

Context Awareness Adoption for Authentication Process in Login System

Fikri Attamami Laguliga^{*}, Parman Sukarno[†] and Rahmat Yasirandi[‡]

Abstract

Many researchers have evaluated authentication system security. The conventional process of authentication systems only requires a username and password to authenticate. But this method is very convenient to be said to be safe from all forms of an attack until you can authenticate without permission by only using a password and username. In this study, we will use the context awareness method as the foundation of the retrieval system, while the system will take user relationship 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 a new authentication process. This research is proven in overcoming the authentication process against unauthorized users based on testing the login scenario on the system. The proposed system also provides a sense of security to the user as evidenced by testing the deployment system so that users can experience the effects of the authentication system submitted, the user who is the object of research is from a General Affair division at PT Telkom Indonesia.

1. Introduction

The last few years the use of mobile devices is very much in the environment around us. The use of a mobile device is because they have advantages, one of them is the comfort in accessing data. But most of the process of obtaining personal data requires an authentication process. The conventional authentication process only needs to specify a username and password to carry out the authentication process

On the other hand, devices with high mobility can easily be lost, stolen, or used by unauthorized people. Paying attention to the parameters of each individual during the authentication process will help secure authentication to ensure that the login process is the owner. If authentication sees more than one parameter it is also known as context awareness.

^{*}E-mail: eriklaguliga@telkomuniversity.ac.id

[†]E-mail: psukarno@telkomuniversity.ac.id

[‡]E-mail: batanganhitam@telkomuniversity.ac.id

Context awareness itself is information that can be used to characterize the situation of an entity and an entity is a user, place, or object that is considered relevant to the user's interaction and the application itself. Research on context awareness is not new to the authentication system. The study has context awareness in the authentication system in mobile cloud computing which is proven to reduce the possibility of unauthorized people can carry out the authentication process, but from research requires historical data authentication users for system needs to study the context of users, so that the authentication system in this study is lacking can be relied upon when a user first uses an authentication system and the user cannot determine the authentication factor based on the user's view.

In this study applying context awareness on the login system that is not dependent on historical user authentication data and the mechanism in this study is also expected to facilitate users to provide several authentication factors based on the user's view. The proposed system is also likely to provide users with a sense of security when conducting authentication.

2. Literatur Review

Authentication system security is essential because it is a factor of consideration for users. The following is a comparison of methods on authentication systems that use context awareness.

Research [2] explains the use of context-awareness by applying a new architecture namely CAA (The Context Awareness Architecture in Mobile Cloud Computing). In this study using several context parameters, namely: telephone records, calendars, Global Position Units, and batteries. This study uses Graphical modeling that allows the system to accommodate a lot of data, which will then be used in the context reasoning process. This study also uses supervised learning reasoning, which in this study is called Decision-making device, this process calculates stored behavior and behavior that is being carried out by the user using and then comparing user data that has been stored in the database, but using supervised learning on context reasoning requires user data that has been saved before, the system recognizes user files and user functions. The use of context distribution in this study uses a query method wherein the query results in authentication results aimed at the user.

In research [6] explains the use of context-awareness that utilizes an accelerometer sensor for authentication systems. The use of context modeling in this study is the same as a research [2], namely graphical modeling, the model process carried out by this research by collecting datasets of 30 data. This data collection is done by each volunteer holding two smartphones for each right hand and left hand. The use of this context reasoning uses a supervised learning method that requires a dataset so that the system recognizes user activity based on the accelerometer sensor movement. The results of this study have an accuracy when the smartphone is held at 61.76% when the smartphone is held and 72.58% while for accuracy when the smartphone training data is held at 82.30% in hand and 62.55% in the bag.

In the study [4] describes the use of context-awareness in the authentication system on IoT smarhome. The use of context modeling in this study is logic based modeling,

TABLE 1

Project name	citation	Project focus	Modeling	Reasoning	Distribution	History and storage	Level of context awareness
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	Probabilistic	Query	Yes	High
Context-AwareActive Authentication Using Smartphone Accelerometer Measurements	[6]	System	Graphical Modeling	Supervised learning	Query	Yes	High

where this model can provide rules that are used to express the user's policies and preferences towards the system. This study also uses the rules method that allows users to determine several conditions for authentication levels based on the user's views. And for context Context Distribution uses a Subscription method that enables context consumers to subscribe to the system by declaring what requirements are needed to determine the level of authentication.

