OPEN ACCESS
Indo-JC SUBMISSION
ISSN XXXX-XXXX
SOCJ.TELKOMUNIVERSITY.AC.ID/INDOJC
IND. JOURNAL ON COMPUTING VOL. XX, NO. XX, SEPTEMBER 2019
PP. XX-XX. DOI:XXX

Context Awareness for Authentication Process in Login System

Fikri Attamami Laguliga #1, Parman Sukarno *2, Rahmat Yasirandi #3

Fakultas Informatika, , Universitas Telkom
Jl. Telekomunikasi No. 1 Bandung (022) 7564108 Bandung, Indonesia

[1] eriklaguliga@student.telkomuniversity.ac.id

[2] psukarno@telkomuniversity.ac.id

[3] batanganhitam@telkomuniversity.ac.id

Abstract

Authentication system security has been evaluated by many researchers. The conventional process of authentication systems only requires a username and password to authenticate. But this method is very convenient to say it is safe from all forms of attack until it can carry out authentication without permission by only using a password and username. In this study will use the context awareness method as the foundation of the authentication system, where the system will take the user context parameters as reference material for the authentication process. Not up to that point, this system is also equipped with an authentication level where this level will be a class of authentication systems. Giving level will be based on the weight of the context that has been identified. The higher the level, the fewer contexts identified and the user must pass an additional authentication process. This research is proven in overcoming the authentication process against users without permission.

Keywords: Context Awareness, authentication system

Abstrak

Keamanan sistem otentikasi sudah banyak dievaluasi oleh banyak peneliti. Proses konvensional sistem otentikasi hanya memerlukan username dan password untuk melakukan otentikasi. Tapi cara tersebut sangat konvensional untuk dikatakan aman dari segala bentuk penyerangan sampai dapat melakukan proses otentikasi tanpa izin dengan hanya menggunakan password dan username. Didalam penelitian ini akan menggunakan metode context awareness sebagai pondasi sistem otentikasi, dimana sistem akan mengambil parameter konteks pengguna sebagai bahan acuan untuk proses authentikasi. Tidak sampai disitu, di sistem ini juga dibekali dengan proses authentication level dimana level ini akan menjadi kelas terhadap sistem otentikasi. Pemberian level akan berdasarkan bobot konteks yang sudah teridentifikasi. Semakin tinggi tingkatannya maka semakin sedikit konteks yang teridentifikasi dan pengguna harus melewati proses otentikasi tambahan. Penelitian ini terbukti dalam mengatasi proses otentikasi terhadap pengguna tanpa izin.

Kata Kunci: Context Awareness, authentication system

I. INTRODUCTION

Beberapa tahun terakhir penggunaan perangkat mobile sangat banyak di lingkungan sekitar kita. Penggunaan ponsel cerdas dikarenakan karena memiliki keunggulan salah satunya adalah kenyaman dalam mengakses data. Tapi sebagian besar proses mengakses data pribadi memerlukan proses otentikasi. Proses otentikasi konvensional hanya perlu menentukan username dan kata sandi untuk melakukan proses otentikasi [1].

Disisi lain perangkat dengan mobilitas tinggi dapat dengan mudah hilang, dicuri, atau digunakan oleh orang yang tidak berwenang [2]. Dengan memperhatikan parameter-parameter setiap individu pada saat melakukan proses otentikasi itu akan membantu mengamankan otentikasi untuk menjamin bahwa yang melakukan proses login itu adalah pemiliknya. Jika otentikasi melihat lebih dari satu parameter itu juga dikenal sebagai context awarenes.

Context awareness itu sendiri merupakan informasi yang dapat digunakan dalam mengakarakterisasi situasi suatu entitas dan entitas adalah pengguna,tempat,atau objek yang dianggap relevan dengan interaksi pengguna dan aplikasi itu sendiri [3]. Penelitian terhadap context awareness tersebut bukan hal yang baru pada sistem otentikasi. Pada penelitian [2] telah context awareness pada sistem otentikasi di mobile cloud computing yang dimana terbukti mengurangi kemungkinan orang yang tidak berwenang dapat melakukan proses otentikasi, namun dari penelitian [2] memerlukan historical data otentikasi pengguna untuk keperluan sistem untuk mempelajari konteks dari pengguna, sehingga sistem otentikasi pada penelitian ini kurang bisa diandalkan ketika pengguna baru pertama kali menggunakan sistem otentikasi dan pengguna tidak bisa menentukan fakotr otentikasi berdasarkan padangan pengguna sendiri.

Pada penelitian ini menerapkan context awareness pada sistem login yang tidak bergantung dengan historical data otentikasi pengguna dan mekanisme pada penelitian ini juga diharapkan dapat memudahkan pengguna untuk memberikan beberapa faktor otentikasi berdasarkan pandangan pengguna. Sistem yang diajukan juga diharapkan dapat memberikan rasa aman pengguna ketika melakukan proses otentikasi.

II. LITERATURE REVIEW

Keamanan sistem otentikasi sangat penting karena merupakan salah satu faktor pertimbangan bagi pengguna. berikut adalah perbandingan metode pada sistem otenikasi yang menggunakan context awareness.

