International Journal of Grid and Distributed Computing
Vol. 10, No. 11 (2017), pp.43-56
http://dx.doi.org/10.14257/ijgdc.2017.10.11.05

An Improved OTP Grid Authentication Scheme Email-based using Middle-square for Disaster Management System

B. B. Jr. Balilo[1], B. D. Gerardo[2], R. P. Medina[1] and Y. Byun[3]

[1]*Technological Institute of the Philippines, Quezon City, Philippines*
[2]*Institute of ICT, West Visayas State University, Lapaz Iloilo City, Philippines*
[3]*Dept. of Computer Engineering, Jeju National University, Jeju, Korea*
benedicto.balilojr@gmail.com, bgerardo@wvsu.edu.ph,
ruji_p_medina@yahoo.com and ycb@jejunu.ac.kr (Corresponding Author)

Abstract

Disaster is an attempt to control or access the system without legal/valid permission and proper authorization protocol from legitimate entity. Nowadays, most organizations managed to save records in an online database transmitted over unpredictable network. To gain access to the system it is better if proper authentication be placed because it may affect the organization operation and sensitive information may be at risk (like early warning notification, casualty monitoring, initial and post assessment, rescue operation, response recovery, etc) if system has been compromised. This paper introduced a new scheme of one time password (OTP) email-based authentication and improved the authentication scheme using middle square technique to protect and secure confidential information for disaster management system. The One-Time Password has been recognized by many organizations as a breakthrough to two-factor authentication technique. It solves the shortcomings of the traditional username/password authentication. The OTP generates the initial seed based from the combination of several parameters like string of characters, numbers, date, time and weather data (humidity and temperature). The values generated changes overtime upon login registration as it extract location weather data producing an approximately 91 possible values or 4,095 possible combinations. The application has primary components namely: about, signup and login. It authenticates the user up to three (3) login attempts only then follows the redirection process. This scheme improved the security, protection and confidence level of the user as it uses a randomized generation of OTP codes sent through secured email account that is free from brute force, dictionary attack, insider attack, and key-logger attacks.

Keywords*: One Time Password, Two-Factor Authentication (2FA), Disaster Management System, Email Protection*

1. Introduction

Disasters can be minimized by instituting policies and appropriate management of information and resources. A sound disaster risk management strategy for managing disasters ensures that loss of life and property is reduced in a disaster event [1]. Information Technology has been part of the daily transaction routine. It may affect the operation of the company or an organization responding to disaster. In fact, technology hold risk to the organization if not properly secured and protected. There are available techniques which can be used in disaster risk management in order to develop and apply

Received (July 10, 2017), Review Result (October 30, 2017), Accepted (November 6, 2017)

ISSN: 2005-4262 IJGDC

disaster management tools. These tools include access model, computer assisted techniques, cost-benefit analysis, disaster risk indexing, environmental impact assessment (EIA), geographic information system (GIS) mapping, hazard mapping, historiacal analysis, risk mapping, movable and deployable ICT resource unit (MRDU), resilient communication system [2].

These technology attempts to support and control part of the process which may result to disaster. The term "disaster" is an event that creates an inability to maintain the flow of data necessary for critical operations over a prolonged period of time. This might mean that data got lost and is completely unavailable, or that it is temporarily irretrievable-preventing its access or update [3]. According to Semer [4], possible IT disasters will include: natural disasters (such as fires, earthquakes, lightning, storms, and static electricity), software malfunctions, hardware or system malfunctions, power outages, computer viruses, man-made threats (such as vandalism, hackers, and sabotage) and human error (such as improper computer shutdown, spilling liquids on the computer, and cigarette ash). Even if we know what types of disasters are possible, there is seldom way to anticipate which type will happen. Therefore, the solution is to prepare all the time for all types. Nowadays, data security has become an issue because most organizations stored their records in the database transmitted over the network. It is better if the user gaining access to the system be provided with better authentication to facilitate verification that said user really the owner of the account, hence, one way of improving the authentication process is the introduction of OTP scheme.