From some of the above studies, it has been explained that there is no use of the context awareness method in the authentication process on the login system. So the proposed system that uses context awareness in the login system that uses logic based modeling is that context modeling and rules are processed using context reasoning that allows users to determine authentication factors based on user preferences, using system methods can easily model the user's mind [3]. The choice of the technique also allows the authentication system not to require the user's training data to determine whether the user is authenticated or not authenticated.

3. Metodelogy

3.1. Problem Identification

In the initial stages of this research, identify problems that are faced. Problem identification has been presented in the introductory chapter. This chapter describes what issues will be related to supporting the course of this research. These problems are also supported by the presence of several other studies that have similar issues.

3.2. Defining goals

The next step in this research is to conduct a review of the research that has similar problems and uses identical methods. Next, we will compare the research related to authentication using this context-aware method to be carried out in the next stage so that at this stage it is expected to get the objectives and techniques to be applied in this study.

3.3. Design and development

In this step, design the authentication system using the context awareness method. Following is a brief explanation of the context awareness method:

3.3.1. Context Awareness

Context is information that can be formalized in the situation as an entity. From these entities can be as a user, place, or object that is considered relevant to the interaction between the user and the application [5].

A system that has context-aware when using multiple contexts that provide information and are relevant to services to users, where the value of that relevance depends on the user itself [5].

In context-aware itself, there is a categorization scheme that can be seen in Figure 1:

- Primary context: Information received without using the current context and with-

out carrying out any sensor data fusion operations [3].

- Secondary context: Information that can be computed using a primary context. Secondary context can be calculated from the sensor or retrieval of operating data such as (telephone data, address, email, etc.) [3].

			Categories of Context (Operational Perspective)	
			Primary	Secondary
Categories of Context (Conceptual Perspective)	Location	Location data from GPS sensor (e.g. longitude and latitude)	Distance of two sensors computed using GPS values Image of a map retrieved from map service provider	
	Identity	Identify user based on RFID tag	Retrieve friend list from users Facebook profile Identify a face of a person using facial recognition system	
	Time	Read time from a clock	Calculate the season based on the weather information Predict the time based on the current activity and calendar	
	Activity	Identify opening door activity from a door sensor	Predict the user activity based on the user calendar Find the user activity based on mobile phone sensors such as GPS, gyroscope, accelerometer	

FIGURE 1: context category

In context-aware it has a life cycle based on the Figure 2. which consists of 4 phases:

- Context Acquisition, collects context data obtained from several sources.
- Context Modeling provides a model or method to produce meaningful results.
- Context Reasoning, processed data to become high-level context information.
- Context Dissemination, high-level context is distributed to users who need results from that context.

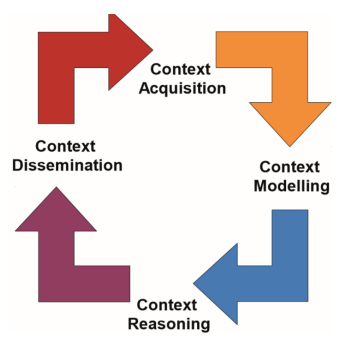


FIGURE 2: context aware life cycle [3]

3.4. Deployment

In this stage, the system that has been developed will then be launched to users who will try the system so that this process is useful for the next process, namely the testing process based on user evaluation.

3.5. evaluation (System scenario)

In this phase, the system that has been deployed will be tested by the system. System testing carried out at this stage uses several login scenarios to computationally analyze the success of the system in managing the user's context for the authentication process.

3.6. Evaluation (User)

In this stage, the system that has been deployed will be evaluated by users who have tried the system. This user evaluation will be carried out by interviewing and collecting the questionnaire to get results from the steps of the users who tried the system proposed in this study.

3.7. Kesimpulan

In this stage, the results of the system scenario evaluation and user evaluations that have been made will be concluded. And at this stage recommendations will be made based on the results of the assessment.

4. system design and development

In this chapter, we will explain the context awareness model that is applied to the authentication process on the login system. The use of the model in the authentication system is based on the context lifecycle described in the previous chapter, so in this chapter we will explain each model flow in detail.

