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 menjamur di lingkungan sekitar kita. Penggunaan perangkat mobile 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.

Maka 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.

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	Logic based	Rules	Subscription	Yes	Low
The context awareness architecture in mobile cloud computing	[2]	System	Graphical Modeling	Probablistic	Query	Yes	High
Fuzzy Logic Based Algorithm for Context Awareness in loT for Smart Home Environment	[6]	Middleware	Graphical Modeling	Fuzzy	Query	Yes	Low
Context-Aware Active Authentication Using Smartphone Accelerometer Measurements	[7]	System	Ontology Based Modelling	Supervised Learning	Query	Yes	High
Penelitian ini		**System**	**Logic based**	**Rules**	**Subscription**	**Yes**	**High**

Pada penelitian [2] menjelaskan penggunaan context awareness dengan menerapkan arsitektur baru yaitu CAA (The Context Awareness Architecture in Mobile Cloud Computing). Pada arsitektur CAA memiliki beberapa details berikut : User's Mobile Device, yang berfungsi sebagai mengumpulan data konteks dari pengguna (catatan telepon, kalender, Global Position System, batterai). Selanjutnya yaitu Decision-making device yang berfungsi sebagai fungsi kalkulasi tingkah laku dan aktifitas berdasarkan algortima context awareness dan dikomparisasi dengan database aktifitas dan tingkah laku pengguna. Service Manager adalah bagian inti dari cloud. Bagian ini berdasarkan hasil dari decision-making device. Bagian ini memiliki kepentingan untuk formulasai dan implementasi untuk protokol baru dan memutuskan apakah mengambil aktivitas yang sering dilakukan oleh pengguna ke database. Selanjutnya Anlyzer and Challenger, pada tahap ini melakukan tingkat karakterisasi berdasarkan pola pengguna yaitu : High-risk, Medium-risk, Low-risk. Selanjutnya Users Characteristics Database pada tahap ini menyimpan karakteristik dan pola dari pengguna ke database untuk bahan anlisis selanjutnya. Hasil dari penelitian ini memungkinkan proses autentifikasi melakukan identifikasi berdasarkan pola pengguna di mobile cloud compiting dan sistem akan menentukan tingkatan keamanan yang akan dipakai berdasarkan pola pemakaian tersebut. Penelitian selanjutnya akan menerapkan metode tersebut pada Android Platform untuk memastikan availability dan flexibility pada algortima CAA.

Pada penelitian [6] membuat sitem otentikasi pada context awareness menggunakan fuzzy logic. Pada fuzzy logic ini pengguna dapat mengatur preferensi dan mengatur rules untuk proses autentifikasi. Pada fuzzy logic yang digunakan dipenelitian ini memiliki beberapa parameter yaitu : nama, lokasi, provider, dan waktu. Setiap parameter tersebut memiliki beratnya masing-masing contoh ketika pengguna tersebut hanya memasukkan nama dan lokasi maka confidence level akan sebanyak 70% tergantung dari syarat dari pengguna. Pada tabel linguistics difuzzy akan menggunakan tingkatan highly, somewhat, more or less.

Tidak sampai disitu, pada penelitian ini juga menggunkan Identity Based Encryption (IBE) yang akan menggabungkan lokasi, nama, email, alamt, dan waktu menjadi informasi yang spesifik pada IBE untuk alasan privasi data pengguna. Hasil dari penelitian ini adalah sangat fleksibel dan proses autentifikasi yang dapat dikembangkan. Penelitian selanjutnya di jurnal ini akan menggunakan secret sharing mechanisms.

Pada penilitian [7] menjelaskan penggunaan context awareness menggunakan algoritma supervised learning. Pada penilitian menggunakan smartphone accelerometers sebagai parameter konteks pengguna. Pengumpulan dataset pada penilitian ini terdiri dari 30 data, data tersebut dari staff atau pelajar. Pengumpulan dataset ini dengan cara setiap sukarelawan akan memegang ponsel cerdas selama 2 menit setiap tangan kanan dan kiri. Hasil dari penelitian [6] yaitu dengan akurasi ketika di pocket data memiliki akurasi 61,76% (hand) dan 72.58% (pocket) sedangkan di hand data meiliki akurasi 82.30% (hand) dan 62.55% (pocket).