One-Time Password (OTP) is a generated string of characters and numbers that is used for authentication and valid only for a single transaction or session. In 1979, [6] introduced the concept of OTP to provide effective protection for distributed client/server interaction. In the scheme, the initial seed was used to generated the passkey values which will be formed part of the succeeding seeding process. Many researches have work on different OTP schemes and mechanisms like random number generation, time-based and attribute-based scheme. Others have work on the combination of some parameters to generate OTP values, but, each existing work has its own unique features designed for specific problems. The OTP has been recognized in authentication technique for it increase the level of security and added features in protecting and securing confidential and sensitive information. The time period of the password's life span is 180 seconds, the time to break the OTP password in ratio is 166 = 16,777,216 possibilities in a single input of passwords [7].

The trend in OTP authentication is growing and will continue to take the advantage of technology trend to guarantee safety and protection on information or data. Every authentication technique has different trade-offs which makes the user dependent on the network infrastructure and authentication protocol established by the service provider. The phone service provider is responsible for delivering the message, but does not guarantee its communication channel. Monitoring GSM network, international roaming, SMS costs, malicious phone applications to obtain mobile transaction authentication number and delays are some factors that put restriction on reliability. Some manifested restrictions in hardware resources of mobile phone are low transition rate, low bandwidth of communication channel, limited calculations capabilities of processor, battery and memory. The OTP SMS-based has considerations in cost, communication signal, and capacity of service provider to guarantee message integrity.

It is in this context that new mechanism shall be introduced to strengthen the application of OTP in email-based authentication for disaster related activities. There is still an opportunity to recognize challenges to expose the capabilities of email as reference medium for receiving OTP and transaction verification code [5]. By adding more parameters and algorithmic scheme to generate OTP, the information will be safe and protected. Thus, the use of random number generation (RNG) and attribute

combination on 8x8 grid lookup system to produce complex OTP values is a defense against replay attack, password guessing, dictionary and brute force attack.

The goal of this research is to develop a one-time password email-based authentication scheme and incorporate new random number generated (RNG) into 8x8 grid schedule. This paper sought to propose for a mechanism that would enhance the traditional authentication by introducing a novel and secure security mechanism using a two-factor authentication through alphanumeric random generated email-based token. The objectives of this study are: to enhance two-factor authentication in OTP using a 8x8 matrix sequence pattern, develop a new scheme by extracting characters based on random coordinates generated by the algorithm and simulate the proposed authentication method through disaster management system. This shall demonstrates generation of passkey from initial seed of random numbers and mapping out in table pattern schedule which will produce a new form of OTP scheme in protecting disaster related activities.

2. Related Studies

Leslie Lamport scheme offers the advantage of, free from impersonation and password will not be reused. The values are stored in client side using the mathematical scheme s=seed, s1=h(s), s2=h(s1), s3=h(s2),….s(n)=h(s(n-1)), where h is a one-way function with s in an incremental value. The core of Lamport's scheme requires that client cooperates and agrees to use a common sequencing algorithm to generate a set of expiring OTP (client side), and validate client-provided passkeys included in each client-initiated request (service side) [6]. Currently, there are various innovations on one-time password researches including those with latest technologies and combination of the different methods—like random number generation [8][20], time based [10][11][12] , monitor [20], keyboard and mouse manipulation [9], location, and IP address. Each method can be applied in both mobile phones using SMS gateway [15][16] and email system.

Other researches include, the use of hash function MD5 together with the username, SPP and random number generation or timestamp [13]. The scheme can withstand decimal attack and re-play attack. However, the weakness of MD5 and SHA-1 algorithm was found to produce collisions with only 242 hashes can be solved by PingPong128 stream cipher. PingPong-128 cipher is a specific cipher from the PingPong family of stream ciphers [14], QR Codes [17][18], and dropped call [19].

3. Methods

The study used two (2) approaches in generating OTP (randomization parameters and extraction) and a new concept of mapping out the numbers in 4x4 matrix schedules. The existing OTP bingo grid schemes deals with combination of several seed attributes which include numbers and characters. The study used the combination and maximization of alphanumeric to produce two (2) pair codes.

The study used Rational Unified Process (RUP) methodology as guide in the development of the proposed study. The Rational Unified Process (RUP) is focused on high-quality software that meets the needs of its end users within a predictable schedule and budget. The researchers believed that with the use of the set of building blocks and content elements including those to be produced and the necessary skills required giving its step-by-step explanation of specific development goals, RUP will position the development process to identify its milestone, artifacts and cut-off what the unnecessary results. The RUP deals with a lifecycle that ends with a milestone. Each cycle in the RUP methodology is broken down into a sequence of four phases, called Inception, Elaboration, Construction, and Transition. Since it provides a specific plan for each step of the development process, it helped prevent resources from being wasted and reduces

unexpected development costs which are fundamental to the development process of the study.

