Scientific Research Publishing

Journal of Computer and Communications, 2021, 9, 1-12
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Authentication Key-Exchange Using SMS for Web-Based Platforms

Benedicto B. Balilo Jr.*, **Jayvee Christopher N. Vibar**

College of Science, Bicol University, Legazpi, Philippines
Email: *bjbbalilo@bicol-u.edu.ph, jcnvibar@bicol-u.edu.ph

How to cite this paper: Balilo, B.B. Jr. and Vibar, J.C.N. (2021) Authentication Key-Exchange Using SMS for Web-Based Platforms. *Journal of Computer and Communications*, **9**, 1-12.
https://doi.org/10.4236/jcc.2021.98001

Received: July 1, 2021
Accepted: July 30, 2021
Published: August 3, 2021

Abstract

One of the advantages of One Time Password (OTP) is that it's free from brute force, replay, and shoulder attacks. The codes may originate from different entropy attributes and schemes, such as true random and digital random number generators. Businesses, organizations, and academic institutions have adopted OTP methods for credit card transaction confirmation, recalling forgotten passwords, and validating web portal accounts. This paper proposed a new method in authenticating login credentials using a 3 × 3 matrix and random system key as Two-Factor Authentication (2FA) with an SMS-enabled feature. We used the 6-codes pseudorandom method and a 4-codes validation to allow mobile flexibility and ensure that the user has the required access. The page link and evaluation form are sent to students, IT professionals, and researchers. The results showed respondents are satisfied in terms of functionality, usability, efficiency, and reliability. The developed system could safeguard information, disallow unauthorized access, and impose acceptable data protection measures and minimal system requirements to use the system.

Keywords

One Time Password, Two-Factor Authentication (2FA), Cryptography, ISO9126

1. Introduction

The proliferation of web applications has empowered businesses and organizations to tap up their clients in a systematic and convenient approach to doing electronic transactions over the Internet. Universities local and foreign are moving on embracing these opportunities. In this paper, Bicol University is the host university used as the model to apply a unique and authentic way of using One-Time-Password (OTP) on top of the QCE System.

The most common form of authentication is the use of username and password. Static and dynamic passwords are used to protect a system from an unauthorized individual; the latter uses a third-party system to generate passwords while the former is prone to keylogging and other forms of attacks [1]. A shared secret seed has proven to enhance TOTP security on web protocol, specifically in OTP authentication [2]. The human factor is a critical weak point in securing confidential information [3]. Password is essential, the loss of which can cause companies damage in productivity and putting employee's data at risk [4].

The selection of appropriate authentication methods is crucial in decision-making, especially in designing secure systems. It may also refer to the process of verifying the identity of a user, tracing the origins of an event, or ensuring that the information comes from a trusted site. It confirms the truth or genuineness of an attribute or entity and establishes authenticity or proves genuineness. Also, it means processes of selecting or making access to a computer network, making purchases online, transferring accounts through bank websites, or visiting social media. Simple presentation of user credentials and authenticating the connection of both parties, but failure to establish can compromise the network and the resources or even vulnerable to misuse [5].

An OTP scheme was introduced in which values are stored on the client-side using the one-way mathematical scheme with incremental value. The scheme's core requires that the client cooperate and agree to use a standard sequencing algorithm to generate a set of expiring OTP (client-side) and validate client-provided passkeys included in each client-initiated request [6] [7]. The OTP evolved from the S/KEY released by Bellcore and was described in work by Haller and RFC 1760 [6].

The One-Time Password (OTP) is a modern authentication scheme that protects users against unauthorized access to restricted resources. It saves the customer time, increases accuracy, and makes the system more secure. Out-of-band, cannot be reused, can be time-limited, can be used over untrusted communication paths, can be used with a compromised user password, and has multiple generation mechanisms that are some of these benefits [8] [9]. SMS, hardware and software token, biometric technology, and smart cards are some of many schemes proposed and implemented to protect information to increase security and reduce the risk of unauthorized access and tampering of data [10]. These protection schemes can be divided into functional properties such as unprotected scheme, all-or-nothing scheme, controlled sharing, and user-programmed [11]. Moreover, many of these schemes still use mathematical methods or simple combinations of parameters to generate passwords but still suffer potential attacked risks [12].