4.1. Context Acquisition

At this stage the system will use context parameters, namely Password / username, location, day, and location [3]. And in this session the context can be generated from threshold violation [3]. Threshold violation where the system needs to detect events to take context [3]. The use of this threshold weight will allow users to determine the weight of their context by the wishes of the user.

4.2. Context Modeling

At this stage the data collected needs to be modeled and presented in a meaningful way. The method used for this model is Logic based modeling [3], the model allows information on new high-level contexts to be extracted using a low-level context. The use of this method will enable users to determine the rules and logic when the system is running.

4.3. Context Reasoning

At this stage the data collected needs to be modeled and presented in a meaningful way. The method used for this model is Logic based modeling [3], the model allows information on new high-level contexts to be extracted using a low-level context. The use of this method will enable users to determine the rules and logic when the system is running.

4.4. Context Distribution

At this stage, the context that has been processed from the context reasoning system will send results from that context. The method used is Subscription [3] which allows the context of users to subscribe to the context of the management system by describing user needs. The system will provide results periodically when something happens or according to the weight of the violation.

Based on some of the flow modes described above, the flow chart of the context model can be seen in figure 3.

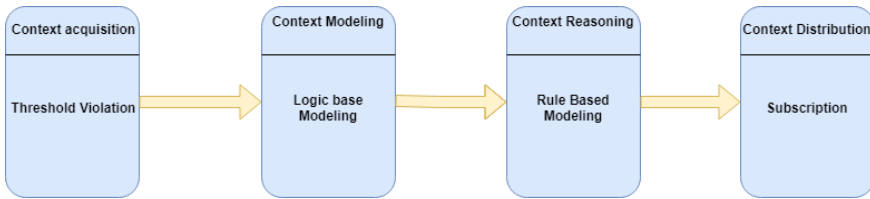


FIGURE 3: Context diagram

4.5. System Design

Figure 4 shows that the authentication system that is built requires the user context to authenticate. First, users are still required to enter a username/password that has been registered into the system as the initial stage of the authentication process. Next, when the user's username/password is correct, the system will take the user's context as an authentication requirement. Furthermore, when the system has collected user context, the system will classify the type of authentication level that is given to users based on the context collected by the system. This authentication level will have a type of authentication starting from level 0, that users can directly enter the system without additional authentication, for level 1 the system will provide security questions about the organizational structure, for level 2 the system will send One Time Password to be sent to users via SMS, and for level 3 the system will provide security questions about the time information when users authenticate. The types of authentication are Multi-factor authentication representations that have something you know, something you have, and something you are [7].

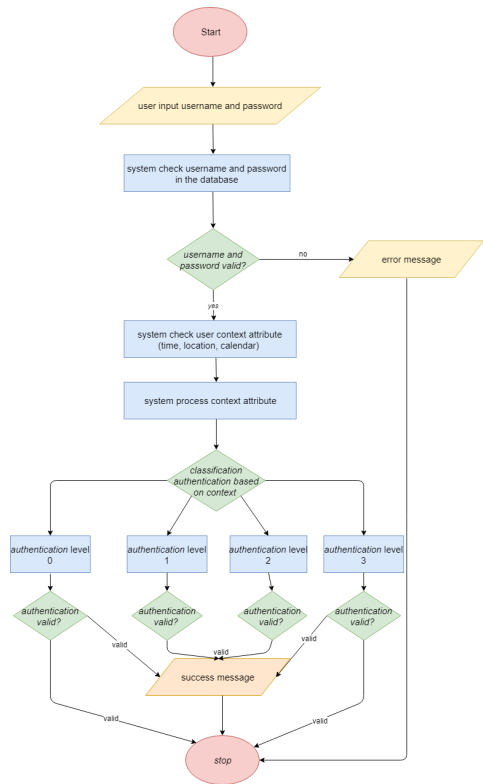


FIGURE 4: System Design

4.6. System Development

This session will explain the process of developing an authentication system for this research. In this chapter, the development process starts from the Context Acquisition process until the most recent process is Context Distribution.

4.6.1. Precondition

In this session, an authentication system with context-aware is implemented on a personal computer. Previously the user has registered and stored in the database. Registration can include username/password and user context User data can be seen in Table 2.