Tabel I: Perbandingan penelitian

Project name	citations	project focus	Modeling	Reasoning	Distribution	History and storage	Level of context awarenes
A Context-Aware Authentication Framework for Smart Homes	[4]	Middleware	K-Value	Rules	Subscription	No	Low
The context awareness architecture in mobile cloud computing	[2]	System	Graphical Modeling	Probablistic	Query	Yes	High
Context-AwareActive Authentication Using Smartphone Accelerometer Measurements	[6]	System	Graphical Modeling	Supervised Learning	Query	Yes	High

Pada Penelitian [2] menjelaskan penggunaan *context-awareness* dengan menerapkan arsitektur baru yaitu CAA(*The context Awareness Architectur in Mobile Cloud Computing*). Pada penelitian ini menggunakan beberapa parameter konteks yaitu: catatan telepon, kalender, *Global Postion Unit*, dan baterai .Penelitian ini menggunakan *Graphical modeling* yang memungkinkan sistem dapat menampung banyak data yang nantinya data tersebut digunakan pada proses *context reasoning*. dipenelitian ini juga menggunakan *reasoning* supervised learning yang dimana dipenelitian ini dinamakan *Decision-making device*, proses ini melakukan kalkulasi perilaku yang sudah tersimpan dan prilaku yang sedang dilakukan pengguna menggunakan dan kemudian membandingkan data pengguna yang sudah disimpan di *database*, namun penggunaan *supervised learning* pada *context reasoning* memerlukan data pengguna yang sudah disimpan sebelumnya agar sistem mengenali aktifitas pengguna dan prilaku pengguna. Penggunaan *context distribution* pada penelitian ini menggunakan metode *query* yang dimana *query* tersebut mengahasilkan hasil otentikasi yang ditujukan kepada pengguna.

Pada penilitian [6] menjelaskan penggunaan context awareness yang memanfaatkan sensor *accelerometer* untuk sistem otentikasi. Penggunaan *context modeling* pada penelitian ini sama dengan penelitian [2] yaitu *graphical modeling*, proses model yang dilakukan penelitian ini dengan mengumpulkan dataset sebanyak 30 data. Pengumpulan data ini dengan cara setiap sukarelawan memegan ponsel cerdas selama 2 setiap tangan kanan dan tangan kiri. Penggunaan *context reasoning* ini menggunakan metode *supervised learnin* yang memerlukan dataset agar sistem mengenali aktifitas pengguna berdasarkan gerakan sensor *accelerometer*. Hasil dari penelitian ini memiliki akurasi pada saat ponsel cerdas dikantung sebesar 61.76% pada saat ponsel cerdas digenggam dan 72.58% sedangkan untuk akurasi ketika data latih ponsel cerdas digenggam sebesar 82.30% ditangan dan 62.55% dikantong.

Pada penelitian [4] menjelaskan penggunaan context awareness pada sistem otentikasi di *IOT smart*

home. Penggunaan *context modeling* pada penelitian ini adalah *logic based modeling* yang dimana model ini dapat memberikan *rules* yang digunakan untuk mengekspresikan kebijakan dan prefensi pengguna terhadap sistem. Penelitian ini juga menggunakan metode *rules* yang memungkin pengguna dapat menentukan beberapa kondisi level otentikasi berdasarkan pandangan pengguna. Dan untuk context *Context Distribution* menggunakan metode *Subscription* yang memungkinkan *context consumer* dapat berlangganan dengan sistem dengan mendeklarasikan persyaratan apa saja yang diperlukan untuk menentukan level otenikasi.

Dari beberapa penelitian diatas menjelaskan belum adanya penggunaan metode *context awareness* dalam proses otentikasi pada sistem login. Maka sistem yang diusulkan akan menggunakan *context awareness* di sistem login yang menggunakan *logic based modeling* diproses *context modeling* dan *Rules* diproses *context reasoning* yang memungkinkan pengguna dapat menentukan faktor otentikasi berdasarkan prefensi pengguna, penggunaan metode sistem dapat memodelkan pikiran pengguna dengan mudah[3]. Pemilihan metode tersebut juga memungkinkan sistem otentikasi tidak memerlukan *data training* pengguna untuk menentukan apakah pengguna terotentikasi atau tidak terotentikasi.

III. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah Context awareness. Penggunaan metode ini akan difokuskan untuk mengatasi masalah dan pengembangan sistem dipenelitian ini.

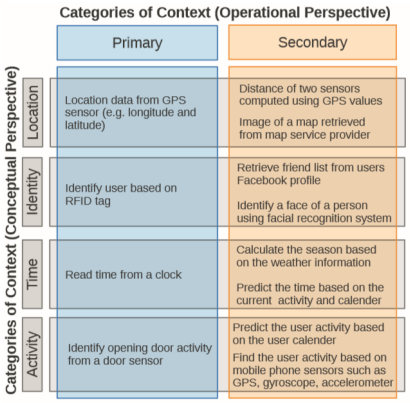
A. *Context Awareness*

Context merupakan sebuah informasi yang dapat dikarekterisasi dalam situasi sebagai entitas. Dari entitas tersebut bisa sebagai pengguna, tempat, atau objek yang dianggap relevan terhadap interaksi antar pengguna dan aplikasi tersebut [5].

Sebuah sistem yang memiliki context-aware ketika menggunakan beberapa konteks yang menyediakan informasi dan relevan terhadap jasa ke pengguna, dimana nilai dari relevansi tersebut tergantung dari pengguna itu sendiri [5].

Didalam context-aware sendiri terdapat skema kategorisasi:

- Primary context: Informasi yang diterima tanpa menggunakan konteks yang ada dan tanpa melakukan operasi fusi data sensor apapun [3].
- Secondary context: Informasi yang dapat dikomputasi menggunakan primary context. Secondary context dapat dikomputasi dari sensor tersebut atau pengambilan data operasi seperti (data telepon, alamat, email, dan lain-lain) [3].

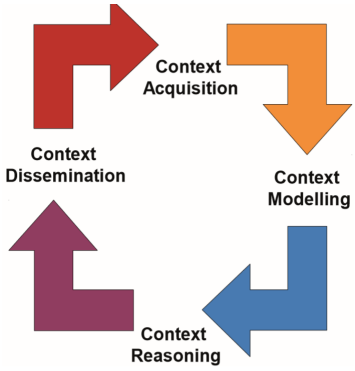


Gambar 1: kategori konteks [3].

Pada context-aware memiliki life cycle berdasarkan pada gambar gambar 2. yang terdiri 4 fase, yaitu:

- Context Acquisition, melakukan pengumpulan data konteks yang didapatkan dari beberapa sumber.
- Context Modelling, memberikan model atau metode untuk menghasilkan hasil yang berarti.
- Context Reasoning, data yang sudah diproses untuk menjadi high-level context information.