Nowadays, OTP tokens are a common authentication mechanism for many companies, institutions, and even governments to upgrade their security strategy. For example, Google uses sending OTP via SMS to authenticate users after numerous failed login attempts. Wifi hotspots in public places like shopping malls and terminals (airport terminals and seaports) also used OTP. In the registration phase, the telcos generate a one-time password and directly send it to the user's mobile phone as authentication privilege to use the free Internet service. This mechanism will be suitable only for a span of 30 minutes, and the user needs to re-login for re-authentication after certain hours or even a day.

QCE Evaluation System is a web-based application system for evaluating faculty teaching effectiveness by students at Bicol University. Online evaluation system naturally requires authentication to be robust and seamless. Faculty deserves to be rated with authentic clientele—the students. In this study, the security and authentication mechanism is to strengthen to a level that is acceptable enough to perform the necessary objective of rating these faculties online in the most convenient way.

A weak authentication scheme can lead to unauthorized access to protected resources. Web applications such as QCE Evaluation System tantamount to illegal entry and thus must be protected. OTP is one of the modern approaches to circumvent these types of problems; however, it is becoming vulnerable since the process has become common in the industry for several years now.

The project aims to provide security in authenticating legitimate users while logging in to the system and use the University Internet service. The system will utilize the algorithm that will produce a random BINGO pattern matrix for one-time password generation. It is attribute-based and combines different schemes and other mechanisms (*i.e.*, keyboard and mouse dynamics, screen manipulation, grid-based, etc.) that have exposed OTP in different transaction levels. The more the parameters involved, the more complex the password produced and the longer the space covered. This authentication factor is about a bingo-like random matrix coordinate lookup system. The random cell in the card letters (BINGO) carries the correct combination of numbers in the cell.

Furthermore, OTP authentication is growing and will continue to take advantage of technology trends to guarantee the safety and protection of information or data. However, authentication technique has different trade-offs, making 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. Some factors put restrictions on reliability like monitoring GSM networks, international roaming, SMS costs, and malicious phone applications to obtain mobile transaction authentication numbers and delays. It also has restrictions in hardware resources like low transition rate, low bandwidth of communication channel, limited calculations capabilities of the processor, battery, and memory. Nonetheless, it provides a comprehensive communication channel with considerations in cost, communication signal, and capacity of a service provider to guarantee message integrity.

The Grid-based authentication is about XY lookup system like BINGO card printed in rows and columns that is easy to manage, economical, and provides flexibility to users. The grid is printed in cards and sends them via mail or courier, SMS, email, and fax [13]. The coordinates (like B2, A3, and C2) are displayed to the user to input the correct numbers and letters. Thus, the study shall support institutions' existing QCE system to improve login authentication using the SMS-OTP method.

2. Methodology

The project has two (2) studies, namely: development and evaluation of the development system. The study used Rational Unified Process (RUP), which will serve as the building block for the development process. It was divided into distinct phases: initiation, elaboration, construction, and transition. RUP was built in the concept of iterative development of which it provides a structured way of preventing the resources from wasted and reduces unexpected development costs as it determines each artifact and milestones for each phase [14].

In the inception phase, existing OTP techniques and methods were analyzed. The needed requirements of the project were identified and presented to use OTP using an SMS-based approach in the web-enabled environment portal. Diagrams and systems models are used to determine the procedures, relationship of entities, and use cases of the study—elaboration phase. Applications and tools are essential in the development process. Thus, the determination of the application best applied for a web-based environment. The construction of the system depends on the command and semantics of HMTL/PHP scripting language with simple javascript language needed to display the screen environment of the system—construction phase.

The developed system has hardware/software requirements to support the simulation process on the localhost with XAMPP for Windows 5.6.20. Other tools used include Sublime 4 text editor, Apache/2.4.17, PHP/5.6.20, and MySql/5.0.11. The system runs on Intel Corei5-4460 32-bit processor-based at a single processor 3.210 GHz, 4 GB DDR3 memory, 500 GB storage capacity, and Intel HD Graphics 4600 display adapter.

The system used username and password as the first-level authentication; once verified, the system generates a one-time password to confirm the owner's identity. The system has a system key and a feature for failed login attempts; this enables the system to monitor the number of the failed access to the system during a specific time range. The 3-failed login attempts prevent the user from continuing and allow the administrator to analyze the failure and render necessary action (**Figure 1**).