Users have also determined the context weights for each parameter of success. This later works when context modeling, users are required to enter a standardized weight and password higher than the other parameters because the internal password and password are the first authentication requirements to enter the system. For more details, see Table 3.

The user has also determined the authentication level requirements. This authentication requirement will function on the provision of authentication conditions based on heavy context calculations, weighting authentication level requirements must be smaller than the previous level because the higher the level of authentication the higher the level

of authenticity the lower the level of trust the user system can be seen in Table 4.

TABLE 2
User Context Attributes

username	admin@gmail.com
Password	admin
Longitude	107.6071
Latitude	-6.9217
start time	09.00.00
end time	17.00.00
day	Monday, Tuesday, Wednesday, Thursday, Friday

TABLE 3
Context weight

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

TABLE 4
Secuirty Level

Security Level	weight requirements
level 0	$x = 100$
level 1	$0 \leq X < 100$
level 2	$41 \leq X < 80$
level 3	$0 \leq X < 41$

4.6.2. Context Acquisition development

Acquisition context is the first thing when the user interacts. Processed this system takes valid parameters. The user performs the process. Users use passwords and passwords, the login user interface can be seen in Figure 5.

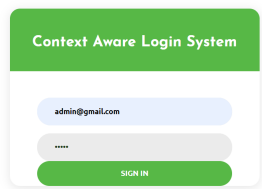


FIGURE 5: Authentication Context Aware System Login Form

In this phase the system performs a validation process of the database by comparing the registered user context and the context of the user that was carried out during authentication, the Context acquisition algorithm can be seen in Algorithm 1. Algorithm 1 describes the Context Acquisition process in the system login. In the early stages the system retrieves the username and password when the username and password are successfully validated, the system retrieves the context parameters that have been stored in the database stored by the new variable. Next, the system takes the current context data (day, time, and location) and compares the context data that has been taken in the database for the context validation process and is forwarded to the context modeling process for the context calculation process.

Algorithm 1: Algortima Context Acquisition di sistem login

```

cek login = database(username,password);
if jumlah data yang ditemukan pada variabel ceklogin > 0 then
    for cek login sebagai variabel cek do
        database(email) = cek(email);
        database(password) = cek(password);
        database(latitude) = cek(latitude);
        database(longtitude) = cek(longtitude);
        database(waktu awal) = cek(waktu awal);
        database(waktu akhir) = cek(waktu akhir);
        database(hari) = cek(hari);
    end
    hari sekarang = get day("D");
    waktu = get time ;
    ip = get content('https://api.ipify.org');
    lokasi =get content ('http://ip-api.com/json/',api);
    lokasi = json decode(lokasi);
    lat = lokasi ->lat;
    lon = lokasi ->lon;
    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

```

4.6.3. Context Modeling Development

At this stage, the parameters that have been validated by context acquisition are given weighting on the parameters that have been verified. The system retrieves context weight data in the database the data has been registered, then this process calculates based on the weight that has been taken. The method of context modeling can be seen in Algorithm 1. In the early stages of the context modeling process, the system takes the score on each parameter that has been stored in the database. furthermore, when the system has validated context parameters, the order will weight the validated context parameters. Later the results of the weight of the context modeling process will be processed again with context reasoning.

Algorithm 2: Algoritma Context Modeling di sistem login

```

cek login = database(username,password);
nilai = 0;
if jumlah data yang ditemukan pada variabel ceklogin > 0 then
    for cek login sebagai variabel ta do
        database(score calender) = ta(score calender);
        database (score identity) = ta(score identity);
        databse (score lokasi)= ta(score lokasi);
        database (score time) = ta(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

```

4.6.4. Context Reasoning Development

Furthermore, the context reasoning process performs a classification process based on the total weights that have been processed in context modeling. This process determines what level of authentication is generated based on the total weight of the context, determining this classification requirement can be seen in the pre-condition of the system (Table IV). Algorithms in this process can be seen in Algorithm 3.