- Context Disseminationcontext, high-level context didistibusikan ke pengguna yang memerlukan hasil dari konteks tersebut.



Gambar 2: context aware life cycle [3].

IV. PERANCANGAN SISTEM

Pada di Bab IV ini akan menjelaskan model context awareness yang diterapkan untuk proses otentikasi pada sistem login.Penggunaan model pada sistem otentikasi ini berdasarkan context lifecyle yang sudah dijelaskan pada bab sebelumnya, pada maka pada bab ini akan menjelaskan setiap alur model secara rinci.

A. Context Life Cycle for Authentication

Pada sesi ini akan menjelaskan beberapa tahapan proses berdasarkan context aware lifecyle yang sudah diteliti pada penelitian [3]. Dipenelitian ini akan melakukan modifikasi model context life cyle untuk sistem otentikasi yang mudah dipahami pengguna untuk menentukan beberapa faktor otentikasi berdasarkan pandangan mereka sendiri.

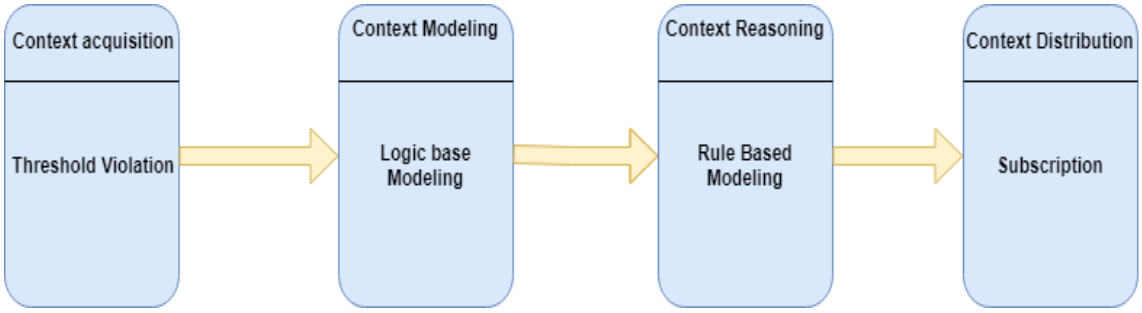
1) Context Acquisition: Pada tahap ini sistem akan menggunakan parameter context yaitu Password/username, lokasi, hari, dan lokasi [3]. Dan pada sesi ini konteks dapat dihasilkan dari threshold violation [3]. Threshold violation dimana sistem perlu menditeksi peristiwa untuk mengambil konteks [3]. Penggunaan bobot threshold ini akan memungkinkan pengguna dapat menentukan bobot konteks mereka sesuai dengan keinginan pengguna.

2) Context Modelling: Pada tahap ini data yang dikumpulkan perlu dimodelkan dan disajikan sesuai dengan cara yang bermakna. Metode yang digunakan untuk model ini adalah Logic based modeling[3], pemodelan tersebut memungkinkan informasi konteks tingkat tinggi baru diekstraksi menggunakan konteks tingkat rendah. Penggunaan metode tersebut memungkinkan pengguna dapat menentukan peraturan dan logika ketika sistem sudah berjalan.

3) Context Reasoning: Pada tahap ini context yang sudah dimodelkan sudah dihasilkan dari context modeling akan menggunakan metode Rules[3], metode ini memungkinkan pembuatan informasi konteks level tinggi menggunakan konteks level rendah. Penggunaan metode rules ini memungkinkan sistem dengan mudah memodelkan pikiran penggunua.

4) Context Distribution: Pada tahap ini context yang sudah diolah dari context reasoning sistem akan mengirim hasil dari konteks tersebut. Metode yang digunakan yaitu Subscreption[3] yang memungkinkan konteks pengguna dapat berlangganan dengan konteks management system denganmendeskripsikan kebutuhan pengguna. Sistem akan memberikan hasil secara periodik saat terjadi sesuatuatau sesuai dengan bobot pelanggaran.

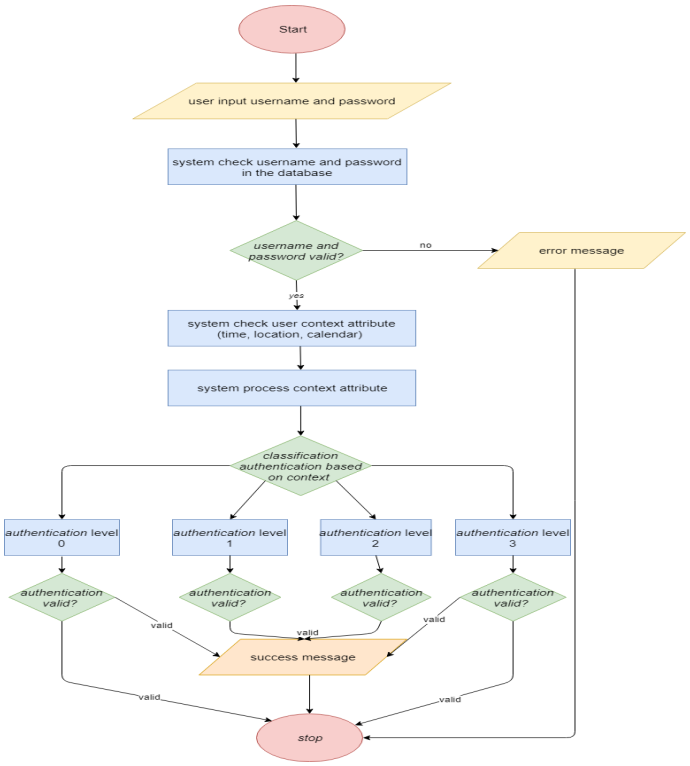
Berdasarkan beberapa setiap alur mode yang sudah dijelaskan diatas maka flow chart alur model context bisa dilihat di gambar 3.



