Journal of Engineering and Applied Sciences 13 (8): 2209-2220, 2018
ISSN: 1816-949X

Implementation of Two-Factor Authentication (2FA) to Enhance the Security of Academic Information System

[1]Gigih Forda Nama and [2]Kurnia Muludi
[1]Department of Informatics Engineering,
[2]Department of Computer Science, University of Lampung, Lampung, Indonesia

Abstract: Academic information system play an important role to serve the information technology needs of the academic programs at University of Lampung these system are usually implemented on higher education in order to provide a validity and reliability of academic data. University of Lampung (Unila) has a long history in development of Academic Information System (Siakad), starting with manual system, semi-online and full online. To enhance the security level of Siakad application, further more in this study, described the design and implementation process of two-Factor Authentication (2FA) that was already deployed on Siakad application and running well, since, 2013 it used the account knowledge (username/password) and also account possession (security token on users mobile phone) factors. Both of these factors are implemented for user authentication, it proven that the security become better and made it more difficult to bypass and minimize the possibility of unauthorized access. Data retrieval of system usage statistic conducted, since, April 2014 until April 2016 from the system report shown there were total 29483 time One Time Password (OTP) code sent to user's mobile phone. Usually on January or August each year there will be an increased number of OTP code sent to user because on January was the end of even semester and August was the end of odd semester. The most popular cellular provider used by user was TELKOMSEL with total 77% registered number, INDOSAT with 18% number used, XL with 3% number registered and TRI with total 2% number registered with this various number of cellular number usage, we analyzed that mean time the OTP code delivery was 22.87 sec, this mean time value was still within the threshold of tolerance time accepted by user, indicated the system research as well.

Key words: Two-Factor Authentication (2FA), one time password, OTP code, academic information system, application security, Siakad Unila

INTRODUCTION

Academic information system play an important role to serve the information technology needs of the academic programs at University of Lampung these system are usually implemented on higher education in order to provide validity and reliability of academic data. University of Lampung (Unila) has a long history in development of academic information systems (Siakad), starting with manual systems, semi-online and full online. Siakad Unila already implemented full online, since, 1999, displacement results of scan study-based off line system which had previously been running for two decades, Unila at that time became one of the pioneer using information technology for academic activities in Indonesia.

At an early stages of Siakad development, the core system software uses a proprietary oracle database and oracle forms. On year 2000 was further developed using cold fusion applications and still use oracle database. With the increasing popularity of PHP programming language at 2005 Siakad developers made an improvement and rewrite program used PHP-based applications and still continue to use oracle database. The increasing number of users (especially, students) affected in increased resource demands on server hardware to perform complex computing activities. Limited license of existing database server, made it cannot work optimally to leveraging the capabilities of CPU and memory that has been upgraded. In the year, 2013 developer took decision to rewrite the script application in open source framework Model-view-controller and database migrated from Oracle to open source postgre SQL.

Currently Siakad development has reached the 4th generation and can be accessed at url address https://siakad.unila.ac.id. Siakad was used by entire academic program in Unila such for undergraduate, graduate and diploma. Siakad handle all the academic activities process involving faculty member, students and employees.

Corresponding Author: Gigih Forda Nama, Department of Informatics Engineering, University of Lampung, Lampung, Indonesia

In addition to offering the ease in many ways on academic fields such as entry of students study plan, results of study information, class information and faculty, update class schedules, filling the students biodata, curriculum changes, grading, Siakad also has an aspects of vulnerability due to the nature of this system that always connected and can be accessed online via. public internet. Siakad quite vulnerable for exploitation activities wiretapping/sniffing by those who attempt to steal information such as username and password. In order to reduce the risk of eavesdropping on Siakad data traffic activity, the system already implemented Hypertext Transfer Protocol Secure (HTTPS) protocol to establish a secure connection between user and server that encrypted using verified Secure Sockets Layer (SSL). Problems that often occur to some lecturer accounts who've hijacked by a cracker was because the used of password combinations was very easy to guess (weak passwords), made an impact of abused account like a modification on students grade course without any notice to lecturer in charge.

As the threat landscape evolves, strong user validation method that incorporates Two-Factor Authentication (2FA) becoming an important component of the security framework. Two-factor authentication was not a new concept but it was became popular especially in today mobile age. There were many financial institutions, driven by banking regulations, already deploy 2FA for customer's online transactions (Nagaraju and Parthiban, 2015) Unila was also considers it necessary to implement the technology.

The aim of this research was to implementing authentication module on Siakad system which adopts the concept of 2FA an authentication system that uses two different factors. These factors are something the individual knows such as username and password to access the application.

Something the individual possesses, the token/random code sent by system to the user's mobile phone via. SMS or using One-Time Password (OTP) device where token code generated by the device and only valid for one time transaction.

Typically, 2FA use the knowledge (username/ password) and possession (security token device or mobile phone) factors (Stallings and Brown, 2012). When both of these factors are required for user authentication on Siakad application, the security model will becomes much more complex, will made it more difficult to bypass or hack (Septama *et al*., 2015).

Implementation of OTPA method on Siakad application was expected to minimize the possibility of unauthorized access, especially at the time when lecturers gave grading for final course. Consideration of using SMS-based mobile phone technology was because today almost everyone makes phone as something that should always be within reach by utilizing SMS (text message), all GSM mobiles can be supported without need to add or support additional software on the phone. With mobile phone act as a security token an OTP can be delivered in a safe condition through GSM/CDMA/WCDMA directly when a user attempts to made critical transactions. By requiring a second form of identification, 2FA decreases the probability that an attacker can impersonate a user and gain access to Siakad application, accounts or another sensitive resources. Passwords can be easily lost or stolen, even if a fraudster gains access to a password but they won't have the second element required to authenticate and continue the transaction.