Algorithm 3: Algoritma 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

```

4.6.5. Context Distribution Development

Furthermore, the process of context distribution, this process is an advanced process of context reasoning. Processed, the results of classifications of context reasoning are continued in a more meaningful way to the user. Each level of authentication has a feature that requires users to use these features to enter the system, these features are a representation of the Multi-factor authentication that has been described in the system design section. The following in the context reasoning process can be seen in Algorithm 4.

Algorithm 4: Algoritma 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

```

When a user gets to level 1 authentication, the user is required to fill out a security question against the user’s organizational knowledge. This level of authentication is a representation of something you know in Multi-Factor Authentication. The form of an authentication form can be seen in Figure 6.

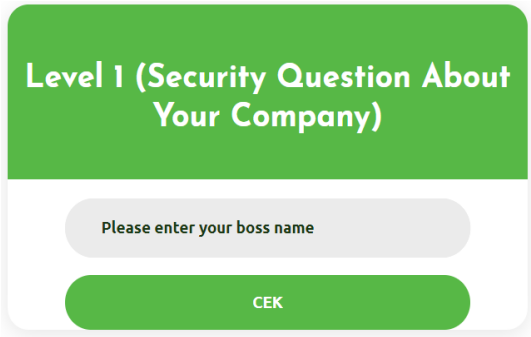


FIGURE 6: User Interface level 1 form

When a user gets to level 2 authentication, the user will be required to fill in the One Time Password, or it can be called an OTP. This OTP code is sent via SMS to the user’s cellphone. One Time Password is a form of representation of something you have in Multi-Factor Authentication. Form user level 2 authentication can be seen in Figure 7.

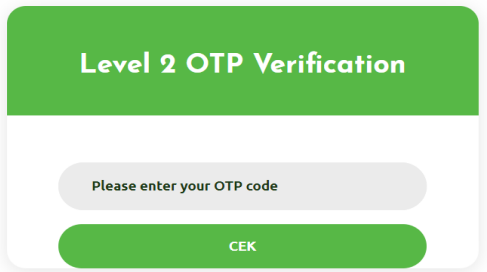


FIGURE 7: User Interface level 2 form

When user users get the lowest authentication level, level 3, users will be required to fill out a Security Question about the information on when the user logged in to the system. Every time the user login information will be sent via SMS sent to the user so that the user can remember the information when the user logged in. Level 3 is a representation of something you are on an authentic multi-factor. The shape of the user interface can be seen in Figure 8.



FIGURE 8: User Interface level 3 form

4.7. The Context Aware Authentication System Protocol

The proposed authentication is an authentication system that can take the context for the authentication process. In this section, it describes the transfer of workflow functions in the authentication process.

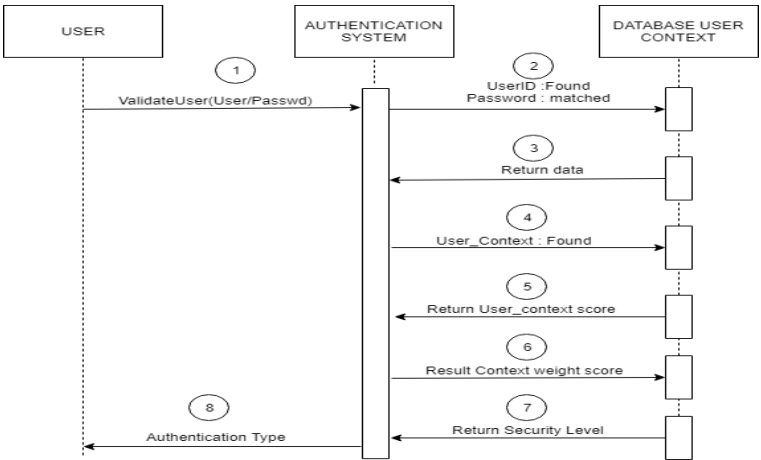


FIGURE 9: Context diagram

5. Testing procedure

Figure 5 shows a sequence diagram that is in the system. Users will still enter their username and password. The user context is processed after the user has entered a valid username and password, for details will be explained below:

- 1. *User → Authentication system*
The user enters a username and password that has been registered in the system. the system will forward to the database for matching

2. *Authentication system → Database User Context*
The system validates passwords and usernames against the system database.
3. *Database User context → Authentication System*
The system will create a session against the authenticated username and password.
4. *Authentication system → Database User context*
The system takes the user context, the context that is made on the user when the login process is: Location, Time, and day. And the system validates the context of the Context Database that has been registered.
5. *Database User Context → Authentication system*
When the user context has been validated, the system will send context weight data that matches the user's context during the authentication process.
6. *Authentication system → Database User Context*
After the system has finished calculating the context the system user sends context to database weights for the security level validation process.
7. *Database User Context → Authentication System*
The database returns a level requirement that matches the weight of the context that has been processed.
8. *Authentication System → User*
The system provides a type of authentication to users based on the security level in the database.