Gambar 3: Context diagram

B. Perancangan Sistem

Pada Gambar 4 memperlihatkan bahwa sistem otentikasi yang dibangun memerlukan konteks pengguna untuk melakukan otentikasi. Pertama pengguna tetap diharuskan untuk memasukkan username/password yang sudah didaftarkan kedalam sistem sebeagai tahap awal proses otentikasi. Selanjutya ketika username/password pengguna benar, sistem akan mengambil konteks pengguna sebagai syarat otentikasi. Selanjutnya ketika sistem sudah melakukan pengumpulan konteks pengguna, sistem akan melakukan klasifikasi jenis level otentikasi yang diberikan kepada pengguna berdasarkan konteks yang dikumpulkan oleh sistem. Level otentikasi ini akan memiliki jenis otentikasi mulai dari level 0 yaitu pengguna langsung bisa masuk ke sistem tanpa otentikasi tambahan, untuk level 1 sistem akan memberikan pertanyaan keamanan tentang struktur organisasi, untuk level 2 sistem akan mengirimkan One Time Password yang akan dikirimkan ke pengguna melalui SMS, dan untuk level 3 sistem akan memberikan pertanyaan keamanan tentang informasi waktu kapan pengguna melakukan otentikasi. Jenis-jenis otentikasi itu merupakan representasi *Multi factor authentication* yaitu memiliki faktor *something you know*, *something you have*, dan *something you are* [7].



Gambar 4: Context diagram

C. Alur kerja sistem otentikasi yang diajukan

Pada sesi ini dilakukan beberapa skenario proses otentikasi. Pada sesini menjelaskan beberapa skenario percobaan terhadap proses otentikasi yang sudah berjalan. Proses yang sudah terjadi pada saat pengguna menggunakan sistem otentikasi akan dijelaskan secara bertahap pada sesi ini. Berikut penjelasan lengkap skenario proses otentikasi yang dilakukan oleh pengguna.

1) Pra-kondisi
   Pada sesi ini sistem otentikasi dengan context aware diimplementasikan di komputer personal. Sebelumnya pengguna sudah melakukan pendaftaran dan tersimpan di *database*. Pendaftaran itu meliputi username/password dan konteks pengguna Data-data pengguna bisa dilihat di tabel II.

Tabel II: Atribut konteks pengguna

Username	admin@gmail.com
Password	admin
latitude	admin
longtitude	-69,222
waktu_awal	09.00.00
waktu_akhir	17.00.00)
Hari	senin, selasa, rabu, kamis,jumaat

   Pengguna juga sudah menentukan bobot konteks untuk setiap parameter keberhasilan. Ini nantinya berfungsi ketika context modeling, pengguna diharuskan memasukkan bobot *username* dan *password* lebih besar dari parameter yang lainnya dikarenakan *username* dan *password* merupakan persyaratan otentikasi pertama untuk masuk kedalam sistem. Untuk lebih rinci bisa dilihat pada Table III.

Tabel III: bobot konteks

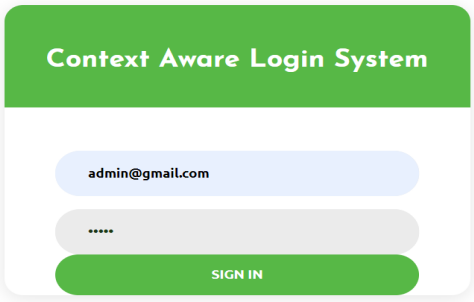
Konteks Parameter	Bobot konteks
Password/username	40
Waktu	10
Hari	20
Lokasi	30

   Pengguna juga sudah menentukan Syarat level otentikasi. Syarat otentikasi ini nantinya akan berfungsi pada pemberian syarat otentikasi berdasarkan perhitungan berat context, pemberian bobot syarat level otentikasi harus lebih kecil dari pada level sebelumnya dikarenakan semakin bertambah level otentikasinya semakin tinggi tingkat otentikasinya semakin kecil tingkat kepercayaan sistem kepengguna .Untuk lebih rinci bisa dilihat pada Table IV.

Tabel IV: Syarat penentuan kelas otentikasi pengguna

Security Level	Syarat Bobot
Level 0	X = 100
Level 1	$80 \leq X < 100$
Level 2	$41 \leq X < 80$
Level 3	$0 \leq X < 41$

2) *Context Acquisition*
   Context Acquisition merupakan tahap pertama pada saat pengguna melakukan otentikasi. Diproses ini sistem mengambil parameter yang valid pengguna ketika pengguna melakukan proses otentikasi. Pengguna melakukan proses otentikasi secara umum yaitu dengan menggunakan *username* dan *password*, *user interface* form login bisa dilihat pada gambar 5.



Gambar 5: User Interface Login form

Ditahap ini sistem melakukan proses validasi terhadap database dengan membandingkan context pengguna yang sudah didaftarkan dan context pengguna yang dibawa pada saat melakukan otentikasi, algoritma *Context acquisition* bisa dilihat pada Algorithm 1. Pada algorithm 1 menjelaskan proses *Context Acquisition* pada login sistem. Ditahap awal sistem mengambil *username* dan *password*, ketika *username* dan *password* berhasil divalidasi maka sistem mengambil parameter konteks yang sudah tersimpan di database yang disimpan ke *variabel* baru. Selanjutnya sistem mengambil data konteks sekarang (hari, waktu, dan lokasi) dan membandingkan dengan data konteks yang sudah diambil di *database* untuk proses validasi konteks dan diteruskan ke proses *context modeling* untuk proses perhitungan konteks.