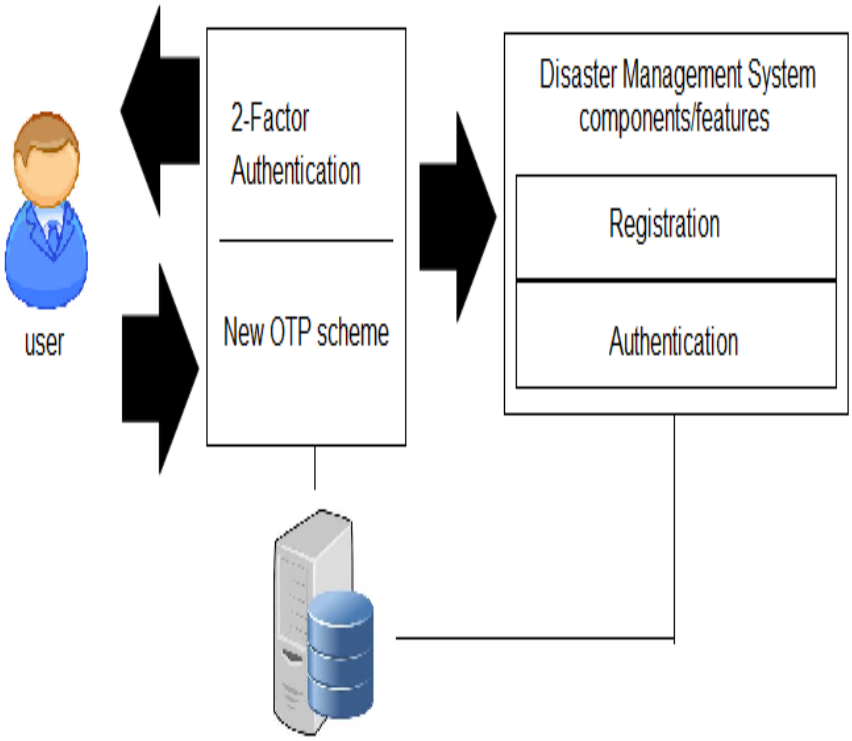


Figure 1. Design Concept of the Proposed Study

In inception phase, the current OTP authentication scheme were analyzed leading to a clear understanding of the objectives and scope of the project study. In Elaboration phase, the goal of this phase is to define and specify the baseline of architecture of the system in order to provide a stable basis for the bulk of the design and implementation effort in the construction phase. The detailed design concept was dissected to give a clear understanding of each requirement in the subsequent development planning. Also, the prototype of the architecture will be implemented and tested to support the use case of the system. The construction phase consists of "design and build" series concept. The production process will give emphasis on developing and constructing the details of the system. The free and open source cross-platform web server solution XAMPP, PHP scripting language and front-end framework called Bootstrap will be used for programming and application development, coding, unit integration and system testing. The weather API will be formed part of the registration phase as discussed in the design concept of the proposed system. This is where the final design and working system are ready for deployment occurred. The milestone of this phase includes the web interface modules which include registration module, authentication module and features of the proposed system and lastly, the transition phase includes the evaluation and feedback of the working system.

The proposed system was simulated using the extracted typhoon data from the Internet and MDRRM records. Following the Rational Unified Process we simulated and analyzed the operation and performance of the developed system. The system was tested in Intel Corei5-4460 processor based running at 3.210GHz with 2GB of RAM.

4. Components of the Proposed Study

4.1. Generation of One Time Password (OTP)

The algorithm used the concept of random number generation, attribute-based and string manipulation technique. Enhancing the Lamport scheme, the study adopted the formula in generating the two (2) pair codes. Let the initial seed represented by letter g to be the string of characters + numbers + date + timestamp + weather data. Using the formula below, the initial seed captures the current OTP and integrated as part of the next OTP to be generated. The letter b represents the OTP to be generated.

$$b=g,\ b1=(b(g+otp1),\ b2=(b1(g+otp2))..\ bn+1=(bn+1(g+otpn)) \quad (1)$$

This method will be free from brute force and dictionary attack as the applied algorithmic pattern used the combination of randomized code with generated OTP. Below is the code applied using PHP scripting language.