It is imperative that nobody wanted a flaw in the system and developed critical use cases. Software testing is a process to look for software bugs within a program or application. Since software bugs are defects in the system, test cases should be constructed to ensure that coverage was maximized [15]. Thus, a survey questionnaire was used to determine the developed system's functionality, usability, and maintainability. **Table 1** shows the evaluation criteria used.

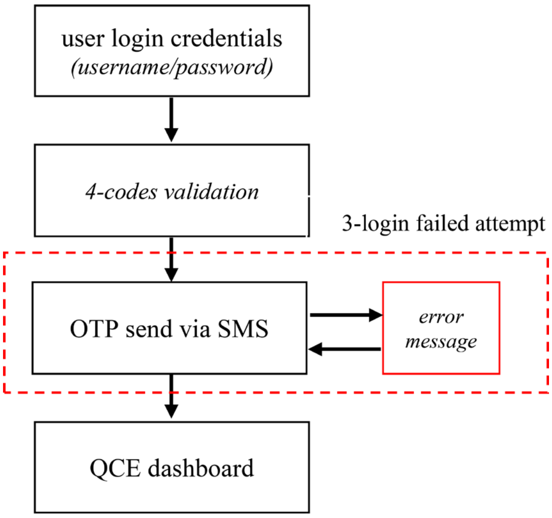


Figure 1. Process flow of accessing the dashboard page of the QCE system.

Table 1. Likert scale for software testing.

Range	Description
4.1 - 5.0	Far more than what is expected
3.1 - 4.0	More than what is expected
2.1 - 3.0	Presence of the expectation
1.1 - 2.0	Less than what is expected
0.0 - 1.0	Absence of the expectation

Table 2. Respondents of the study.

Respondents	Number	Percentage
Students	36	86%
IT Professionals	3	7%
Researchers	3	7%
TOTAL	**42**	**100%**

The researchers registered a free domain and hosting as a testing site of the system. The class group chats served as a venue to promote the page link. And, Google form was disseminated for one (1) month, requesting respondents to visit the site, register, navigate and evaluate the developed system. Table 2 shows the respondents of the study.

3. New Method

A One-Time Password (OTP) is a mechanism that allows user authentication using a unique password sent either SMS, token, or email. As reported, the assignment of static OTP was vulnerable to various attacks, *i.e.*, brute force, shoulder attack. The OTP is a more secure mechanism than the static password. It provides complete protection of the login-time authentication against replay attacks [16].

Table 3 shows the proposed OTP scheme in which random codes are mapped in the matrix. This scheme is similar to a bingo-like concept, only that cells and numbers are limited. It is a combination of 6 numbers following the address of the code. For example, the coordinates A2 B1 C3 represent the code "811522," which shall form the OTP that the user must provide in the OTP request window.

The enrolled "OneWaySMS" SMS-enabled feature facilitates the forwarding of OTP codes to the user registered mobile number. The SMS provider shall serve as the gateway to access the student evaluation features. And, with the inclusion of the System Key to the system provides an extra level of validation. This way, we could state that the one who is currently accessing the QCE Student Evaluation portal is the legitimate owner of the registered account.

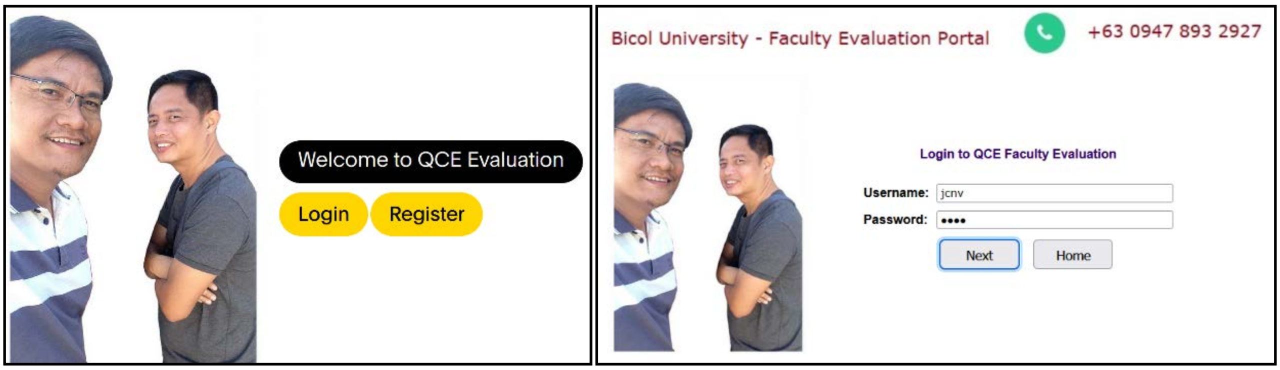
4. The Developed System

Introducing a new OTP method and generation of codes are just part of a system that may be a solution to a problem like improving security protocols or an extra level of authentication to secure and protect confidential information. Figure 2 shows the main page of the developed system. The interface served only as support for testing the developed OTP method.

