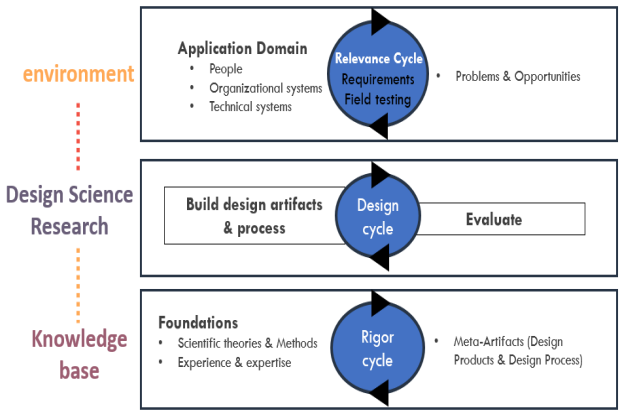

Fig. 2 Proposed Design Science research methodology

1) Application Domain: Any organization that *designs* software systems must prioritise communication *factors* with users, because users' requirements and experiences might change and differ from time to time. Some variables that should be considered at this stage: people, organizational and technical systems, and *problems* & opportunities.

There are two types of demographic people that can be appraised to the study, which are:

a) Classify user

Surveys and interviews are two most popular and well-proven ways for categorising individuals, and the user profile is one approach for doing so [17]. A user interview's main objective is to find out how people feel about security, i.e., their perception on threats, type of protection that they want, and other matters on security choices. Another aim is to determine who the user trusts and on what basis, as well as what concepts and vocabulary they use while communicating [18]. Although users' interviews or observations are critical, inquiring about the users' desired security goals might be difficult. They clearly need to be secured as viable as could be expected, yet the genuine inquiry is would they say they will go additional miles for that? [19]. Once this data is gathered and analysed, it is possible to identify some of the users' characteristics as well as the activities that they could perform in the system, avoiding a security-usability conflict.

b) Stakeholder

People who are actively involved in gathering usability and security demands to determine usability objectives and viable security approaches are known as stakeholders. They consist of expertise in the related field. These parties should evaluate their varied requirements while making decisions, including the need for usable security [20].

2) Build design artifacts and process: This level consists of two diverse functionalities, i.e., design of the task, and the particulars. These two are the major *factors* in building up the general process of interaction design. The process, later, will proceed to the implementation of the design and simulation purposes. The design will be handled with the *code* by using appropriate tools. The development of an *application entails* testing elements such as verifying its functionalities, figuring out aspects related to the application interface, validating navigation, and testing new techniques from the start, among other things.

The design of interactive systems may be approached in two ways which are:

a) Empirical approach

This approach is a combination of the designer's very own approach together with other expertise's method, which is accumulated through compilations of relevant advice for the creation of a successful interface. User assessment studies often back up these findings.

b) Methodological approach

The approach is based on some theoretical concept and the implementation of several processes for the design's reality. The technique to build systems with accessibility and usability is based on empirical approximation and guidance [21], [22]. This type of design may not be the best option, but we believe that it is the most suitable starting point for future research, in designing a system using a methodological approach to available safety.

According to the experimental approach, proposals for commercial analysis must be obtained at the design stage without abstraction, and without relying on complex security procedures [23]. Nielsen [24] has proposed a few principles in developing user interface. However, these principles do not reflect the security features and therefore the design of safe and usable interactive applications [25].

3) Evaluate: In achieving the goal of this stage, some elements are tested and evaluated to find out whether it works properly, or does it meet all the expectations, or maybe to simply understand *how a specific* tool works. For usable and accessible interactive systems, evaluation is very critical. At this stage, certain strategies are employed to get input from customers. It also has something to do with usability metrics and evaluation methods.

In this phase, the strategies required to gain response from both users or expert evaluators are being executed, which will be reflected in the design of safe and usable interactive applications.

a) Heuristic evaluation

The heuristic evaluation is a validation method, in which the main characteristic is the presence of experts (so-called evaluators) who will evaluate the usability and security aspects of the system interface. This is possibly the primary objective of this study, which is based on the concepts of user's security and authentication [25].