Literature review: In the research on study Mulliner *et al*. (2013) and Cristofaro *et al*. (2014) said that SMS-based OTP was one of the most user friendly multi-factor authentication mechanisms that can be used and doesn't require any additional device, especially on study Mulliner they found there were 89:95% from total respondents use Email/SMS as a second factor. In study, Parameswari and Jose (2011) they developed computer based software token that supposed to replace the hardware token devices in their research it involves generation process of secured OTP using cryptographic algorithm and delivering the OTP code to user's mobile phone through SMS with transaction details and validating the OTP using the same cryptographic algorithm. They proposed a system which secured and consists of 2 parts. The server application, a GSM modem that connected to server directly. The research on study Gholami *et al*. (2007) studied about the important and sufficient conditions for achieving a secure communications using smartcard and also GSM network as a transfer platform while on research on Vapen and Shahmehri (2010) describe the evaluation of an authentication solutions where mobile phones are used as hardware device. The research on study Moore *et al*. (2013), Modrek *et al*. (2014) and Nglazi *et al*. (2013) said that text messaging was an acceptable method of collecting data related to medical research area, SMS further more offers a potentially low cost for rapid delivery information. The research on study (Jasang *et al*., 2015) introduce their product that called off line Personal Authentication Device (Off PAD) act as a trusted device to support the different forms of authentication that are very necessary for trusted interactions between users and system. According to their research, Off PAD prototype has been implemented and already tested and running well in user experiments. The research on study of Bamberger *et al*. (2007) propose a security model

architecture for access control to the communication infrastructure that was also message based. To comply with the requirements of ubiquitous machines communication standard, all algorithms process on the sender's side are implementing symmetric cryptography resulting in low computation needs. The research on study of Zhao *et al*. (2010) elaborates the detail of designing and implementation of agriculture service system which revolutionized the agriculture information can be deliver in to underserved and rural areas they implemented mobile wireless protocols act as a platform that allows mobile phones to acquired and send the data for an agricultural information and links farmer with agronomist for a real time Decision Support System (DSS). The Norwegian company has been developed a system that allow individuals person to use their mobile phones act as OTP generators (Raddum *et al*., 2010), especially considering communication channels on study of Vapen and Shahmehri (2011) introduced intermediary security levels to improve the granularity at which authentication methods can be compared. The research on study of Nama *et al*. (2014, 2015a, b) described the used of several open source application for developing an information system, although using General Public Licensed (GNU) the application can run well and appropriate to solving the problem. Subashini on their research explain the important factor of adaptive security especially cloud environments for securing the high value assets.

MATERIALS AND METHODS

Design and implementation

The architecture design: At this study, we describe the architecture of our 2-factor academic information system for user authentication with OTP code sent by SMS method shown on Fig. 1.

General terminal: A general terminal, placed on faculty member buildings at Lampung University or outside of campus such as PC/tablet/laptop that used by academician (lecturer, graduate school administration, dean, etc.) to access the application.

Cell phone or mobile phone: A general cellphone or mobile phone with specific caller ID, minimal requirement it has SMS functionality, the caller ID should be already register on academic application for receiving the OTP code, only specifies user can register their caller ID that classified to some role such lecturer, graduate school administration for enabling the critical transaction through the academic application.

Servers: The servers was connected to the PC/tablet/smart phone through the Local Area Network (LAN) campus and global internet. Cloud computing and virtualization technology was adopted for server deployment there are private cloud placed on data center that consist of application server, database server and sms-gateway server. Application server will receive any request of academic transaction from PC or other devices and sends a user authentication request if the user succeeds in user authentication process then users can access their menu that appropriate to their role, application server has main function as a WEB server while the data will store to database server through ISCSI connection if it necessary for application server to send the OTP code then it will contact the sms-gateway server on same private cloud and sent the code using sms.

Figure 2 shown the private cloud architecture for application server, database server and sms-gateway server. Blade server M1000e series provide the private