Pada penelitian [4] menjelaskan penggunaan context awareness terhadap IOT smart home. Pada penelitian ini menggunakan bobot threshold yang dan security level yang sudah ditentukan oleh pengguna sehingga pengguna dapat menentukan proses otentikasi berdasarkan pandangan pengguna sendiri. Penggunaan threshold itu sendiri untuk menentukan security level apa saja yang akan didapatkan oleh pengguna untuk proses otentikasi.

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.

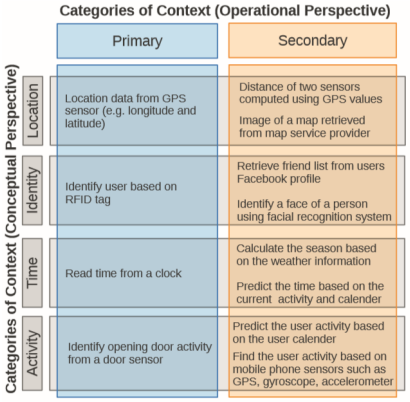
A. *Context Awareness*

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:

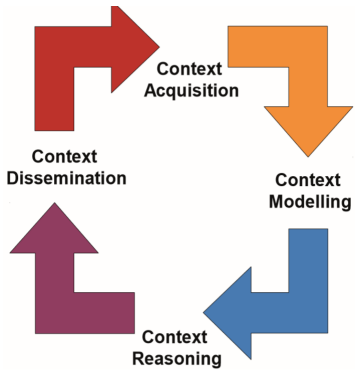
- Primary context: Informasi yang diterima tanpa menggunakan konteks yang ada dan tanpa melakukan operasi fusi data sensor apapun [3].
- Secondary context: Informasi yang dapat dikomputasi menggunakan primary context. Secondary context dapat dikomputasi dari sensor tersebut atau pengambilan data operasi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



Gambar 1: kategori konteks [3].

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

- Context Acquisition, melakukan pengumpulan data konteks yang didapatkan dari beberapa sumber.



Gambar 2: context aware life cycle [3].

- 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.

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.

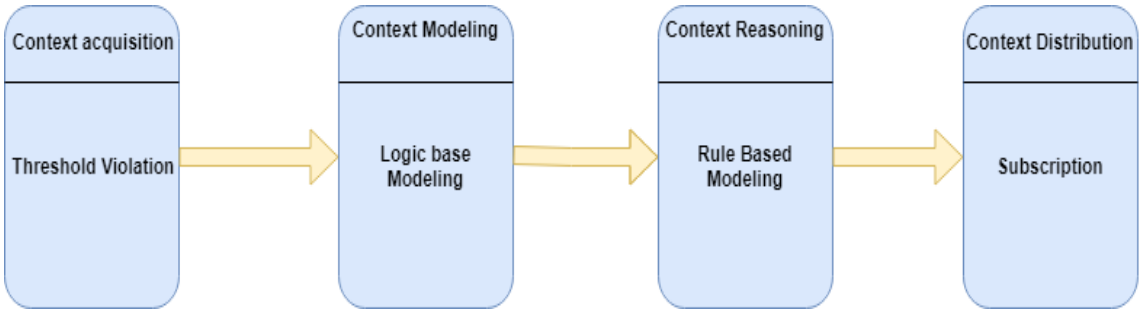
1) Context Acquisition: Pada tahap ini sistem akan menggunakan parameter context yaitu Password/username, lokasi, hari, dan lokasi [3]. Dan pada sesi ini konteks dapat dihasilkan dari threshold violation [3]. Threshold violation dimana sistem perlu menditeksi peristiwa untuk mengambil konteks [3]. Penggunaan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