6. Evaluating

Testing on the system proposed by performing several authentication scenarios and measuring the user's sense of security in using the proposed system. This test was conducted to prove the purpose of this study, namely an authentication system that does not depend only on username and password and authentication systems that can manage the user context for the authentication process. Before testing, pre-conditions that must be met will be determined:

1. the system must have the ability to manage user context.
2. The user already has user context data, the proposed user context data can be seen in the previous sub-section.

6.1. System testing scenario

The following scenarios are carried out during testing:

1. Obtain User Login and Password: in this scenario the user's username and password are stolen, compromised, or even lent. Users who are not responsible for the authentication process, users also do not know the original user context information. So, the expected result is that the system can recognize the user's authentication

pattern irresponsibly and provide additional authentication to enter the system. For reviewing the test scenario can be seen in Table 1.

TABLE 5
System Scanrio 1

Test type	Obtain User Login and Password
Criteria	The system requires a username and password, and the system manages the user's context
Procedure	User's username and password were stolen. Irresponsible users will carry out the authentication process.
Expectations	the system can recognize the user's authentication pattern irresponsibly and provide additional authentication to enter the system.

2. Users authenticate outside the context agreement: in this scenario, the original user performs an authentication but in this scenario, the user performs authentication but outside the context that has been registered in the authentication system. Expected results users will get additional authentication to enter the system based on the results of managing the context when users authenticate. For a summary of the test scenario, see Table 2.

TABLE 6
System Scanrio 1

Test type	Login trial
Criteria	The system requires a username and password, and the system manages the user's context
Procedure	this scenario, the original user authenticates, but the user authenticates outside the context agreement.
Expectations	the user will get additional authentication to enter the system based on the results of managing the context when the user authenticates.

6.2. *Questionnaire testing*

Next, the testing procedure uses questionnaire. Users who will fill out this questionnaire are members of a division that is not related to IT, namely the General Affair division, which is responsible for managing organizational administration and secretariat. The objectivity of this questionnaire is:

1. Uncover the system of user authentication on enterprise enterprise applications: Users will be asked questions about knowledge about corporate counseling about procedural authentication.
2. evaluation of authentication factors that users use in enterprise applications: Users will be given questions about the authentication system knowledge used by the

company and provide information on some of the worst possibilities when the authentication system only has one authentication factor, namely username and password.

3. Evaluation of the proposed authentication system: Users will be given several questions to evaluate the authentication system they want.

7. Results and Discussion

In this section, we will explain the results of testing the system proposed in this study.

7.1. System testing scenario

This section will explain the results of the test based on the proposed scenario, summary scenario. The test results in the second scenario are users getting authentication. This is definitely due to not all user contexts being validated in the system. The following is the user context data when performing authentication, which can be seen in Table 7. The system provides additional authentication, namely OTP that is sent by SMS to the original user's email, sothat unauthorized users cannot enter the system. So the results of the first scenario for theproposed authentication system reject unauthorized users entering the system. So the expected results in this scenario prove that users get additional authentication.

TABLE 7
Valid context data

User context during the authentication process	Context listed on the system	Validation
username (admin@gmail.com)	username (admin@gmail.com)	True
password (admin)	password (admin)	True
location(-6.9222 , 107.6069)	lokasi (-6.9222 , 107.6069)	True
time(11.40.01)	waktu (09.00.00 - 17.00.00)	False
day(Friday)	day (Monday, Tuesday, Wednesday, Thursday, Friday)	True

Next is the result of testing the authentication system submitted. In the scenario obtained in the authentication system that is submitted is that the unauthorized user cannot directly enter the system because the legitimate context is not fully validated in the system where the unauthorized user cannot directly enter the user's system, only the username and password, the parameter valid context can be seen in Table 8.So that based on valid context calculations with context data registered in the database, the user gets the authentication added by the security question about the information when the user is doing authentication.