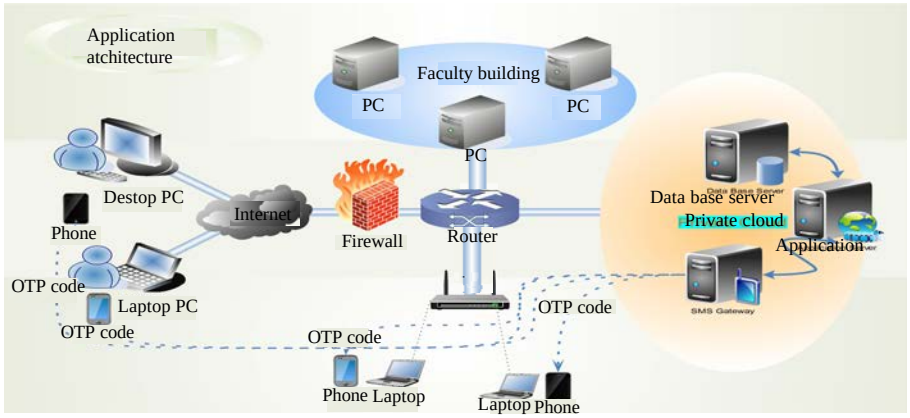

Fig. 1: Application architecture design

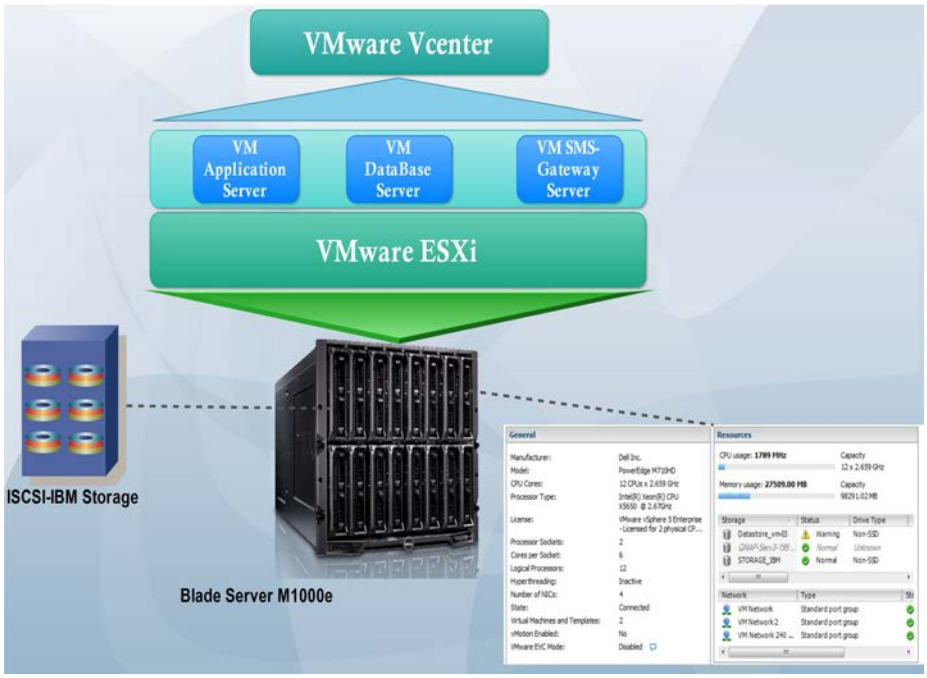

Fig. 2: Private cloud architecture

cloud to all server, IBM storage was used for store all data through I-SCSI connection, all Virtual Machine (VM) manage by a vcenter application. Resource specification of each VM system was:

- CPU Cores: 12 CPUS×2.659 GHz
- Processor type: Intel (R) Xeon (R) CPU
- X5650@2.67 GHz
- Processor sockets: 2
- Cores per socket: 6
- Logical processor: 12
- Number of NIC: 4
- Memory: 98291.02 MByte

The security system design of academic information system: At this stage explained design of the authentication system using Unified Modeling Language (UML) including use case diagrams and activity diagrams.

Figure 3 describe the interaction between actors and system, there are 3 main actors namely Lecturer, Graduate School Administration (GDA) and SMS-gateway system, each actor has use case that was.

Use case: Critical transactions. This use case is used by Lecturer and GDA to conduct critical transactions such as grading of final course by lecturer, semester course timetable and curriculum design by GDA.

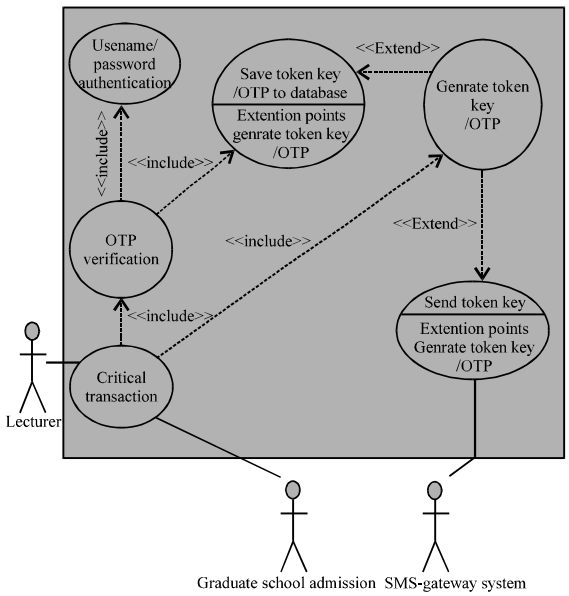

Fig. 3: Use case diagram of Siakad security system

Use case: Username and password authentication, this use case was used by lecturer and GDA to authenticate their self to system.

Use case: Verify OTP this use case was used by lecturer and GDA for token key verification owned by users before made critical transaction.