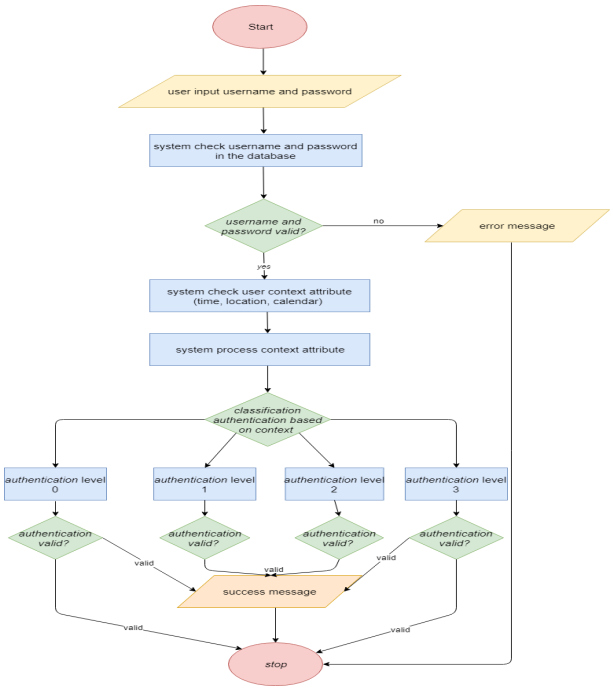
Berdasarkan beberapa setiap alur mode yang sudah dijelaskan diatas maka flow chart alur model context bisa dilihat di gambar 3.



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*.



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. Pendaftaran itu meliputi username/password dan onteks pengguna Data-data pengguna bisa dilihat di tabel II.

Tabel II: Atribut konteks pengguna

Username	admin@gmail.com
Password	admin
latitude	-69,222
longtitude	107.6069
waktu_awal	09.00.00
waktu_akhir	17.00.00

   Pengguna juga sudah menentukan bobot konteks untuk setiap parameter keberhasilan. Ini nantinya berfungsi ketika context modeling.

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.

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. Ditahap ini sistem melakukan proses validasi terhadap database dengan membandingkan context pengguna yang sudah didaftarkan dan context pengguna yang dibawa pada saat melakukan otentikasi. Pada table V memperlihatkan beberapa parameter context pengguna yang valid yang dilakukan oleh pengguna tidak waktu yang bersamaan.

Tabel V: Context Acquisition

Parameter yang diterima
Password/username, hari, lokasi, waktu
Password/username, hari, lokasi
Password/username, lokasi
Password/username

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 (Tabel III), selanjutnya proses ini melakukan perhitungan berdasarkan bobot yang sudah diambil. Proses context modeling bisa dilihat di Table VI.

Tabel VI: Context Modelling

Paramter yang diterima	Bobot Parameter	Total Bobot
Password/username, hari, lokasi, waktu	(40+10 +20+30)	100
Password/username, hari , lokasi	(40+20+30)	90
Password/username, dan lokasi	(40+30)	70
password/username	(40)	40

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 dihasilkan berdasarkan total bobot konteks, penentuan syarat klasifikasi ini bisa dilihat pada pra-kondisi sistem (Tabel IV). Hasil klasifikasi ini diteruskan ke proses context distribution, proses context reasoning bisa dilihat di Tabel VII.

Tabel VII: Context Reasoning

Total Bobot	level
100	Level 0
90	Level 1
70	Level 2
40	Level 3

5) Context Distribution
Selanjutnya proses context distribution, proses ini merupakan lanjutan proses dari context reasoning. Diproses ini hasil dari klasifikasi dari context reasoning diteruskan dengan cara yang lebih bermakna ke pengguna. Setiap level otentikasi memiliki fitur yang mengharuskan pengguna untuk menggunakan fitur tersebut untuk masuk kedalam sistem. Proses context Distribution bisa dilihat pada table VIII

Tabel VIII: Context Reasoning

Total Bobot	level	Jenis Otentikasi
100	Level 0	Grant access
90	Level 1	Security Question about structural company
70	Level 2	One Time Password
40	Level 3	Security Question about last login

D. Prosedur pengujian

Pengujian sistem dilakukan dengan membandingkan sistem kemanan otentikasi yang diajukan dan sistem otentikasi yang ada. Selain itu, pengujian ini dilakukan untuk membuktikan tujuan dari penelitian ini yaitu sistem otentikasi yang tidak bergantung hanya dengan password dan username untuk masuk kedalam sistem dan sistem dapat mengelolah informasi konteks pengguna

Sistem yang akan dibandingkan ada sistem otentikasi yang konvensional yang memiliki *username* dan *password* sebagai salah satu faktor otentikasi, untuk melihat perbandingan sistem bisa dilihat di tabel IX:

Tabel IX: Perbandingan sistem

Sistem Otentikasi	Username/password	Context Awareness
Sistem yang sudah ada	✓	
Sistem yang diajukan	✓	✓

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.