Algorithm 1: Algortima Context Acquisition di sistem login

```
cek login <- database(username,password);
if jumlah data yang ditemukan pada variabel ceklogin > 0 then
    for hasil cek login do
        email <- database(email);
        password <- database(password);
        latitude <- database(latitude);
        longtitude <- database(longtitude);
        waktu awal <- database (waktu awal);
        waktu akhir <- database (waktu akhit);
        hari <- database (hari);
    end
    hari sekarang <- get day;
    waktu <- get time ;
    ip <- mendapatkan informasi ip ('api ip');
    lokasi <- mendapatkan kontent lokasi berdasarkan ip ('api lokasi',ip);
    lokasi <- menerjemah kontent (lokasi);
    lat <- lokasi(lat);
    lon <- lokasi(lat);
    if hari == hari sekarang then
        proses context modeling;
        if waktu sekarang > waktu and waktu < waktu sekarang then
            proses context modeling;
        end
    end
    if latitude == lat and lontitude == lon then
        proses context modeling;
    end
end
```

3) *Context Modeling*
Diproses ini parameter yang sudah tervalidasi oleh *context acquisition* dilakukan pemberian bobot pada parameter yang sudah tervalidasi. Sistem mengambil data bobot konteks didalam database

yang datanya sudah terdaftar, selanjutnya proses ini melakukan perhitungan berdasarka nbobot yang sudah diambil. Proses *context modeling* bisa dilihat di Algortihm 1. Ditahap awal proses context modeling, sistem mengambil *score* pada setiap parameter yang sudah tersimpan didatabase. selnjutnya ketika sistem sudah melakukan validasi parameter konteks, maka sistem akan melakukan pemberian bobot terhadap parameter konteks yang sudah tervalidasi. Nantinya hasil bobot dari proses *context modeling* akan diproses lagi *context reasoning*.

Algorithm 2: Algortima Context Modeling di sistem login

```
cek login <- database(username,password);
nilai <- 0;
if jumlah data yang ditemukan pada variabel ceklogin > 0 then
    for hasil cek login do
        score calendar <- database(score caldendar);
        score identity <- database(score identity);
        score lokasi <- database(score lokasi) ;
        score time <- database(score time)
    end
    nilai <- score indentity;
    if hari == hari sekarang then
        nilai <- nilai + score calendar;
        if waktu sekarang > waktu and waktu < waktu sekarang then
            nilai <- nilai + score time;
        else
            nilai <- nilai + 0;
        end
    else
        nilai <- nilai + 0;
    end
    if latitude == lat and lontitude == lon then
        nilai <- nilai + score lokasi;
    else
        nilai <- nilai + 0;
    end
else
    nilai <- nilai + 0;
end
```

4) *Context Reasoning*
Selanjutnya proses *context reasoning* melakukan proses klasifikasi berdasarkan total bobot yang sudah diproses di *context modeling*. Proses ini menentukan level otentikasi apa saja yang dihasilkanberdasarkan total bobot konteks, penentuan syarat klasifikasi ini bisa dilihat pada pra-kondisi sistem(Tabel IV). Algoritma pada proses ini bisa dilihat pada Algorithm 3.

Algorithm 3: Algortima Context Reasoning di sistem login

```
if nilai == level 1 then
    authentication level 0;
end
if (nilai < level 1) and (nilai level 2) then
    authentication level 1;
end
if (nilai < level 2) and (nilai >= level 3 ) then
    authentication level 2;
end
if (nilai < level 3) and (nilai>= level 4) then
    authentication level 3;
end
```

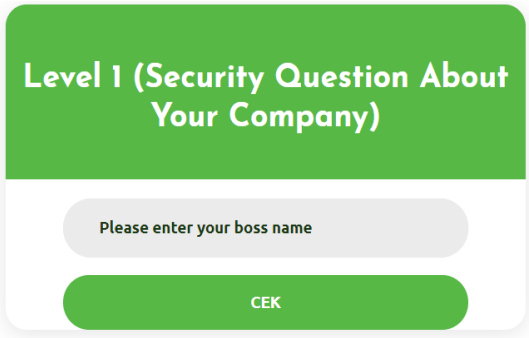
5) *Context Distributio*n

Selanjutnya proses *context distribution*, proses ini merupakan lanjutan proses dari context reasoning. Diproses ini hasil dari klasifikasi dari context reasoning diteruskan dengan cara yang lebihbermakna ke pengguna. Setiap level otentikasi memiliki fitur yang mengharuskan pengguna untuk menggunakan fitur tersebut untuk masuk kedalam sistem, fitur-fitur tersebut adalah representasi dari *Multi-factor authentication* yang sudah dijelaskan pada bagian perancangan sistem. Berikut pada proses context reasoning bisa dilihat pada Algortihm 4.

Algorithm 4: Algortima Context Reasoning di sistem login

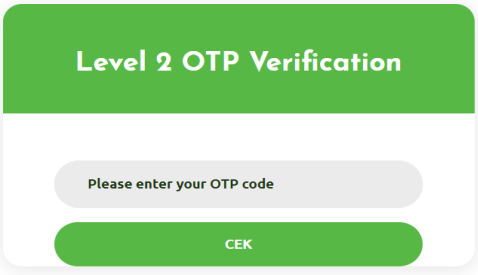
```
if nilai == level 1 then
    authentication level 0;
end
if (nilai < level 1) and (nilai >= level 2) then
    Security question about when user last login attempt;
end
if (nilai < level 2) and (nilai >= level 3 ) then
    One Time Password;
end
if (nilai < level 3) and (nilai>= level 4) then
    Security question about when user last login attempt;
end
```

Ketika pengguna mendapatkan otentikasi level 1, pengguna diharuskan mengisi *security question* terhadap pengetahuan oraginsasi pengguna. Otentikasi level ini merupakan representasi dengan *something you know* di *Multi Factor Authentication*. Bentuk form otentikasi bisa dilihat pada gambar 6.