The user has the option to either log in or register to the system. Students with registered accounts need to select the "Login" button and the "Register" button for students with no record yet in the system. Students should filled-out the registration form presented in Figure 3. This form provided the basic and essential

Table 3. Sample generated random codes.

	A	B	C
1	74	15	86
2	81	32	64
3	89	97	22



Bicol University - Faculty Evaluation Portal

+63 0947 893 2927

Login to QCE Faculty Evaluation

Username: jcnv

Password: ••••

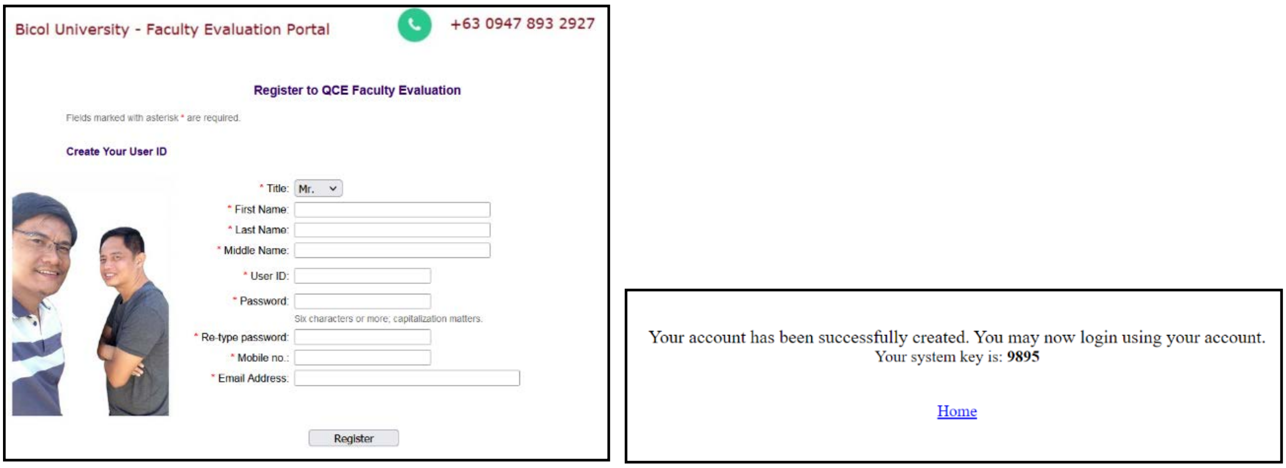
(a)

(b)

Figure 2. The main page: (a) Sample QCE Evaluation page, (b) login user page.

requirements, including the student's name, user ID, password, mobile number, and email contact. These are essentials to the system procedures as the OTP shall be sent through SMS and System Key to add up in the authentication process.

The system assumed an existing QCE Evaluation system in which students are enrolled in different subjects. Aside from proposing a new OTP method, this study aims to determine the feasibility of integrating OTP into the system cycle and determine student's perceptions. In the process, registered students need to secure authentication by inputting usernames and passwords. An OTP shall be directly forwarded to the student registered mobile phone number (Figure 4). Businesses typically used SMS OTPs because this approach was relatively easy to implement, and most of the customers have mobile phones and are familiar with OTPs [17]. Students have a positive perception of using m-learning using a mobile phone. Students used mobile phones as alternative media during the conduct of


Bicol University - Faculty Evaluation Portal ☎ +63 0947 893 2927

Register to QCE Faculty Evaluation

Fields marked with asterisk * are required.