ALGORITHM:

```
set default = "A..Z","a..z","0..9"
param = date("MmDdY").time().weatherdata
do
{
   Increment flag;
   if (flag>7)
            {  flag=0;
      increment cn; }
}
otp1 = implode$result[row_element][0])
otp2 = implode(result[0][col_element])
print final OTP
```

The user is requested for authentication by supplying the username and password as the first level of authentication. The username and password will be searched from the database. If they match, the server retrieves the PassCode and relogin for failed attempts. The system has provided automatic blocker, after three (3) failed attempts the user account will be locked and will allow the administrator for a challenge/answer for unlocking.

After the first level of authentication, the PassCode together with alphanumeric combinations, a pair of code will be generated. The XY coordinate will be randomly chosen together with the assigned pair of codes. These will be mapped out into randomly generated 8x8 sequence schedule as shown in Figure 2.

ae	pI	l2	su	bt	gW	08	BM
aP	D4	fT	zW	DZ	aU	uN	yE
nz	mr	mY	P8	wC	iW	tS	sA
Z6	p9	v2	W3	iF	rY	W4	04
yO	W7	E6	nB	dw	tK	LN	bs
d2	ag	nM	gI	fn	ft	k2	DO
fU	L7	oD	yL	GW	G1	SZ	wB
d9	A7	M8	u0	bH	vN	yz	AR

Figure 2. Sample Generated 8x8 Table Pattern Schedule

It is important to avoid producing the 1:1 XY coordinate in the table as it will only duplicate the values producing similar codes. In Table 1, in order to avoid such result, the row and column element was processed randomly and checked whether the zero value was produced, if the values generated matched the zero value then randomization process shall be initiated.

Table 1. Sample XY-Duplication Prevention Statements

Line	Statement
1	$row_element = rand(0,7);
2	$col_element = rand(0,7);
3	if ($row_element==0)
4	{
5	$row_element = rand(0,7);
6	}
7	if ($col_element==0)
8	{
9	$col_element = rand(0,7);
10	}

4.2. Disaster Management System Interface

Figure 3 shows the sample web application providing security to administrator upon login into the system. An Administrator or webAdmin is an individual or person who is responsible for the control, supervision and management of an application system.

Figure 3. Sample GUI of Disaster Management System

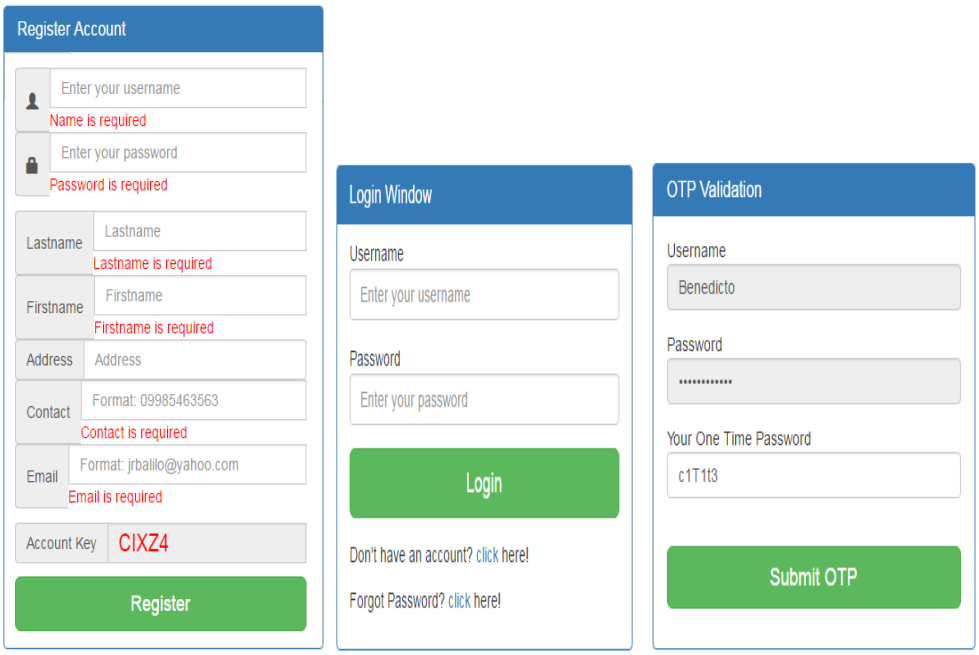
The webAdmin applied unique security mechanism to preserve the confidentiality, integrity and availability of information. Any compromised threat or attack to the system is critical to the entire operation of the system including the information and its clientele. The primary component of the interface consists of about, signup and login.