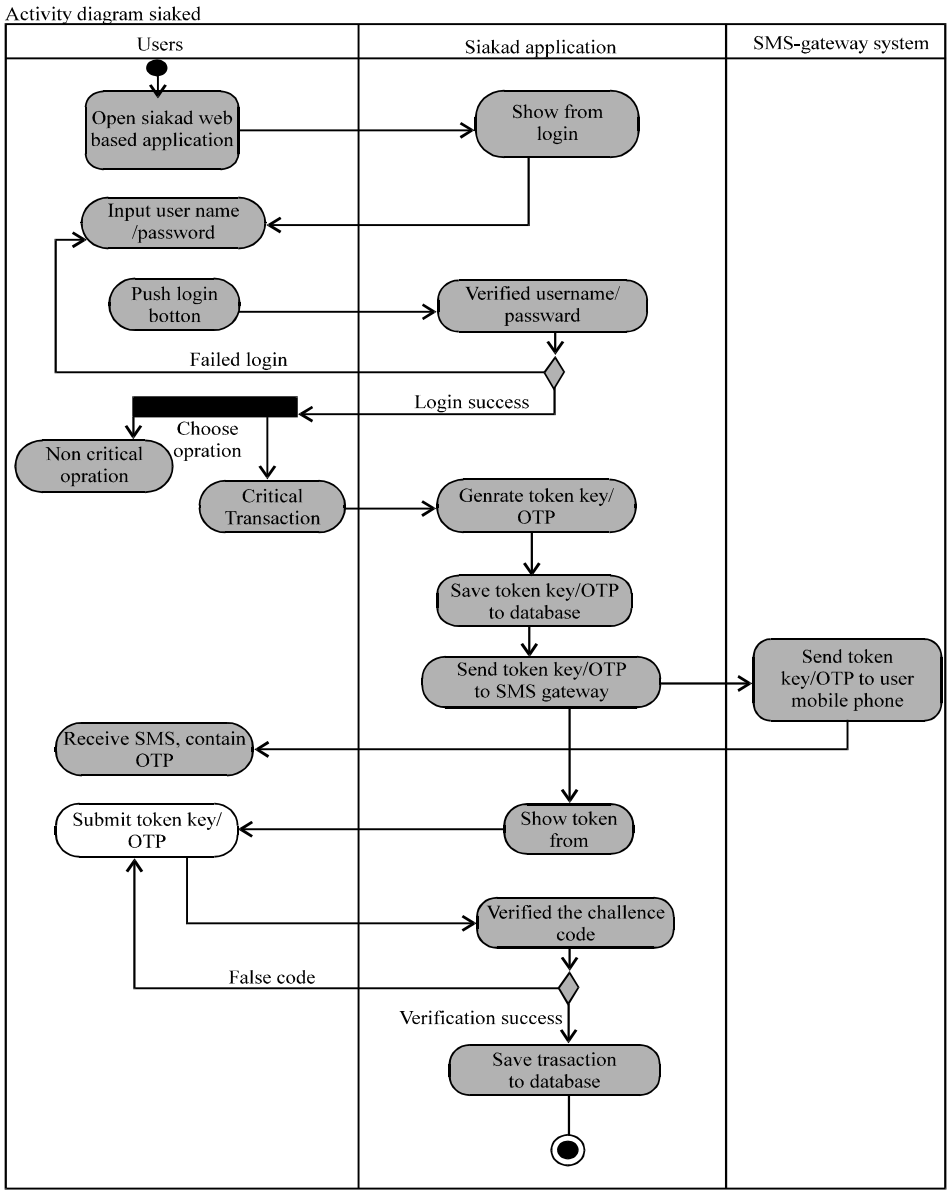

Fig. 4: Activity diagram of Siakad security system

Use case: Generate token key/OTP, this use case was used by SMS-gateway system to get the OTP code and delivered to users mobile phone.

Figure 4 explains activity diagram when users (lecturer and GDA) running the application it will automatically displays authentication page. If authentication success then users will get a menu that appropriate with their privileges when users will perform critical transactions, system will generate a challenge code. OTP challenge code then will be sent to user's mobile phone, furthermore users should submit the challenge code to continued transactions process. Application will verified the token code that entry by users with token code stored in the database if the code was verified the application will record the transaction into the database.

RESULTS AND DISCUSSION

Implementation of authentication system and One Time Password Authentication (OTPA): In this implementation phase there are several modules have been made. Program for password generator that used PBKDF2 algorithm for user login and password verification. Program for OTP

generator and verification. Program for OTP delivery to users mobile phones via. SMS gateway. Program for usage statistic

Password encryption: PBKDF2 algorithm: PBKDF 2 applies a pseudorandom function to derive keys. The length of the derived key was essentially unbounded (Josefsson, 2011). The user password used this encryption within format operation.

Algorithm 1:

PBKDF2 (P, S, c, dkLen)

Options:	PRF	underlying pseudorandom function (hLen denotes the length in octets of the pseudorandom function output)
Input:	P	Password, an octet string
	S	salt, an octet string
	c	iteration count, a positive integer
	dkLen	intended length in octets of the derived key, a positive integer, at most (2^32 - 1)*hLen
Output:	DK	derived key, a dkLen-octet string

One Time Password (OTP) generator and verification: OTP process using a challenge-response procedure, challenge-response was a family of protocols in which one party presents a question ("challenge") and another party should provide a valid answer ("response") to be authenticated, challenge code occurs when user will perform critical transactions such as grading of final course by lecturer, plan of semester course timetable and curriculum design by GDA, token code will sent to users mobile phone via. SMS gateway system, user just submit the appropriate token code if the code match then system will give grant access to user to continue the transaction.

The process carried out at OTP generator can be divided into three phase that is initial process in which all inputs are combined, the computation process in which a hash function was applied several times and the output process where the 53 bit OTP converted into human readable format.

Processes performed at OTP generator

Initial step: Define of secret user's passphrase.

Computation step: OTP is produced by implementing random algorithm library of Python language program, the library implements pseudo-random number generators depend on the basic function random () which generates a random float uniformly in the semi-open range (0.0, 1.0). Python uses the mersenne twister as the core generator.

Output step: OTP that generated from step no 2 with 53-bit precision float format will be converted into integer format with 6 characters length and also stored on to database that shall be used for user's challenge-response authentication.

OTP verification on server: In the verification process, will be checked whether the OTP inserted by users is same with OTP stored in the database or not. Every time a user has successfully logged into the system, users name, date and time will be recorded to find out who logged into the system. Administrators perform user registration and determine userID and password. When user want to perform critical transactions through web application then the system will ask for OTP code before transaction can proceed, the code given by user will be compared with OTP code that stored in the database. If the code same than user can proceed the transaction.

Figure 5 shown a screen view of Siakad application when GDA want to create course schedule before they can continue transaction they should put in the OTP code/token on the form that provide on web application, previously the OTP code was sent on their mobile phone through sms gateway.

OTP code delivery to user's mobile phones via. SMS Gateway: SMS-gateway system was used to deliver the OTP code, we deploy the system using open source technology, the main sms engine carried out by Gammu Daemon. This system accept OTP code that was sent by Siakad system and deliver to the users mobile phone via sms, we use single USB modem with TELKOMSEL cellular number installed on this modem.

Figure 6 shown a screen view of token code that received by user's mobile phone, sms gateway system takes time duration around 20 sec to send this code to user's mobile phone, the code sent with 6 characters in numerical format this numerical format was choose to make users easily identified each number. Beside contain