Create Your User ID

* Title: Mr.
* First Name:
* Last Name:
* Middle Name:
* User ID:
* Password:
Six characters or more; capitalization matters.
* Re-type password:
* Mobile no.:
* Email Address:

Register

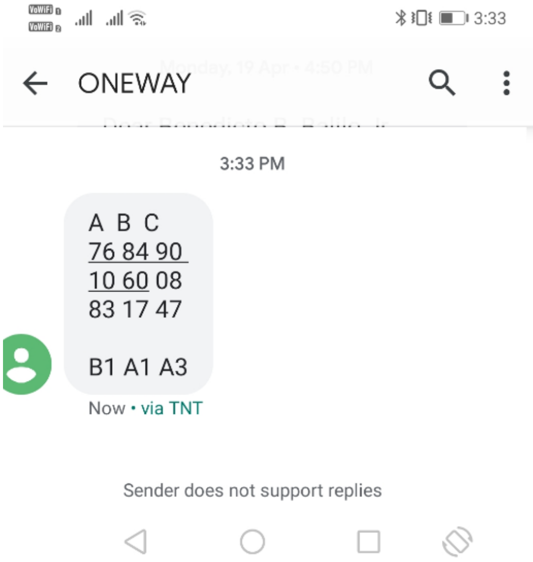
Your account has been successfully created. You may now login using your account.
Your system key is: **9895**

Home

(a)

(b)

Figure 3. (a) QCE Faculty Evaluation Registration and (b) System Key generated.


3:33

ONEWAY

3:33 PM

A B C
76 84 90
10 60 08
83 17 47

B1 A1 A3

Now • via TNT

Sender does not support replies

Figure 4. Sample OTP received via SMS.

online learning classes in this time of pandemic [18].

Once the OTP was received, students need to input the correct and appropriate OTP code for the given session (Figure 5). The session was called to store the OTP codes, and this could be used across multiple pages. By default, the session stays until the user closes the browser. In the system, the application of a 3-failed attempt was highlighted. This enhanced the security feature of the system as it only allows valid login attempts.

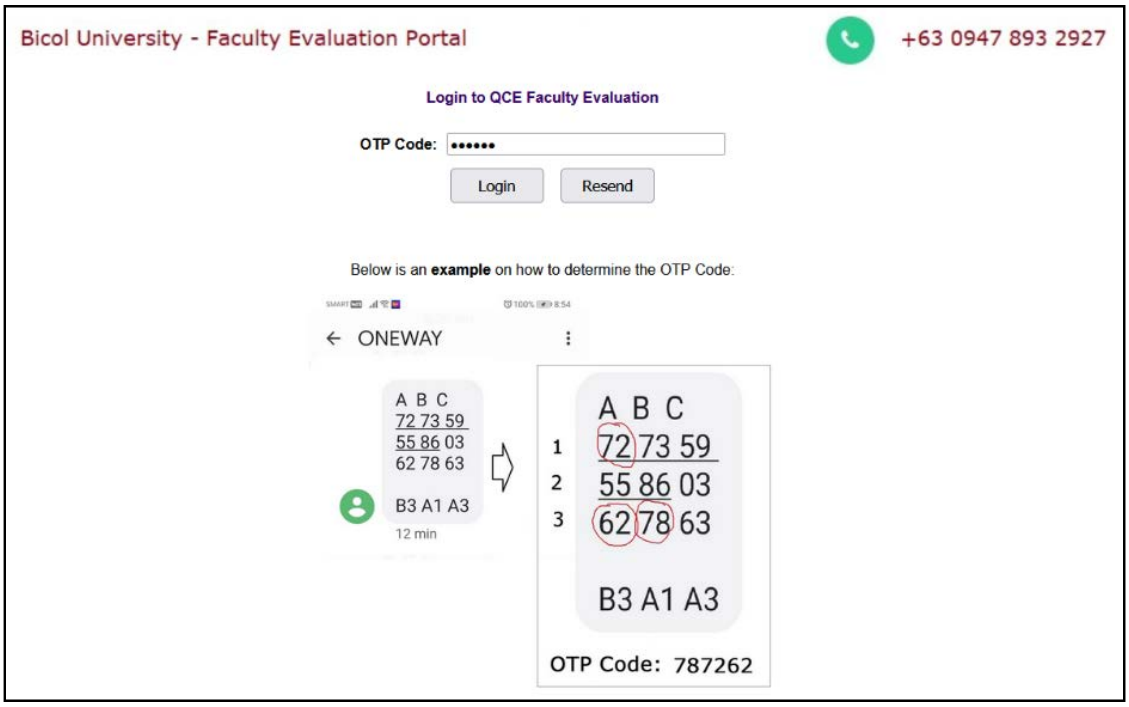
Instructions are essential, especially in reading the received OTP. Students may have different brands and models of mobile phones, which may cause problems. The simple pattern and codes offered by the system may provide a solution and simplify the process.