About. This refers to the overall description of the study, anything that the user wanted to know about the study can be found here.

SignUp. also known as Register. This module allows the user to own an account

Login. A process where user gain access to the system through verification and authentication process. The login consists of username, password and OTP code to ensure that the one requesting access is legitimate user.

The simple application of username and password require each user to provide the system with necessary information for authentication purpose. First the user need to supply the correct username and password, the server with mutual agreement with the database shall look into the records if said user is in the list with privilege access to the system, if matched the server generates the OTP then send the generated XY coordinates together with the matrix table.



(b) (c)

Figure 4. (a) Sample Registration, (b) Login and (c) OTP Window

The privileged access shall be granted to limited user only. The minimal access control and least privilege to the system will bring slice to security level allowing access only to information and resources that are necessary for legitimate purpose. The principle of least privilege is important in enhancing the protection of data and functionality from faults and malicious behavior. Among the benefits of this principle includes better system stability, better system security, and ease of deployment [19].

4.3. Email Notification

In Figure 5, shows the reference code and the OTP sent to user registered email address. The purpose of sending the randomly generated XY coordinates is to free the user from brute force attack and do physical matching of the XY coordinates then input the full detail codes into the OTP input box for server authentication. Once authenticated, the system displays the main system page and user can now manipulate the features of the system.

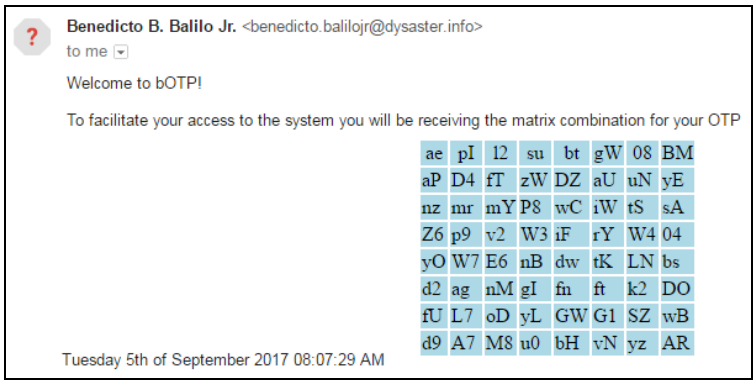


Figure 5. Sample OTP Email Notification

5. Results

5.1. Proposed OTP Grid Authentication Scheme using Middle-square

The combinations of characters were initialized in an array together with the parameters to form the initial seed of the code. A two-dimensional was set for XY values, each of which had parameters but produced different randomized codes. The weight of the algorithm put emphasis on the generation of two separate randomized codes stored in array as temporary storage and random selection of XY coordinates from the mapped table schedule avoiding the 0,0 values. The mapping of values returns the row and column element.

The created 8x8 rule schedule will be sent to the registered user's email address. The user needs to complete the challenge process given by the xy pattern like nz and BM that intersect the code sA. These patterns of code will be grouped to form the initial seed (*i.e.* nzBMsA), and the center four (4) characters will be extracted as the final OTP codes.