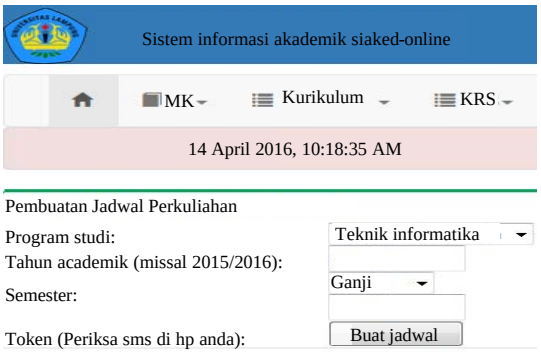

Fig. 5: Input form for OTP code

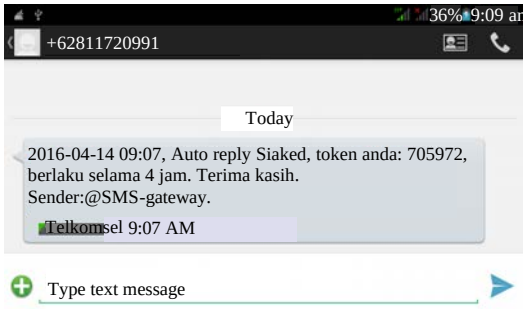

Fig. 6: SMS of token code received by user's mobile phone

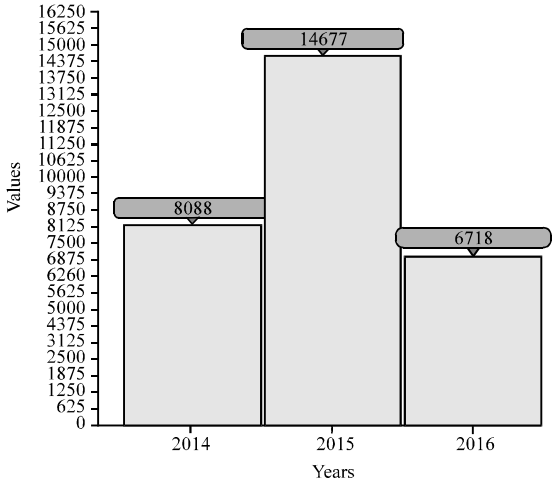

Fig. 7: Annually report of OTP code that sent by SMS-Gateway system

the OTP code, the sms message was also consist of time stamp when the code delivered by sms-gateway and also the expiration time of token usage.

Program OTP usage statistic: Data retrieval of sms-gateway usage statistic conducted, since, 2FA system was implemented on April 2014 until April 2016, during the period there were total 29483 time the sms-gateway sent OTP code to user's mobile phone with details are as follow.

Figure 7 shown the annual report of token code delivered by sms-gateway system, since, the implementation of 2FA in 2014 there were total 29483 OTP code sent to user's mobile phone with details in 2014 total 8088 token sent in 2015 increased significantly with total 14677 token sent and until April 2016 total there are 6718 token sent.

Figure 8 shown monthly report of toke code sent by sms-gateway system from the picture shown that the large amount of OTP code sent occurred on July and January each year on January 2016 there were total 4481 OTP code sent, on July 2015 there were 3300 code sent. January was the end of even semester and on July was the end of odd semester, during this month the critical transaction that needed token code verification will held.

Table 1: Statistic of OTP code delivery time

Parameters	Values (sec)
Mean	22.87
Standard error	0.69
Median	19.00
Mode	32.00
Standard deviation	114.35
Sample variance	13077.99
Kurtosis	2762.74
Skewness	46.99
Range	8038.00
Minimum	2.00
Maximum	8040.00
Sum	619929.00
Count	29483.00

Figure 9 shown daily report statistic of token code delivery by sms-gateway in January 2016, the most busiest day occurred on January 29 2016 with total 478 OTP code sent to user's mobile phone through sms, usually the academic activities of odd semester ends in January, during this period the lecturer busy in filling of course subject grading that impact of the large amount of OTP code sent to their mobile phone. On February the number of OTP code sent by system decreased.

Figure 10 shown classification and amount of cellular provider used by users, the most popular cellular provider used by user was TELKOMSEL with total 819 number, INDOSAT with 197 number used, XL with 35 number and TRI with total 16 number. Figure 11 shown the percentage of cellular provider used by users, TELKOMSEL was dominated with total amount 77% users.

Table 1 shown descriptive statistics of OTP code delivery time from the table can concluded that mean time the OTP code delivery was 22.87 sec this mean time value was still within the threshold of tolerance accepted by user that indicated the sms-gateway system research as well. The maximum time was 8040 sec or 134 h this value appears due to differences in cellular provider used by sms-gateway server and users. We cannot predict the main problem why it take, so, many time to deliver the OTP code because we have no access to provider data.

Security analysis: Our proposed scenario can refuse any off-line guessing attack to application because this system has strong authentication feature consist of two factor authentication (security that users know and possess) to prevent the OTP generator sent the same