Figure 6 shows the sample system interface with student's subjects for evaluation. The evaluation criteria used were similar to the actual evaluation form used in evaluating faculty at the end of the semester. The criteria are commitment, knowledge of the subject, management of independent learning, and management of education.

The "Option" button was used to select and scroll from the choices quickly. Like the traditional evaluation process, students can ignore or leave blank options and click the "Submit" button entries as final.

5. Evaluation of the Developed System

A group of students, IT professionals, and researchers evaluated the system. Table 4 shows the evaluation results based on ISO 9126 regarding functionality, reliability, usability, efficiency, maintainability, and portability. There is no guarantee of



Bicol University - Faculty Evaluation Portal

☎ +63 0947 893 2927

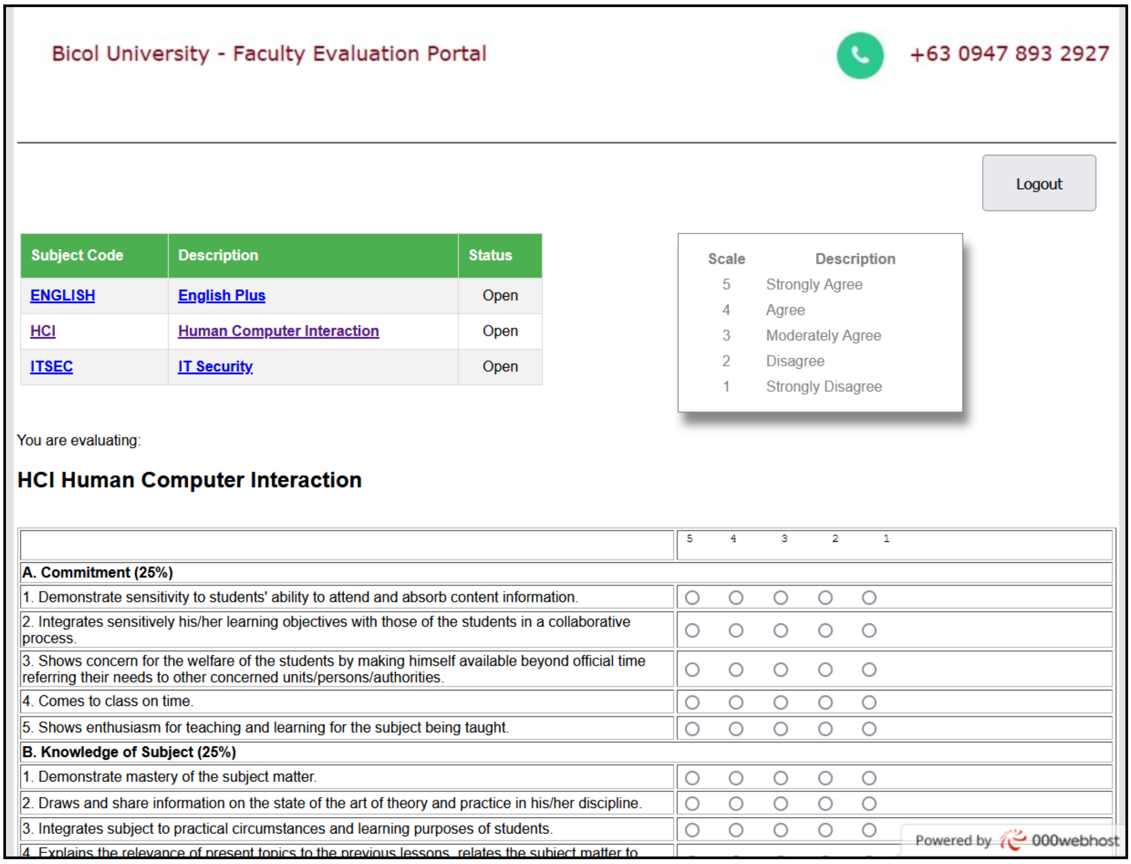
Login to QCE Faculty Evaluation

OTP Code: ••••••

Below is an **example** on how to determine the OTP Code:

OTP Code: 787262

Figure 5. Validation of the One-Time Password sent via SMS.