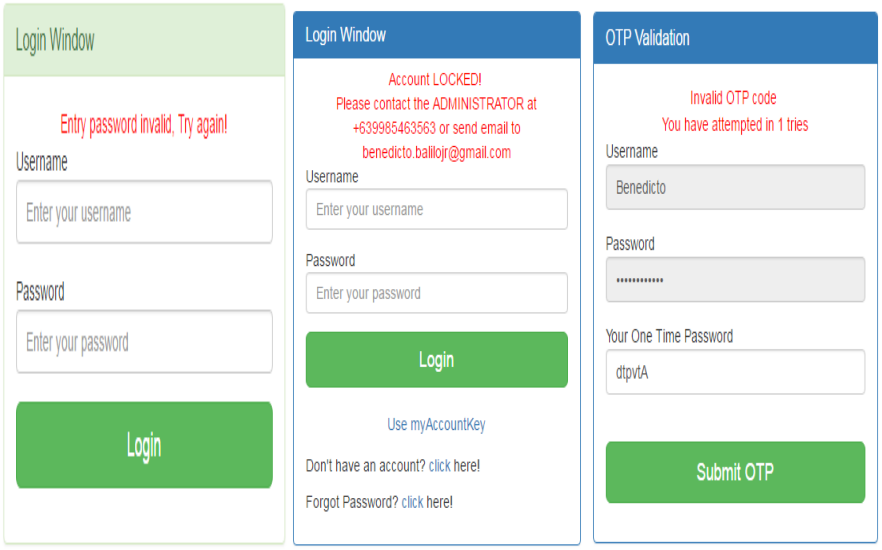
Figure 6. Sample Result of OTP using Middle Square Technique

The result shows that the XY-axis coordinate 1:1 was never selected throughout the entire simulation of the algorithm. This was the consideration in the inception phase of the study as this will produce a redundant two-pair value which may be a possible hint for guess attack and an easy to obtain brute force attack. With the in-placed statements in the algorithm, XY-axis 1:1 will be bypassed from the selection. The deployment of this segment allows the generation of OTP values to be reliable, free from some form of attacks (like guess attack, dictionary and brute force attack) which is one of the primary goals of this study.

5.2. Application of OTP to Disaster Management System

The user applies unique security mechanism to preserve the confidentiality, integrity and availability of information. Any compromised threat or attack to the system is critical to the entire operation of the system including the information and its clientele. Each user shall be provided with a unique AccountKey generated by the system. The AccountKey shall be part of the validation process which allows the user to be secured in requesting reauthentication procedure.

In the login request, the user needs to supply the correct username and password (Figure 6). The server with mutual agreement with the database server looks into the records and process the login request. In the event of invalid username and password, an error message will appear prompting the user to supply the correct entries.



(b) (c)

Figure 7. User Login Window with Error message (a) Invalid Password, (b) Account Locked and (c) Invalid OTP Code

In case of failed attempts, the user account will be locked. This is to prevent the user from unlimited attempts and lessen the chances from attack. The user will be prompted with message requesting to contact the administrator to unlock said account. The privileged access is granted to authorize, verify or limit the user only. A limited control privilege will minimize access to information and resources only to those with legitimate purposes. The principle of least privilege is important in enhancing the protection of data and functionality from faults and malicious behavior. Among the benefits of this principle includes better system stability, better system security, and ease of deployment. Thus, the system considered the limited privilege security as it allows autoblocker and human intervention after a number of failed attempts. In case of incorrect combination, the system will generate another code and repeat sending the codes to the user. The system allows the user up to three (3) successful attempts to input the correct OTP combination before the system rejects any input request.

Two-level pass refers to the process where user requires to passs through verification process. As mentioned earlier, the user allows to three successful attempts only. As added level of security of the system automatic redirection was introduced. Automatic redirection refreshes the current page and redirect to homepage if noticed no event was recognized in the OTP code. This prevent the system from prolonged event which may be a source of potential threat.

6. Conclusion

Security and protection of information in web-enabled application becomes a special concern. The creation of rules and policies are supplementary measures to safeguard the data Protection of the system with improved authentication mechanism adds a level of security to the system. The most important procedures relating to information for disasters aside from recording, monitoring, processing, sharing and dissemination is the protection and security of information.

Over the years, disaster risk management played a client-centric approach to disaster risk reduction management in which vital information was passed through a web-centric application. This information is stored either in host network or via third party provider. Transmission over the network does not guarantee the integrity of information. The new

algorithmic OTP scheme based on table sequence pattern schedule provided a new level of security for users as it applied a new scheme in generating OTP codes allowing the pair of codes to be randomly generated and mapped out in tables. It made use of XY schedule send to user with successful advantage over the printed grid scheme like BINGO card.

The results were conclusive that the proposed improvement on OTP scheme proved to generate a randomize XY values to be complex. The effect of restriction in 1:1 value allowed the system to be free from brute force attack and dictionary attack.