Gambar 6: User Interface level 1 form

Ketika pengguna mendapatkan otentikasi level 2, pengguna akan diharuskan mengisi *One Time Password* atau bisa disebut OTP. Kode OTP ini dikirimkan melalui SMS ke ponsel pengguna, One Time Password ini merupakan bentuk representasi dari *something you have* di *Multi Factor Authentication*.Bentuk *user interce* level 2 otentikasi bisa dilihat pada gambar 7.



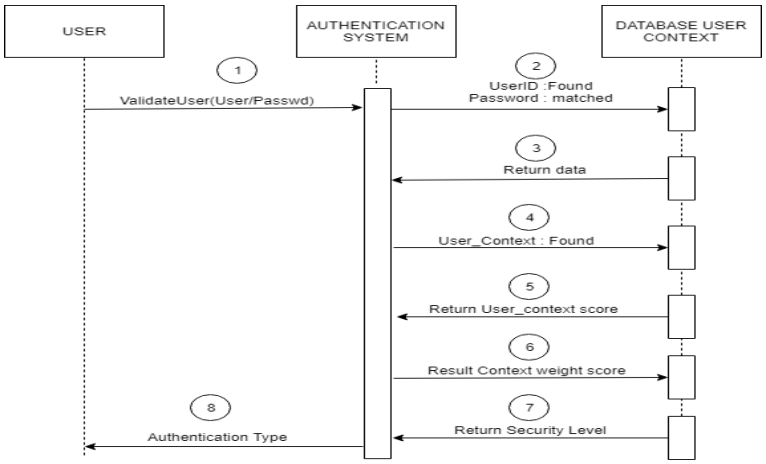
Gambar 7: User Interface level 2 form

Ketika pengguna pengguna mendapatkan otentikasi level yang paling rendah yaitu level 3, pengguna akan diharuskan mengisi *Security Question* tentang informasi waktu kapan pengguna melakukan *login* disistem. Setiap waktu informasi login pengguna akan dikirimkan melalui SMS yang dikirimkan ke pengguna agar pengguna dapat mengingat informasi waktu pengguna melakukan login. Level 3 ini merupakan representasi dari *something you are* di *multi factor authenticatio*. Bentuk *user interface* bisa dilihat pada gambar 8.

Gambar 8: User Interface level 3 form

D. Protokol Sistem Otentikasi Context Aware yang diajukan

Otentikasi yang diajukan yaitu sistem otentikasi yang dapat mengambil konteks untuk proses otentikasi. Pada bagian ini menjelaskan tentang perpindahan alur kerja fungsi dalam proses otentikasi.



Gambar 9: Context diagram

Pada gambar 5 memperlihatkan diagram sequence yang ada pada sistem. Pengguna akan tetap memasukkan username dan password. Context pengguna diolah setelah pengguna sudah memasukkan username dan password yang valid, untuk detailnya akan dijelaskan dibawah:

1) *User –> Authentication system*
   Pengguna memasukkan *username* dan *password* yang sudah terdaftar kedalam sistem. sistem akan meneruskan ke database untuk dilakukan proses *matching*
2) *Authentication system –> Database User Context*
   Sistem melakukan validasi *password* dan *username* terhadap *database* sistem.
3) *Database User context –> Authentication System*
   Sistem akan membuat session terhadap username dan password yang sudah terotentikasi.
4) *Authentication system –> Database User context*
   Sistem mengambil context pengguna, context yang diambil pada pengguna disaat proses login yaitu : Lokasi, Waktu, dan hari. Dan sistem melakukan validasi context terhadap Database Context yang sudah terdaftar.

5) *Database User Context –> Authentication system*
   Ketika context pengguna sudah tervalidasi maka sistem akan mengirimkan data bobot konteks yang sesuai dengan context pengguna disaat proses otentikasi.
6) *Authentication system –> Database User Context*
   Setelah sistem selesai melakukan perhitungan bobot context pengguna sistem mengirimkan bobot context ke database untuk proses validasi *security level*.
7) *Database User Context –> Authentication System*
   Database mengembalikan syarat level yang sesuai dengan bobot context yang sudah diproses.
8) *Authentication System –> User*
   Sistem memberikan jenis otentikasi ke pengguna berdasarkan *security level* yang ada di *database*.

E. Prosedur pengujian

Pengujian pada sistem yang diajukan dengan melakukan beberapa skenario ontentikasi dan melakukan pengukuran rasa keamanan pengguna dalam meenggunakan sistem yang diajukan. Pengujian ini dilakukan untuk membuktikan tujuan dari penelitian ini yaitu sistem otentikasi yang tidak bergantung hanya *username* dan *password* dan sistem otentikasi yang dapat mengelolah konteks pengguna untuk proses otenitkasi. Sebelum dilakukan pengujian, akan ditetapkan pra-kondisi yang harus dipenuhi yaitu:

1) sistem harus memiliki kemampuan melakukan pengelolahan konteks pengguna.
2) Pengguna sudah memiliki data konteks pengguna, data konteks pengguna yang sudah diusulkan bisa dilihat pada bagian sub sesi sebelumnya.

Berikut skenario yang dilakukan pada saat pengujian :

1) Memperoleh Login dan Kata Sandi Pengguna : pada skenario ini *username* dan *password* pengguna dicuri, dikompromikan, atau bahkan dipinjamkan. Pengguna yang tidak betanggung jawab akan melakukan proses otentikasi, pengguna juga tidak mengetahui informasi konteks pengguna yang asli. Sehingga, hasil yang diharapkan adalah sistem dapat mengenali pola otentikasi pengguna tidak bertanggung jawab dan memberikan otentikasi tambahan untuk masuk kedalam sistem. Untuk ringakasan skenario pengujian bisa dilihat pada Tabel 1.