TABLE 8
Valid context data

User context during the authentication process	Context listed on the system	Validation
username (admin@gmail.com)	username (admin@gmail.com)	True
password (admin)	password (admin)	True
location(-6.9217 , 107.6071)	lokasi (-6.9222 , 107.6069)	False
time(18.36.11)	waktu (09.00.00 - 17.00.00)	False
day(Sunday)	day (Monday, Tuesday, Wednesday, Thursday, Friday)	False

7.2. Questionnaire testing

This section will explain the results of user responses to the proposed system. Based on the results of the interviews that have been conducted, the following are the results of interviews with users:

- 1. Topics 1. *Uncover system authentication on enterprise enterprise applications*
Based on Figure 10, it can be concluded that most of the divisions that have been interviewed have received counseling about the authentication process of username, password. This is because companies are very concerned about the authentication process that is included in their internal application systems that have very sensitive business processes, this is also reinforced by the issuance of special regulations for the authentication process, namely "Regulation of Director of Network IT Solution" which addresses secure authentication procedures to the requirements general password. For answers received in the interview process, namely one is yes and two is no.

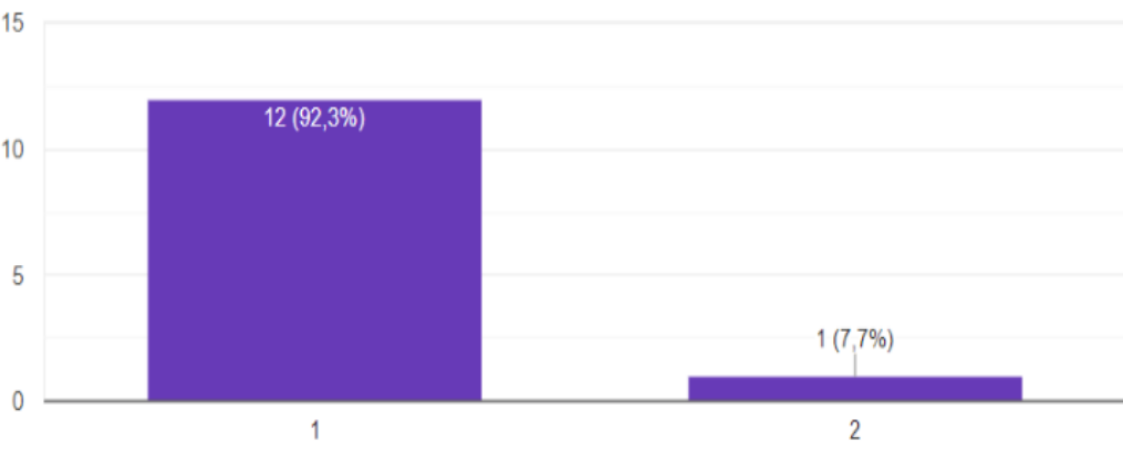


FIGURE 10: Kuisoner 3 topik 1

2. Topics 2. Evaluation of user authentication factors

Based on the results of interviews for topic two which can be seen in Figure 11, it can be concluded that most of the division members are very worried about the consequences of what will happen when the username and password are stolen or lent to someone else. This is also supported by enterprise application systems that only rely on one authentication factor, namely username and password to enter the system. For answers received in the interview process, starting from number 1 is very insecure until number 5 is very safe.