Bicol University - Faculty Evaluation Portal

☎ +63 0947 893 2927

Subject Code	Description	Status
ENGLISH	English Plus	Open
HCI	Human Computer Interaction	Open
ITSEC	IT Security	Open

Scale	Description
5	Strongly Agree
4	Agree
3	Moderately Agree
2	Disagree
1	Strongly Disagree

You are evaluating:

HCI Human Computer Interaction

	5	4	3	2	1
A. Commitment (25%)					
1. Demonstrate sensitivity to students' ability to attend and absorb content information.	○	○	○	○	○
2. Integrates sensitively his/her learning objectives with those of the students in a collaborative process.	○	○	○	○	○
3. Shows concern for the welfare of the students by making himself available beyond official time referring their needs to other concerned units/persons/authorities.	○	○	○	○	○
4. Comes to class on time.	○	○	○	○	○
5. Shows enthusiasm for teaching and learning for the subject being taught.	○	○	○	○	○
B. Knowledge of Subject (25%)					
1. Demonstrate mastery of the subject matter.	○	○	○	○	○
2. Draws and share information on the state of the art of theory and practice in his/her discipline.	○	○	○	○	○
3. Integrates subject to practical circumstances and learning purposes of students.	○	○	○	○	○
4. Explains the relevance of present topics to the previous lessons, relates the subject matter to					

Figure 6. System interface with subjects ready for evaluation.

Table 4. Evaluation results of the developed system.

Criteria	Mean	Explanation
Functionality	3.07	Presence of the expectation
Reliability	3.11	More than what is expected
Usability	3.08	Presence of the expectation
Efficiency	3.23	More than what is expected
Maintainability	3.11	More than what is expected
Portability	3.24	More than what is expected
Total Mean	**3.14**	**More than what is expected**

the quality of the developed products for the first time of its release. Much of the success in software projects can be attributed to user satisfaction and the quality of the generated products. Competence, training, knowledge, level of user involvement, and resistance to change are relevant factors identified that could influence the quality of the product. The ISO 9126 is a model based on software quality products specifying software quality requirements [19].

The results showed that the overall mean 3.14, which means respondents are satisfied *more than expected* with the developed system. Some of these include safeguarding information, disallow unauthorized access, and imposes acceptable measures for data protection, minimal transaction interval, and minimal system requirement to use the system. However, there are concerns to be addressed for the system to functionally and usable when integrating into the existing QCE Evaluation system. These are enhancements of three (3) failed-attempt features of the design, error-response mechanism, page layout, and detailed guide for the user on the proper use of the system.

The researchers did not focus on the page layout as the OTP will serve as an additional feature and procedure to the existing system. Nonetheless, the objective to generate a new OTP method that would add up to the level of security of the system was accepted and considered (74%) by students, faculty, and IT professionals, and twenty-six (26%) percent answered, "*Maybe*."

Respondents were asked if they have suggestions to improve the developed system. Among the recommendations raised were on the graphical user interface, detailed instructions, and design features improvement. Some raised concerns on browser compatibility, security protocol/SSL certificates, the importance of implementing the OTP, and navigation to use the system. Respondents recognized the proposed method as an alternative security mechanism for login authentication and provided a reasonable requirement for web-platform applications.

6. Conclusion

The study introduced a new scheme for generating and applying OTP as two-factor authentication (2FA) using pseudorandom and matrix patterns using SMS. The use of the 6-codes method allows mobile flexibility and a 4-codes validation to ensure that the user has the required access. The page link and evaluation form are sent to students, IT professionals, and researchers. With a total mean of 3.14, the developed system achieved the expected functionality, reliability, usability, efficiency, maintainability, and portability. Also, with the new method, the system could safeguard information, disallow unauthorized access, and impose acceptable data protection measures and provide minimal system requirements.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Yusuf, S.I., Boukar, M.M., Mukhtar, A. and Yusuf, A.D. (2018) User Define Time Based Change Pattern Dynamic Password Authentication Scheme. 2018 14*th International Conference on Electronics Computer and Computation* (*ICECCO*), Kaskelen, 29 November-1 December 2018, 206-212.
https://doi.org/10.1109/ICECCO.2018.8634675
https://ieeexplore.ieee.org/document/8634675

[2] Uymatiao, M.LT. and Yu, W.E.S. (2014) Time-Based OTP Authentication via Se-

cure Tunnel (TOAST): A Mobile TOTP Scheme Using TLS Seed Exchange and Encrypted Offline Keystore. 2014 4*th IEEE International Conference on Information Science and Technology*, Shenzhen, 26-28 April 2014, 225-229. https://doi.org/10.1109/ICIST.2014.6920371