Untuk mendapatkan perbandingan keamanan dari kedua sistem. Digunakan beberapa skenario yang dapat terjadi di sistem otentikasi *login system*. 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.
2) Pengguna yang sah melakukan otentikasi dengan konteks pengguna tidak lengkap : pada skenario ini pengguna melakukan otenikasi seperti biasa menggunakan *username* dan *password* tetapi pengguna tidak menyertakan informasi konteks yang sah atau tidak lengkap. Sehingga, pengguna akan mendapatkan faktor otentikasi tambahan berdasarkan konteks yang sah ke dalam sistem. Skenario ini diharapkan pengguna dapat masuk kedalam sistem melalui jenis otentikasi.

V. HASIL DAN PEMBAHASAN

Pada bagian ini akan menjelaskan hasil pengujian berdasarkan skenario yang sudah dijelaskan pada sesi sebelumnya. Hasil yang didapatkan dari skenario pertama yaitu pengguna yang tidak sah. Pada sistem otentikasi yang konvensional yang digunakan yang hanya mengandalkan *username* dan *password*, pengguna yang tidak sah dapat masuk kedalam sistem. Sehingga skenario pertama untuk sistem ontentikasi konvesional gagal. 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 hanya memiliki *username* dan *password* valid. Sistem akan memberikan pertanyaan keamanan kapan waktu terakhit pengguna asli melakukan proses otentikasi yang dimana hanya pengguna asli lah yang hanya mengetahui informasi tersebut, sehingga pengguna yang tidak sah tidak dapat memasuki kedalam sistem. Sehingga hasil dari skenario pertama untuk sistem otenikasi yang diusulkan menolak pengguna yang tidak sah masuk kedalam sistem.

Pada skenario kedua, sistem otentikasi konvensional pengguna yang sah dapat langsung masuk kedalam otentikasi dengan hanya menggunakan *username* dan *password*. Untuk sistem otentikasi yang diajukan, pengguna yang melakukan otentikasi dengan membawa paramter konteks yang valid yaitu (password/username, hari, dan lokasi) sehingga sistem memberikan otentikasi tambahan yaitu OTP. Sehingga hasil dari pengujian untuk skenario ini pengguna sukses masuk kedalam sistem. Tabel X menunjukan hasil pengujian berdasarkan hasil skenario pengujian.

Tabel X: Hasil pengujian

Sistem Otentikasi	Skenario 1	Skenario 2
Sistem yang sudah ada	Sukses	Sukses
Sistem yang diajukan	Tidak Sukses	Sukses

VI. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan disesi sebelumnya, sistem otentikasi yang diusulkan pada penelitian ini terbukti dapat mengelolah informasi konteks pengguna dan sistem otentikasi ini tidak hanya mengandalkan *username* dan *password* sebagai syarat utama untuk masuk kedalam sistem.

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, Tirupur, India, 2013.
[2] Z. Jinglu, C. Jing, L. Lei and Z. Zhihong, "The context awareness architecture in mobile cloud computing," in 2012 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," in 2017 IEEE 30th Canadian on Electrical and Computer Engineering (ICCECE), Oshawa,Ontario,L1H7K4 Canada, 2017.
[5] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith and P. Steggles, "Towards a better understanding of context and context-awareness," in Proc. 1st international symposium on Handheld and Ubiquitous Comput, London, 1999.
[6] Arpit Patel, Prof. Tushar A. Champaneria, "Fuzzy Logic Based Algorithm for Context Awareness in loT for Smart Home Environment ," India, Ahmedabad,
[7] Abena Primo, Vir V. Phoha, Rajesh Kumar and Abdul Serwadda , "Context-AwareActive Authentication Using Smartphone-Accelerometer Measurements," in IEEE Conference on Computer Vision and Pattern Recognition Workshops, Ruston, Louisiana, USA, 2014.
[8] B. Y. Lim and A. K. Dey, "Toolkit to support intelligibility in context-aware applications," in Proc. 12th ACM international conference on Ubiquitous computing, New York, NY, USA, 2010.
[9] MaÂĺelick Claes, Mika MÂĺantylÂĺ , Miika Kuutila and Bram Adams, "Abnormal Working Hours: Effect of Rapid Releases and Implications to Work Content," in 2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR), Finland , 2017.