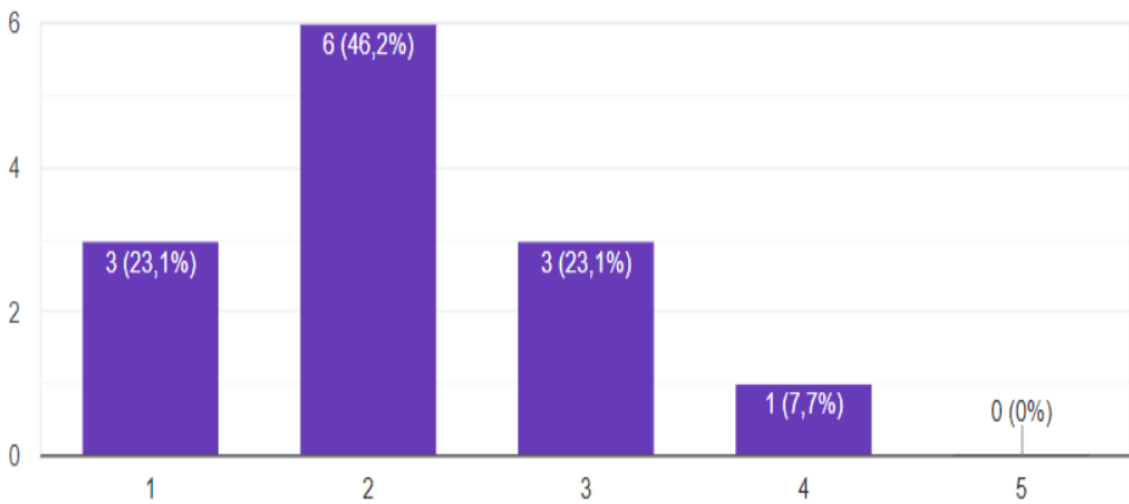


FIGURE 11: Kuisoner 3 topik 1

3. Topics 3. Evaluation of the authentication system submitted

Based on the results of interviews for topic three which can be seen in Figure 12 it can be concluded that most of the division members are safer by using the proposed authentication system compared to the existing authentication process in the company’s internal application system. Users expect this authentication system to be applied to companies so that the company’s inner business secrets are safer than irresponsible users.

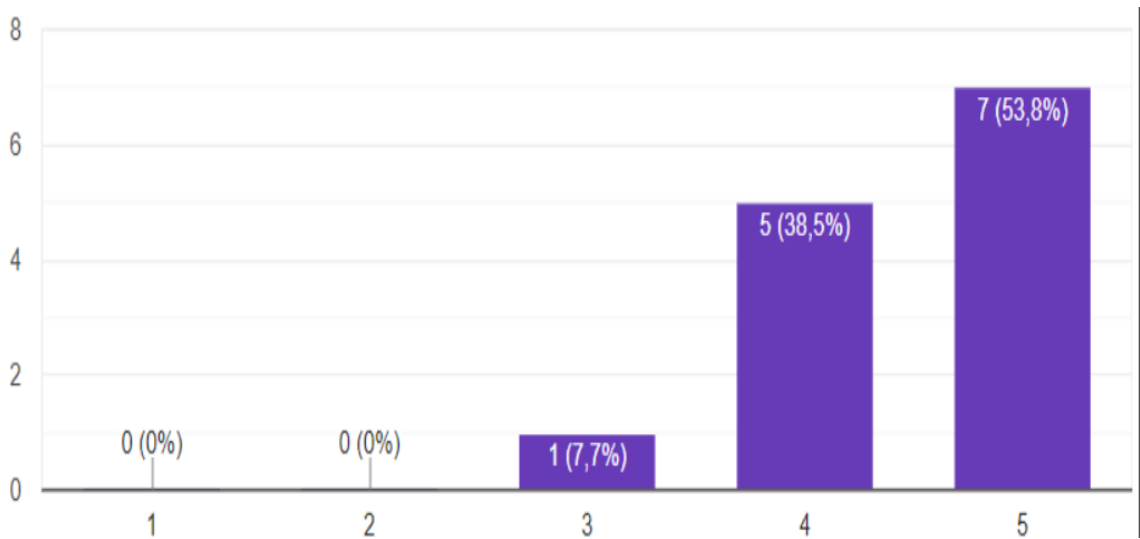


FIGURE 12: Kuisoner 3 topik 1

8. Conclusion

Based on the tests carried out in the previous session, the authentication system proposed in this study proved to be able to manage user context information. So that this authentication system does not only rely on usernames and passwords as the main requirement to enter the system. Also, the proposed system can reduce user concerns when other users steal or know their username and password. Also, based on the system testing process directly to the users of the results, it can be concluded that this system is proven to increase the user's sense of security in the authentication process.

In the future, this authentication system can be applied in a workplace that has the confidentiality of sensitive data to better secure confidential information.

References

[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-AwareActive Authentication Using SmartphoneAccelerometer 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.