[3] Lartey, K.H., Li, M., Botchey, F.E. and Qin, Z. (2021) Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things. *Heliyon*, **7**, Article No. E06522. https://doi.org/10.1016/j.heliyon.2021.e06522

[4] Centrify (2014) Centrify Survey Results. Finn Partners. https://www.centrify.com/resources/5778-centrify-password-survey-summary/

[5] Duncan, R. (2001) An Overview of Different Authentication Methods and Protocols. White Paper, SANS Institute, North Bethesda.

[6] Lamport, L. (1981) Password Authentication with Insecure Communication. *Communication of the ACM*, **24**, 770-772. https://doi.org/10.1145/358790.358797

[7] Haller, N., Metz, C., Nesser, P. and Straw, M. (1998) A One-Time Password System. *Network and Distributed System Security Symposium*, San Diego, 11-13 March 1998, 98-100. https://doi.org/10.17487/rfc2289

[8] Alghathbar, K. and Mahmoud, H.A. (2009) Noisy Password Scheme: A New One Time Password System. 2009 *Canadian Conference on Electrical and Computer Engineering*, St. John's, 3-6 May 2009, 841-846. https://doi.org/10.1109/CCECE.2009.5090247

[9] Bansal, N. and Singla, N. (2016) Cash Withdrawal from ATM Machine Using Mobile Banking. 2016 *International Conference on Computational Techniques in Information and Communication Technology* (*ICCTICT*), New Delhi, 11-13 March 2016, 535-539. https://doi.org/10.1109/ICCTICT.2016.7514638

[10] Liao, K.C., Lee, W.H., Sung, M.H. and Lin, T.C. (2009) A One-Time Password Scheme with QR-Code Based on Mobile Phone. 5*th International Joint Conference on INC*, *IMS*, *and IDC* (*NCM* 2009), Seoul, 25-27 August 2009, 2069-2071. https://doi.org/10.1109/NCM.2009.324

[11] Saltzer, J.H. and Schroeder, M.D. (1975) The Protection of Information in Computer Systems. The University of Virginia, Department of Computer Science, CS551: Security and Privacy on the Internet, Fall 2000. https://www.cs.virginia.edu/~evans/cs551/saltzer/

[12] Fan, Y.T. and Su, G.P. (2009) Design of Two-Way One-Time-Password Authentication Scheme Based on True Random Numbers. 2*nd International Workshop on Computer Science and Engineering* (*WCSE* 2009), Qingdao, 28-30 October 2009, 11-14. https://doi.org/10.1109/WCSE.2009.611

[13] Corum, C. (2006) Grid-Based Two-Factor Authentication Comes to Campus Cards. https://www.secureidnews.com/news-item/grid-based-two-factor-authentication-comes-to-campus-cards/

[14] Britton, C. and Doake, J. (2005) A Student Guide to Object-Oriented Development. Butterworth-Heinemann, 1-9. https://doi.org/10.1016/B978-075066123-2/50001-3

[15] Woodward, M.R. and Hennell, M.A. (2005) Strategic Benefits of Software Test Management: A Case Study. *Journal of Engineering and Technology Management*, **22**, 113-140. https://doi.org/10.1016/j.jengtecman.2004.11.006

[16] Huang, Y., Huang, Z., Haoran Zhao, H. and Lai, X. (2013) A New One-Time Password Method. *IERI Procedia*, **4**, 32-37. https://doi.org/10.1016/j.ieri.2013.11.006

[17] Stephens, C. (2020) Why Are SMS Codes Still the Global ID Solution? *Biometric Technology Today*, **8**, 8-10. https://doi.org/10.1016/S0969-4765(20)30110-7

[18] Biswas, B., Roy, S.K. and Roy, F. (2020) Students Perception of Mobile Learning during COVID-19 in Bangladesh: University Student Perspective. *Aquademia*, **4**, Article No. ep20023. https://doi.org/10.29333/aquademia/8443

[19] Curcio, K., Malucelli, A., Reinehr, S. and Paludo, M.A. (2016) An Analysis of the Factors Determining Software Product Quality: A Comparative Study. *Computer Standards & Interfaces*, **48**, 10-18. https://doi.org/10.1016/j.csi.2016.04.002