In relation to these concepts, usability and security experts analyse the user interface. This evaluation is insufficient as it only focuses on the design of the user interface without considering the core functions and processes. Evaluation methods in the next stage can help to identify the main problems caused by inadequate process modelling.

b) Evaluation method

The data will be examined to produce some results for evaluator reference. Representative evaluator will use the results to evaluate how the user interface assists users with their tasks. Security and privacy are not the primary goal of users [26]. Therefore, it can easily be omitted from the interface, generating risks due to possible mistakes they can make. The accomplished objectives will be performed with the result analysis and infrequent tasks. Based on this, users will be able to provide information that will help in

establishing improvements to the system for adequate usable security. Heuristics evaluation only is inadequate to find available security issues [18]. It should coordinate with the user's perceptions as every one sees a bunch of undertakings performed by the application. These users are monitored throughout each task to see how they used the interface during implementation, how long does it require, and whether the task was fortunately or unfortunately. The qualitative and quantitative findings of the evaluation and task analysis are presented, and this assessment will be able to identify the issues that users face when security is involved in the task. The information gathered is examined to determine critical aspects of the application's usability and security. The determination of most representative activities that users should achieve for applications where convenience and security are available is a fundamental part in the execution of the test system. In this study, the tasks were chosen based on literature that contained the application's most common tasks to collect information about users' challenges. Time and task success of percentage by indicators are produced using this approach.

4) Foundations: This stage is concluded *with scientific* theories and methods, experience, and expertise or meta-artificial of design products and design process. The foundation will be proposing a model and an algorithm for the flow of the user authentication online payment banking application.

The methodology is used for the purpose of bridging the gap between the usability and accessibility of user authentication online payment banking applications. The accessibility consists of the user interface which include application domain, build design artifacts and process, evaluation, and foundations. Usability considers human computer interaction. This is one of the essential justifications for why this approach was picked as a medium in incorporating the findings of this study into the development of secure and usable applications. Some factors of why this methodology was chosen is as below:

a. The user: The core of development and throughout all the model's phases.
b. Conceptual organization: Organize each notion in the proper order based on known scientific information.
c. Simple: Easy to grasp, with barely any nodes and branches, as well as no conditional routes.
d. Multidisciplinary team: Working in diverse teams is both necessary and beneficial (e.g. designers and programmers).
e. Flexibility: The concept is not linear or limiting in any way, but rather invites its unrestricted use.
f. Validation: Real-world testing has confirmed the model's accuracy.

III. Results and Discussion

According to the approach depicted in Figure 1, each discovered principle was analysed and assigned to the appropriate location to Table 1. From Table I, we can see that a total of 20 principles has been distributed to each attribute. Table II presented some of the principles of reliability.

TABLE I
NUMBER OF PRINCIPLES FOR EACH ATTRIBUTE

Attributes	Number of principles
Accessibility	4
Usability	5
Operability	3
Security	3
Reliability	3
Performance	2

TABLE II
PRINCIPLES OF RELIABILITY

Coded	Measurement items	References
	Reliability	
RE 1	Services performance of the online banking applications are absolutely reliable	George, A. [15]
RE 2	My choice to use the online banking applications was a wise one	Altobishi, T., Erboz, G., & Podruzsik, S. [16]
RE 3	The online banking application services is great	

A survey has been given randomly to a few communities from Kedah and Johor. The demographic of peoples and trends has been discovered. There are 106 respondents of the survey, and from here, 39% are male and 61% are female. There are 52% from 18 to 25 years old, 12% from 26 to 35, 30% from 36 to 45, 5% from 46 to 55, and 2% from 56 to 60 years old. From this point, we can conclude that the majority of the users who care about online banking applications functionalities are adults. Among them, 6% graduated from secondary schools, 4% from qualified certificates, 45% from diploma level, 13% from 1st degree, 17% from master's degree and 15% from PhD holders. Next, 34% comes from government sectors, 14% from private sectors, 45% from students and 7% are unemployed. For the monthly income aspect, 50% of them earn below RM 1000, 9% are within RM 1000 to RM 3000, 11% earn RM 3001 to RM 5000, 13% earn RM 5001 to RM 7000, 16% are within RM 7001 and above. There are 9% who just have 1 account, 63% have 2 to 3 accounts, 26% have 4 to 5 accounts and 2% have 6 to 7 accounts. According to this, most of the people who always used online applications for daily routine are within the B40 category.