The performance of the algorithm and the system in general were conclusive that the new algorithm posed advantage over traditional authentication and OTP printed scheme as this incured cost in printing the OTP codes. The study further states that the comparative analysis yielded conclusive ratings taking advantage of the proposed OTP scheme. This means the new OTP scheme managed to handle the procedure with less operations with minimal number of elements.

Acknowledgements

Following(above) are results of a study on the "Leaders INdustry-university Cooperation+" Project, supported by the Ministry of Education, (MOE). Our thanks to Technological Institute of the Philippines, Commission on Higher Education and Bicol University for the support extended.

References

[1] QueensLand Government, "Disaster Management Phases", The State of Queenland 2010-2013. Retrieved from http://www.disaster.qld.gov.au dated January 6, 2017.
[2] Phil-Japan, Philippines, Japan sign agreement on disaster communication. May 19, 2014. Retrieved from http://www.gov.ph.
[3] M. Zukime, M. Junoh, A. Osman,M.S. Ab Halim and S. Adbullah, "Data Security: Issues And Challenges For Disaster Management In The New", in International Journal of Scientific & Technology Research ISSN 2277-8616, vol. 3, no. 8, **(2014)**.
[4] L.J. Semer, "Disaster recovery planning for thedistributed environment", Internal Auditor, vol. 55, no. 6, **(1998)**, pp. 41-7
[5] R. Javidan and M.A. Pirbonyeh, "A new security algorithm for electronic payment via mobile phones", in 2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies, ISABEL 2010, **(2010)**.
[6] L. J. Lacona, "Lamport's one-time password algorithm", A design pattern for securing client/service interactions with OTP. March 31, 2009. Retrieved January 22, 2017 from JavaWorld http://www.javaworld.com/article/2078022/open-source-tools/lamport-s-one-time-password-algorithm--or--don-t-talk-to-complete-strangers--.html, **(2009)**.
[7] Shally and G. Singh Aujla, "A Review of One Time Password Mobile Verification", in Jun 2014 International Journal of Computer Science Engineeringand Information Technology Research (IJCSEITR), ISSN (P): 2249-6831; ISSN (E): 2249-7943, vol. 4, issue 3, pp. 113-118
[8] Y.T. Fan and G.P. Su, "Design of two-way one-time-password authentication scheme based on true random numbers", in 2nd International Workshop on Computer Science and Engineering, WCSE 2009, vol. 1, **(2009)**. pp. 11–14.
[9] X.J. Chen and F. Xu, (n.d.), "A Practical Real-Time Authentication System with Identity Tracking Based on Mouse Dynamics".
[10] S.A. El-Booz, G. Attiya and N. El-Fishawy, "A secure cloud storage system combining Time-based One Time Password and Automatic Blocker Protocol", in 2015 11th International Computer Engineering Conference: Today Information Society What's Next?, ICENCO 2015, **(2015)**, pp. 188–194.
[11] K. Sudhakar, S. Srikanth and M. Sethuraman, "Secured mutual authentication between two entities", in Proceedings of 2015 IEEE 9th International Conference on Intelligent Systems and Control, ISCO 2015, **(2015)**.
[12] Y. Huang, Z. Huang, H. Zhao and X. Lai, "A new One-time Password Method", IERI **(2013)**.
[13] Y. Li, "Research on e-business identity authentication system based on improved one-time password", in 2008 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2008, **(2008)**.

[14] B. Davaanaym, Y.S. Lee, H. Lee, S. Lee and H. Lim, "A Ping Pong based one-time-passwords authentication system", in NCM 2009 - 5th International Joint Conference on INC, IMS, and IDC, **(2009)**, pp. 574–579.
[15] E. Sediyono, K. I. Santoso and Suhartono, "Secure login by using One-time Password authentication based on MD5 Hash encrypted SMS", in Proceedings of the 2013 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2013, **(2013)**, pp. 1604–1608.
[16] K. Alghathbar and H.A. Mahmoud, "Noisy password scheme: A new one time password system", in Canadian Conference on Electrical and Computer Engineering, **(2009)**, pp. 841–846.
[17] D. Kumar, A. Agrawal and P. Goyal, "2015 International Conference on Advances in Computer Engineering and Applications", IMS Engineering College, Ghaziabad, India. 978-4673-6911-4/15. 2015 IEEE, **(2015)**.
[18] K.C. Liao, W.H. Lee, M.H. Sung and T.C. Lin, "A one-time password scheme with QR-code based on mobile phone", in NCM 2009 - 5th International Joint Conference on INC, IMS, and IDC, **(2009)**, pp. 2069–2071.
[19] B. Sodhi, "Using dropped call as an authentication factor", in Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, **(2015)**, pp. 2031–2035.
[20] Margosis, "Problems of Privilege: Find and Fix LUA Bugs", August 2006, **(2006)**, Microsoft.