Tabel V: Sekanrio pengujian 1

Jenis tes	Memperoleh Login dan Kata Sandi Pengguna
Kriteria	Sistem memerlukan username dan password dan sistem mengelolah konteks pengguna
Prosedur	username dan password pengguna dicuri. Pengguna yang tidak betanggung jawab akan melakukan proses otentikasi
Ekspektasi	sistem dapat mengenali pola otentikasi pengguna tidak bertanggung jawab dan memberikan otentikasi tambahan untuk masuk kedalam sistem

2) Pengguna melakukan otentikasi diluar perjanjian konteks : pada skenario ini pengguna asli melakukan ontikasi tapi pada skenario ini pengguna melakukan otentikasi tapi diluar konteks yang sudah didaftarkan kedalam sistem otentikasi. Hasil yang diharapkan pengguna akan mendapatkan otentikasi tambahan untuk masuk kedalam sistem berdasarkan hasil pengelolahan konteks ketika pengguna melakukan otentikasi. Untuk ringkasan skenario pengujian bisa dilihat pada Tabel 2.

Tabel VI: Skenario pengujian 2

Jenis tes	Percobaan login
Kriteria	Sistem memerlukan username dan password dan sistem mengelolah konteks pengguna
Prosedur	skenario ini pengguna asli melakukan ontikasi tapi pengguna melakukan otentikasi diluar perjanjian konteks
Ekspektasi	pengguna akan mendapatkan otentikasi tambahan untuk masuk kedalam sistem berdasarkan hasil pengelolahan konteks ketika pengguna melakukan otentikasi.

Selanjutnya prosedur pengujian menggunakan kueisoner. Pengguna yang akan mengisi kuesioner ini merupakan anggota disebuah divisi yang bukan terkait dengan IT yaitu divisi *General Affair* yang dimana bertanggung jawab mengelola administrasi dan kesekretariatan orgranisasi. Objektifitas dari kuesioner ini adalah :

1) *Uncover* sistem otentikasi user pada aplikasi enterprise perusahaan;
2) Melakukan evaluasi pada faktor otentikasi yang digunakan pengguna pada aplikasi enterprise perusahaan;
3) Pengguna memberikan peneliaian keamanan terhadap sistem otentikasi yang diajukan.

V. HASIL DAN PEMBAHASAN

A. Hasil Scenario Pengujian Sistem

Pada bagian ini akan menjelaskan hasil pengujian berdasarkan skenario yang sudah diusulkan, ringkasan skenario. Hasil pengujian pada skenario kedua adalah pengguna mendapatkan otentikasi. Hal ini pasti terjadi dikarenakan tidak semua konteks pengguna yang tervalidasi disistem. Berikut data konteks pengguna saat melakukan otentikasi yang bisa dilihat pada Tabel VII. Sehingga berdasarkan kalkulasi konteks yang valid dengan data konteks yang terdaftar didatabase pengguna mendapatkan otentikasi tambahan yaitu *security question* tentang informarsi kapan pengguna melakukan otenikasi, data konteks yang sudah terdaftar dan syarat level otentikasi bisa dilihat pada Tabel III dan Tabel IV. Sehingga hasil yang diharapkan pada skenario ini terbukti pengguna mendapatkan otentikasi tambahan.

Tabel VII: Parameter kontek yang valid

Konteks pengguna pada saat proses otentikasi	Konteks yang terdaftar pada sistem	validasi
username (admin@gmail.com)	username (admin@gmail.com)	✓
password (admin)	password (admin)	✓
lokasi (-6.9217 , 107.6071)	lokasi (-6.9222 , 107.6069)	x
waktu (18.36.11)	waktu (09.00.00 - 17.00.00)	x
hari (minggu)	hari(senin, selasa, rabu, kamis, jumaat)	x

Selanjutnya adalah hasil pengujian sistem otentikasi yang diajukan. Pada skenario yang didapatkan pada sistem otentikasi yang diajukan adalah pengguna yang tidak sah tidak bisa langsung masuk kedalam sistem karena konteks yang sah tidak sepenuhnya tervalidasi didalam sistem yang diamana pengguna yang tidak sah tersebut tidak bisa langsung masuk kedalam sistem pengguna hanya *username* dan *password*, parameter yang konteks yang valid bisa dilihat pada Tabel IX. Sistem memberikan otenikasi tambahan yaitu OTP yang dikirimkan dengan SMS ke posel pengguna asli, sehingga pengguna yang tidak sah tidak dapat memasuki kedalam sistem. Sehingga hasil dari skenario pertama untuk sistem otentikasi yang diusulkan menolak pengguna yang tidak sah masuk kedalam sistem.

Tabel VIII: Parameter kontek yang valid

Konteks pengguna pada saat proses otentikasi	Konteks yang terdaftar pada sistem	validasi
username (admin@gmail.com)	username (admin@gmail.com)	✓
password (admin)	password (admin)	✓
lokasi (-6.9222 , 107.6069)	lokasi (-6.9222 , 107.6069)	✓
waktu (11.40.01)	waktu (09.00.00 - 17.00.00)	x
hari (Jumaat)	hari(senin, selasa, rabu, kamis, jumaat)	✓