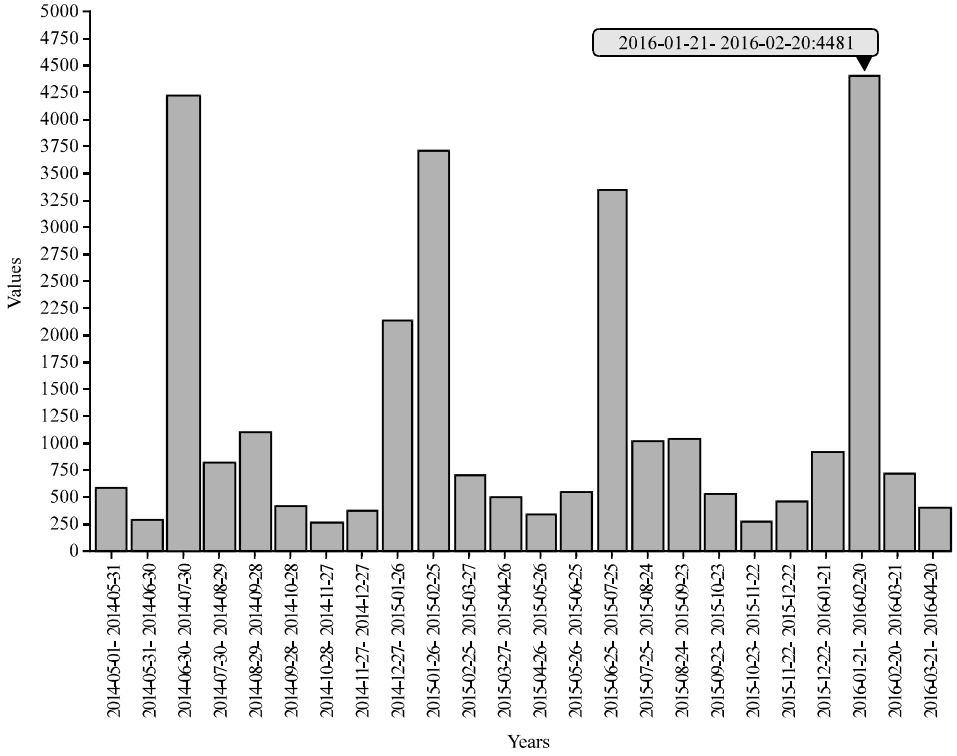

Fig. 8: Monthly report of SMS-gateway system

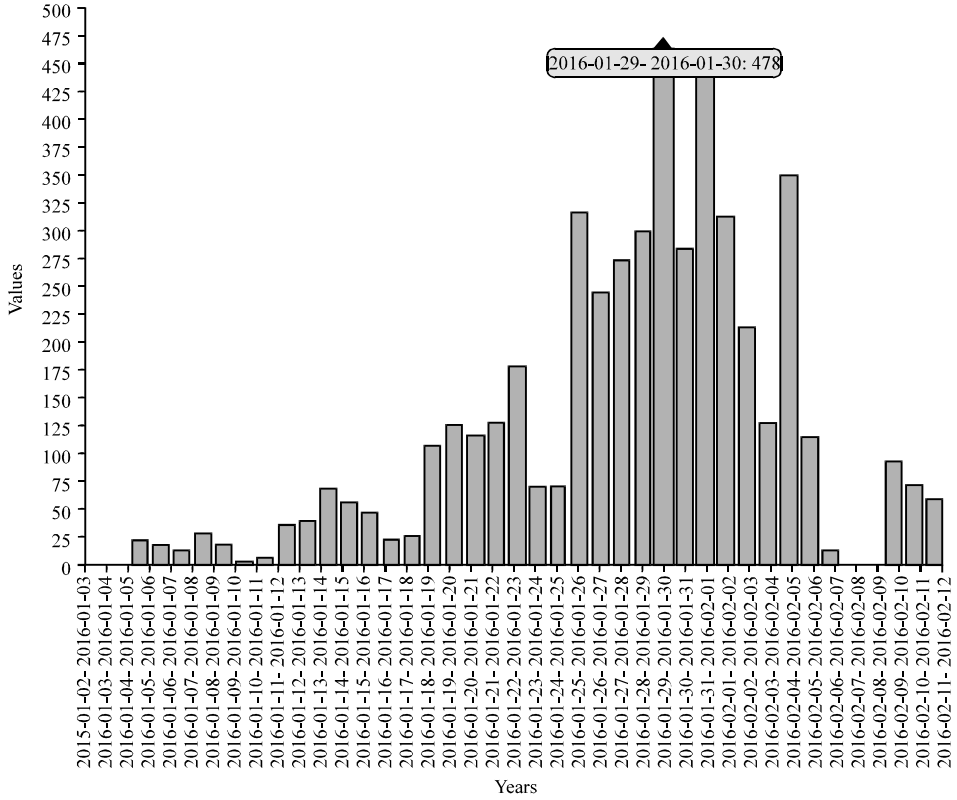

Fig. 9: Daily report of SMS-gateway system

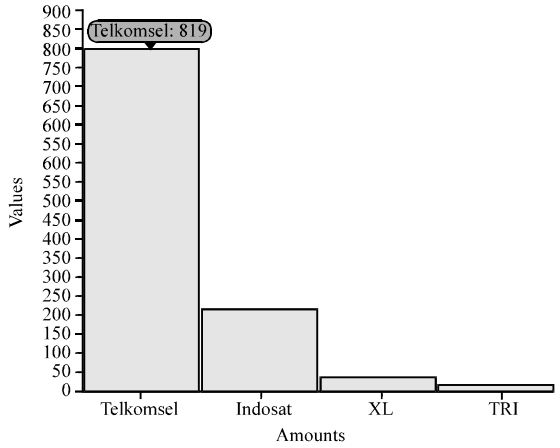

Fig. 10: Classification and amount of cellular provider used by the users

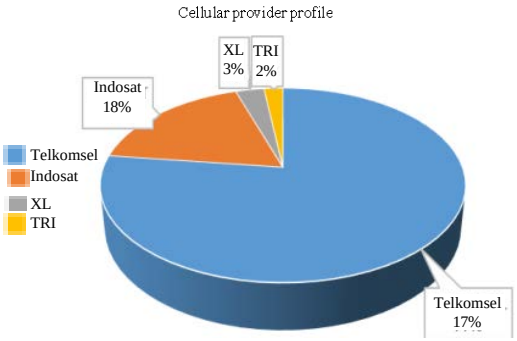

Fig. 11: Percentage of cellular provider usage

code for users we implementing the pseudo-random code algorithm before sending the token code to reduce the cost of sms payment we also implementing an algorithm to keep the token code valid until 4 h.

Design goals review: We implemented the sms technology that is easy and friendly to all users, all types of mobile phone should be able to use this technology, all mobile phone with sms feature activated will be able to accept the token code. On the server side by simply adding a GSM modem then the token code directly can be sent. Cloud computing technology that was implemented in the academic system can help simplify the management in running and monitoring the applications.

Challenge attack: An attacks based on man in the middle attack by intruders who impersonate the communication from host to server will be prevented by implementing HTTPS technology. For web application, the security level will be as strong as how the users choosing the good combination of User ID and password. For some case especially for weak password, the intruders can be success get in to academic system used the stolen account but they have to guess of the 6-digit OTP code that sent to user's phone.

When users caller-ID change: A regular OTP token sent to registered caller-ID that appropriate with specified user record on database. If there any issue of caller-ID change on user's phone than the user should report to administrator and make a request for updating the phone number on database for change the old number to the new one.