Authors

Benedicto B. Balilo Jr., he received the B.S. degree in Computer Science from Dynamic Computer Centrum, Legazpi City, Philippines in 1994. He is a recipient of BU-UC MIT offshore program under CHED FDP II scholarship grant earning his Master's degree in Information Technology (MIT) in 2015 and Master in Business Administration from Aquinas University in 2012. Also, he earned units in Master in Information System in UPOU and Bachelor of Laws in Aquinas University, Legazpi City. He is a 3-termer Municipal Councilor of LGU Sto. Domingo, Albay from 1998-2007 and former Regional BOD of PCL and NMYL of the Province of Albay.

Currently, he is a recipient of CHED FDP II scholar for the program Doctor in Information Technology (DIT) at Technological Institute of the Philippines (TIP), Quezon City, Philippines. He is presently working his research in information security. He is a faculty member of Bicol University, Legazpi City, Philippines with a rank of Assistant Professor III. In 2012, he was designated Extension Coordinator of the College of Science. His extension project "WebDev in Action: The CS/IT Way" was awarded 3rd Best Extension Paper Award during the 1st BU in-house extension review in September 11, 2013. He is the PSITE (Bicol Region) Regional President and a member of Philippine e-Learning Society (PeLS), NMYL, PCL and Association for Computing Machine (ACM-Student).

Bobby D. Gerardo, he is currently the Vice President of Administration and Finance of West Visayas State University, Iloilo City, Philippines. His dissertation is "Discovering driving patterns using rule-based intelligent data mining agent (RiDAMA) in distributed insurance telematic system". He has published 54 research papers in national and international journals and conferences. He is a referee of international conferences and journal publications in IEEE Transactions on Pattern Analysis and Machine Intelligence and IEEE Transactions on Knowledge and Data Engineering. He is interested in the following research fields: distributed systems, telematics systems, CORBA, data mining, web services, ubiquitous computing and mobile communications.

Dr. Gerardo is a recipient CHED Republica Award in National Science Category (ICT field) in 2010. His paper entitled "SMS-based automatic billing system of household power consumption based on active experts messaging" was awarded best paper on December 2011 in Jeju, Korea. An excellent paper award was given for his paper "Principal component analysis mechanism for association rule mining," on Korean Society of Internet Information's (KSII) 2004 Autumn Conference on November 5, 2004

Ruji P. Medina, he is Dean of the Graduate Programs and concurrent Chair of the Environmental and Sanitary Engineering Program of the Technological Institute of the Philippines in Quezon City. He holds a Ph.D. in Environmental Engineering from the University of the Philippines with sandwich program at the University of Houston, Texas where he worked on the synthesis of nanocomposite materials. He finished his MS in Environmental Engineering from the Mapúa Institute of Technology, graduating Summa Cum Laude. He obtained his Bachelor's degree in Chemical Engineering from the University of the Philippines in Diliman, Quezon City. His research interests include urban mining, electronic wastes, and nanomaterials, He counts among his expertise environmental modeling and mathematical modeling using multivariate analysis.

Yungcheol Byun, he is a full professor at the Computer Engineering Department (CE) at Jeju National University. His research interests include the areas of Artificial Intelligence and Machine Learning, Signal Processing & Security, Intelligent Computing, Ubiquitous Computing, and RFID & IoT Middleware. Outside of his research activities, Dr. Byun has been hosting international conferences, CNSI (Computer, Network, Systems, and Industrial Engineering), ICESI (Electric Vehicle, Smart Grid, and Information Technology), and also serving as a conference and workshop chair in various kinds of international conferences and workshops. He received his Ph.D. from Yonsei University in 2001. Before joining the current university, he was a senior researcher of Electronics and Telecommunications Research Institute (ETRI)