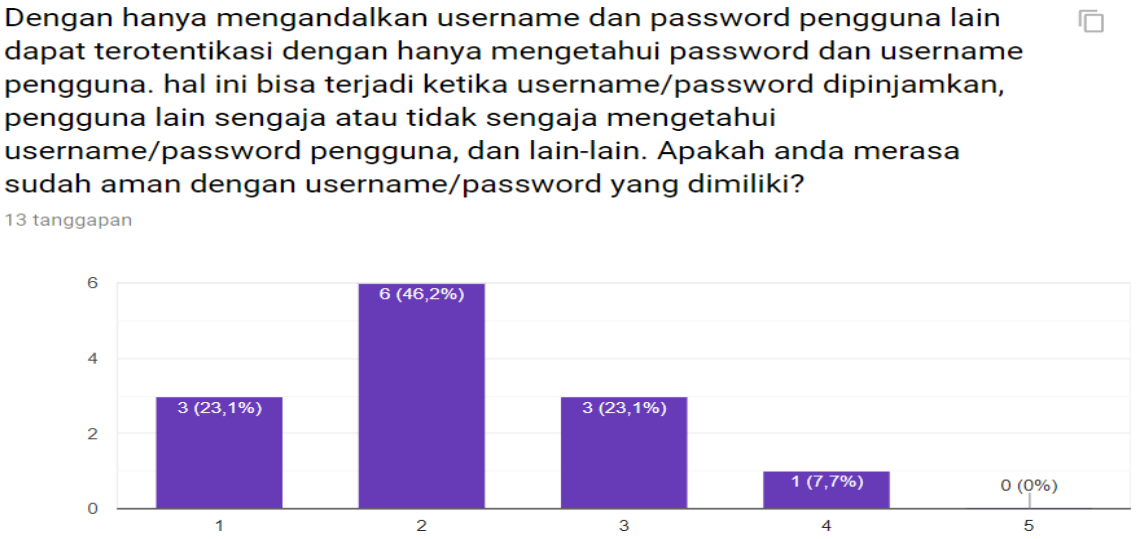
B. Hasil tanggapan pengguna terhadap sistem yang diajukan

Pada bagian ini akan menjelaskan hasil tanggapan pengguna terhadap sistem yang diajukan. Berdasarkan hasil wawancara yang sudah dilakukan, berikut hasil wawancara terhadap pengguna :

1) Topik 1. *Uncover sistem otentikasi pada aplikasi enterprise perusahaan*
   Berdasarkan gambar 10 dapat disimpulkan bahwa sebagian besar dari divisi yang sudah diwawancara telah mendapatkan penyuluhan tentang proses otentikasi (*username,password*. Ini dikarenakan perusahaan sangat memperhatikan proses otentikasi yang masuk dalam sistem aplikasi internal mereka yang memiliki proses bisnis yang sangat sensitif, hal ini juga diperkuat dengan dikeluarkannya peraturan khusus untuk proses otentikasi yaitu "Peraturan Direktur Network IT Solution" yang membahas prosedur otentikasi yang aman sampai persayaratan umum *password*. Untuk jawaban yang diterima pada proses wawancara yaitu 1 adalah iya dan 2 adalah tidak.

Gambar 10: Kuisoner 3 topik 1

2) Topik 2. Evaluasi pada faktor otentikasi pengguna
Berdasarkan hasil wawancara untuk topik 2 yang bisa dilihat pada Gambar 11 dapat disimpulkan bahwa sebagian besar dari anggota divisi sangat khawatir dengan akibat apa yang akan terjadi ketika *username* dan *password* dicuri atau dipinjamkan ke orang lain. Hal ini juga didukung dengan sistem aplikasi *enterprise* perusahaan yang hanya mengandalkan satu faktor otentikasi yaitu *username* dan *password* untuk masuk kedalam sistem. Untuk jawaban yang diterima pada proses wawancara yaitu mulai dari angka 1 adalah sangat tidak aman sampai angka 5 adalah sangat aman.



Gambar 11: Kuisoner 3 topik 1

3) Topik 3. Evaliasi terhadap sistem otentikasi yang diajukan
Berdasarkan hasil wawancara untuk topik 3 yang bisa dilihat pada gambar 12 dapat disimpulkan bahwa sebagian besar dari anggota divisi lebih aman dengan menggunakan sistem otentinkasi yang diajukan dibandingkan proses otentikasi yang sudah ada pada sistem aplikasi internal perusahaan. Pengguna mengharapkan sistem otentikasi ini dapat diterapkan pada perusahaan agar rahasia bisnis internal perusahaan lebih aman dari pengguna yang tidak bertanggung jawab.

Gambar 12: Kuisoner 3 topik 1

VI. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan disesi sebelumnya, sistem otentikasi yang diusulkan pada penelitian ini terbukti dapat mengelolah informasi konteks pengguna. Sehingga sistem otentikasi ini tidak hanya mengandalkan *username* dan *password* sebagai syarat utama untuk masuk kedalam sistem. Selain itu, sistem yang diusulkan dapat mengurangi kekhawatiran pengguna ketika pengguna lain mencuri atau mengetahui *username* dan *password*. Selain itu, berdasarkan proses pengujian sistem langsung ke pengguna hasilnya dapat disimpulkan sistem ini terbukti dapat meningkatkan rasa aman pengguna dalam melakukan proses otentikasi.

Kedepannya sistem otentikasi ini dapat diterapkan ditempat kerja yang memiliki kerahasiaan data yang sensitif agar dapat lebih mengamankan informasi sensitif.

PUSTAKA

[1] M. M. S. A, "ProcurePass: A User Authentication Protocol to Resist Password Stealing and Password Reuse Attack," *in International Symposium on Computational and Business Intelligence*, 2013.

[2] Z. Jinglu, C. Jing, L. Lei and Z. Zhihong, *"The context awareness architecture in mobile cloud computing,"*, Fifth International Symposium on Computational Intelligence and Design, 2012.

[3] P. Charith , Z. Arkady , C. Peter and G. Dimitrios , "Context Aware Computing for The Internet of Things: A Survey," *in IEEE COMMUNICATIONS SURVEYS TUTORIALS*, 2013.

[4] A. Yosef, k. Dylan and H. M. Qusay, "A Context-Aware Authentication Framework for Smart Homes," *IEEE 30th Canadian on Electrical and Computer Engineering (ICCECE)*,2017.

[5] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith and P. Steggles, "Towards a better understanding of context-aware applications," in *Proc. 1st international symposium on Handheld and Ubiquitous Comput*, 2013.

[6] Abena Primo, Vir V. Phoha, Rajesh Kumar and Abdul Serwadda , "Context-Aware Active Authentication Using Smartphone-Accelerometer Measurements," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops*,2014.

[7] Andrew Bissada, Aspen Olmsted , "Mobile Multi-Factor Authentication ", in *The 12th International Conference for Internet Technology and Secured Transactions*,2017.