraborty, and S. K. Ghosh, "A Survey of Fog Computing and Communication: Current Researches and Future Directions," no. i, pp. 1–47, 2018.

[2] M. S. Pardeshi and S.-M. Yuan, "SMAP Fog/Edge: A Secure Mutual Authentication Protocol for Fog/Edge," *IEEE Access*, vol. 7, pp. 101327–101335, 2019, doi: 10.1109/access.2019.2930814.

[3] K. H. Abdulkareem *et al.*, "A review of fog computing and machine learning: Concepts, applications, challenges, and open issues," *IEEE Access*, vol. 7, pp. 153123–153140, 2019, doi: 10.1109/ACCESS.2019.2947542.

[4] Z. Mahmood and M. Ramachandran, *Fog computing: Concepts, principles and related paradigms*. 2018.

[5] S. W. Shah and S. S. Kanhere, "Recent Trends in User Authentication - A Survey," *IEEE Access*, vol. 7, pp. 112505–112519, 2019, doi: 10.1109/ACCESS.2019.2932400.

[6] F. Dewanta, "Secure Microservices Deployment for Fog Computing Services in a Remote Office," *2020 3rd Int. Conf. Inf. Commun. Technol. ICOIACT 2020*, pp. 425–430, 2020, doi: 10.1109/ICOIACT50329.2020.9332025.

[7] F. Dewanta and M. Mambo, "A mutual authentication scheme for secure fog computing service handover in vehicular network environment," *IEEE Access*, vol. 7, pp. 103095–103114, 2019, doi: 10.1109/ACCESS.2019.2931217.