Cellular phone is lost, stolen or confidential file is secretly copied: The cellular phone is small and often times to get lost, stolen or its confidential files secretly copied. If the phone be stolen by malicious person hand, they should to crack or guessing the user's credential first before activating OTP function.

When sms-gateway credit balance running out: The sms-gateway server installed with GSM modem on it for almost 3 years (since, 2013-2015) we used pre-paid number attached on modem at the earlier time when we use this pre-paid service there were a problem when the credit balance running out and impact to OTP code could not be sent to user, the problem solved with an application module that check the credit balance periodically and will report to administrator when the credit-balance was below the minimum threshold determined by system. Nowadays, since, 2015 we change the GSM-number with post-paid service, so, the system wouldn't worry about the credit balance we paid at the end of the month for all sms transaction.

Academic system performance analysis: Figure 12 shown the performance statistic of Virtual Machine (VM) academic system application from the graph shown that on January or August there were increase number of resource hardware consumption, maximum number of network usage was 1244 Kbps, maximum CPU usage was 25.45% while maximum memory usage was 33.80 GByte. This was happen because on January was the end of even semester and August was the end of odd semester, during this month there were many users access the academic application.

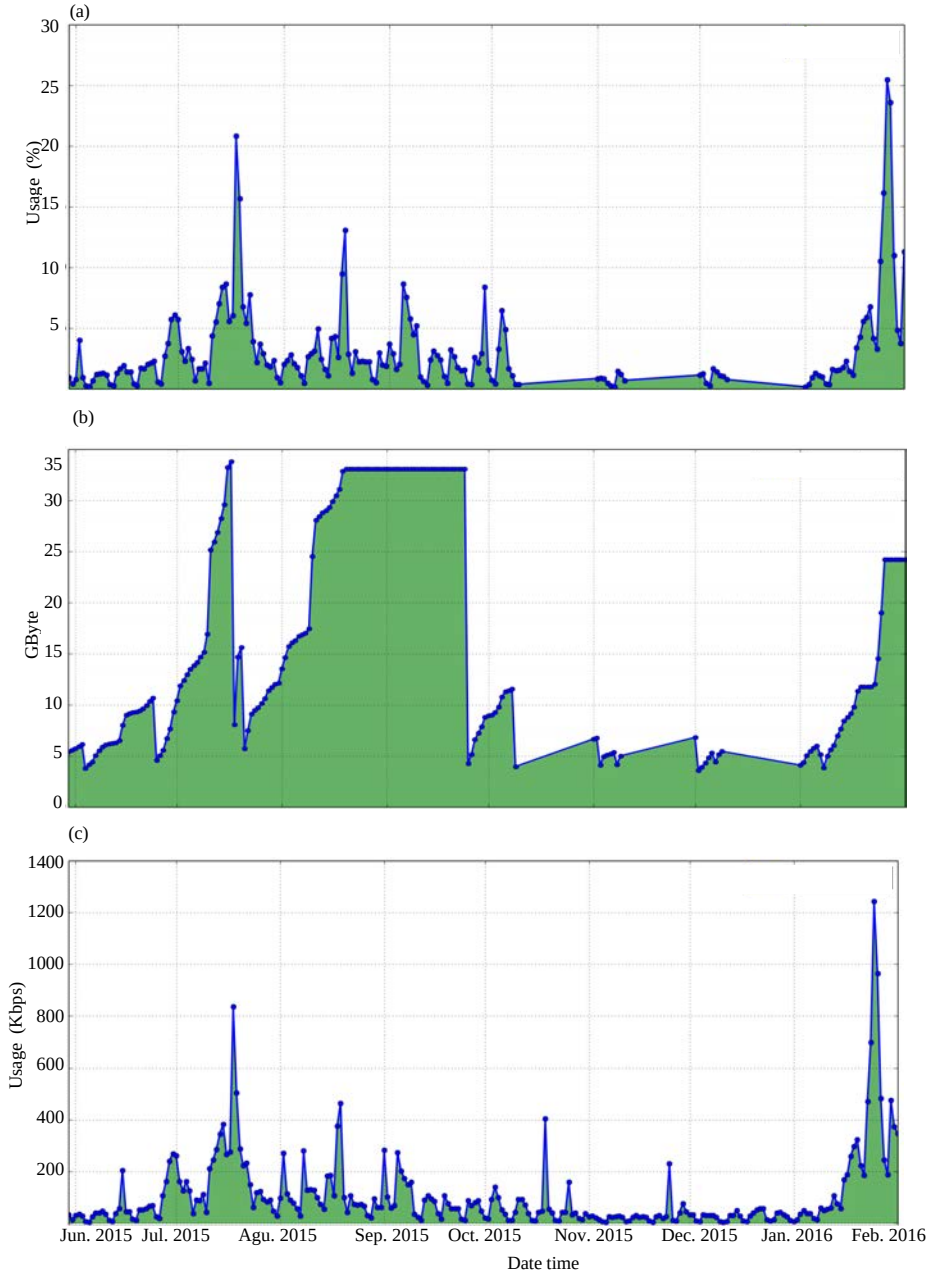

Fig. 12: a) CPU Usage; b) Memory usage and c) Network usage

CONCLUSION

In this study, Two-Factor Authentication (2FA) system already deploy and integrated with Siakad application and running well since, 2013 it used the account knowledge (username/password) and also account possession (security token on users mobile phone) factors. Both of these factors are implemented for user authentication it proven that the security becomes better more complex and made it more difficult to bypass or hack (looks from 2 years implementation there were no critical issue especially in modification of student's grade).

Data retrieval of sms-gateway usage statistic conducted, since, 2FA system was implemented on April 2014 until April 2016 from the report shown there were total 29483 time OTP code sent to user's mobile phone, especially on January or August on each year, usually there will be an increase number of OTP code sent by server because on January was the end of even semester and on August was the end of odd semester.

The most popular cellular provider used by user was TELKOMSEL with total 819 number, INDOSAT with 197 number used, XL with 35 number and TRI with total 16 number with this various number of cellular number usage, we analyzed that mean time the OTP code delivery was 22.87 sec, this mean time value was still within the threshold of tolerance accepted by user that indicated the SMS-gateway system was research well.

ACKNOWLEDGEMENTS

This research was fully supported by University of Lampung grant. The authors fully acknowledged Ministry of Higher Education and University of Lampung for the approved fund which made this important research viable and effective.

REFERENCES

Bamberger, W., O. Welter and S. Spitz, 2007. Mobile phones as secure gateways for message-based ubiquitous communication. Proceedings of the 1st International Workshop on Information Security Theory and Practices, May 9-11, 2007, Springer, Heraklion, Greece, pp: 175-188.

Cristofaro, E.D., H. Du, J. Freudiger and G. Norcie, 2014. A comparative usability study of two-factor authentication. Proceedings of the 2014 International Workshop on National Diabetes Surveillance System (NDSS'14), February 23, 2014, Catamaran Resort Hotel and Spa, San Diego, California, USA., ISBN: 1-891562-37-1, pp: 1-10.

Gholami, M., S.M. Hashemi and M. Teshnelab, 2007. A Framework for Secure Message Transmission Using SMS-Based VPN. In: Research and Practical Issues of Enterprise Information Systems II, Xu, L.D., A.M. Tjoa and S.S. Chaudhry (Eds.). Springer, Boston, Massachusetts, ISBN:978-1-4757-0563-8, pp: 503-511.

Josang, A., C. Rosenberger, L. Miralabe, H. Klevjer and K.A. Varmedal *et al*., 2015. Local user-centric identity management. J. Trust Manage., Vol. 2,

Josefsson, S., 2011. Password-Based Key Derivation Function 2 (PBKDF2) test vectors. Internet Eng. Task Force, 1: 1-5.

Modrek, S., E. Schatzkin, A. De La Cruz, C. Isiguzo and E. Nwokolo *et al*., 2014. SMS messages increase adherence to rapid diagnostic test results among Malaria patients: Results from a pilot study in Nigeria. Malar. J., Vol. 13,

Moore, S.C., K. Crompton, S. Goozen, M. Bree and J. Bunney *et al*., 2013. A feasibility study of short message service text messaging as a surveillance tool for alcohol consumption and vehicle for interventions in university students. BMC. Public Health, Vol. 13,

Mulliner, C., R. Borgaonkar, P. Stewin and J.P. Seifert, 2013. SMS-Based One-Time Passwords: Attacks and Defense. In: Detection of Intrusions and Malware and Vulnerability Assessment, Rieck, K., P. Stewin and J.P. Seifert (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-39234-4, pp: 150-159.

Nagaraju, S. and L. Parthiban, 2015. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. J. Cloud Comput., Vol. 4,

Nama, G.F., M. Komarudin and H.D. Septama, 2015a. Performance analysis of Aruba™ wireless local area network Lampung University. Proceedings of the International Conference on Science in Information Technology (ICSITech), October 27-28, 2015, IEEE, Yogyakarta, Indonesia, ISBN:978-1-4799-8384-1, pp: 41-46.

Nama, G.F., M. Komarudin, P.H. Mardiana and H.D. Septama, 2014. Electricity, temperature and network utilization monitoring at Lampung University data centre using low cost low power single board mini computer. Proceedings of the Regional Conference on Computer Information Engineering, October 7-8, 2014, Eastparc Hotel, Yogyakarta, Indonesia, pp: 184-189.

Nama, G.F., M. Ulvan, A. Ulvan and A.M. Hanafi, 2015b. Design and implementation web based geographic information system for public services in Bandar Lampung City: Indonesia. Proceedings of the International Conference on Science in Information Technology (ICSITech), October 27-28, 2015, IEEE, Yogyakarta, Indonesia, ISBN:978-1-4799-8384-1, pp: 270-275.

Nglazi, M.D., L.G. Bekker, R. Wood, G.D. Hussey and C.S. Wiysonge, 2013. Mobile phone text messaging for promoting adherence to anti-tuberculosis treatment: A systematic review protocol. Syst. Rev., Vol. 2,

Parameswari, D. and L. Jose, 2011. SET with SMS OTP using two factor authentication. J. Comput. Appl., 4: 109-112.

Raddum, H., L.H. Nestas and K.J. Hole, 2010. Security analysis of mobile phones used as OTP generators. Proceedings of the 4th International Workshop on Information Security Theory and Practices (WISTP'10), April 12-14, 2010, Springer, Passau, Germany, pp: 324-331.

Septama, H.D., A. Ulvan, G.F. Nama, M. Ulvan and R. Bestak, 2015. Dynamic tunnel switching using network functions visualization for HA system failover. Proceedings of the 2015 International Conference on Science in Information Technology (ICSITech'15), October 27-28, 2015, IEEE, Yogyakarta, Indonesia, ISBN:978-1-4799-8384-1, pp: 259-263.

Stallings, W. and L. Brown, 2012. Computer Security: Principles and Practice. 2nd Edn., Pearson Education, Upper Saddle River, New Jersey, ISBN:9780133072631, Pages: 816.

Vapen, A. and N. Shahmehri, 2010. Security levels for web authentication using mobile phones. Proceedings of the 2010 Prime Life International Summer School on Privacy and Identity Management for Life, August 2-6, 2010, Springer, Helsingborg, Sweden, pp: 130-143.

Zhao, J., W. Li, Y. Yang, H. Meng and W. Huang, 2010. Design and Realization of Information Service System of Agricultural Expert Based on Wireless Mobile Communication Technology. In: Computer and Computing Technologies in Agriculture, Li, D., Y. Liu and Y. Chen (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-18353-9, pp: 598-603.