In addition, 12% of them prefer over branch bank counters as their frequently used banking activities, 80% prefer to use ATM & CDM, 92% prefer the internet methods, and 44% prefer to via telephone. About 91% of them used the online banking applications, and only 8% never used it at all. With this finding, we can say that most of them often use the online banking applications rather than going to the ATM machine or over the counters to make some transaction activities. 13% of them often used the online banking application daily, 45% of them used it weekly, 39% used it on a monthly basis, 1 % used it yearly and 2% never used it at all. About 91% of them are often used for online shopping, 64% to pay bills, 34% for hire purchase, 70.1% just to check account balance, 84% to transfer money to other banks, and 9% for credit cards. Next, 66% of them choose Maybank2U as the most popular and easy to use online banking application, 47% vote for CIMB Clicks, 36% for Bank Muamalat, 21% choose Bank Islam, 10% for MyBSN, 9% for iRakyat (Bank Rakyat), 6% goes to

Public Bank, 5% for RHB Now (RHB Bank), 2% each from AMBank and Affin Bank and 1% for HSBC Online.

Following this, we can conclude that the usability of online applications and the accessibility to make transaction activities are very crucial to most people in Malaysia. They want better performance and qualities while using the online application, especially online banking applications. Although each of the applications has its own difficulty in terms of security, people will still use it because it is in trend, and easier as it can be done at their fingertips. A simulation of an online application has been developed according to the preliminary results. The prototype depicted in Figure 3.

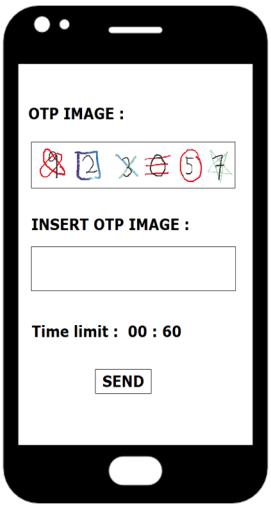

Fig. 3 Simulation of online payment application

From the figure 3, the simulation is made based on the discussed usability and accessibility attributes. The process begins with the requested OTP images as shown above. Any images of numbers will be generated by the server for the purpose of verification by the user. When user the generated numbers that were sent to them, the transaction will be verified, and the user can proceed with their transaction. If the user inserted the wrong number, the transaction will not be able to proceed, and the user will be asked to repeat the step again. This process will be done within 60 seconds or 1 minute, or it will be processed back to make sure the transaction is authenticated.

IV. Conclusions

User interface design has a difficulty with security. As a result, developers need tools to help them to enhance their designs in terms of usable security for applications, such as user authentication. The UAce principles can be used to alleviate accessibility and usability design difficulties. This is a significant addition to the area of UAce. We are proposing a design science research (DSR) methodology integrated with a user-centered design approach to align and bridge the gap between the usability and security of user authentication online payment banking applications. Following the ISO 9241-210 standard, it complements multiple design techniques by giving a structure to human-centered design that incorporates different procedures and improvement fit for a specific situation. This standard establishes a development method and tool for assessing subjectively and quantitatively usable security and user authentication while taking into account specific elements, qualities, and features of the ISO 25010:2011. Despite the fact that there are several ways for assessing the usability of security systems, these techniques are not user-centered owing to a lack of appropriate concepts. Future study will focus on analysing and reviewing the expert-developed heuristics in order to assign a value to each principle in addition with the security element. This also can be evaluated in relation to Internet Banking Acceptance [27]. These ideas and assessment methodologies provided in this study, together with the DSR, may be used to provide user interface design solutions.

Acknowledgment

We would like to thank UTHM by giving the opportunity of the grant of Tier 1 (H808) entitled A Graphical-based Authorization using Multiple Media variation to enhance the Efficiency of Verification process during Online Transaction, to support the research activities.

References

[1] Fuglerud, K. S., & Røssvoll, T. H. (2010). Previous and related research on usability and accessibility issues of personal identification management systems. Norwegian Computing Center, Oslo (Norway), Tech. Rep. DART/10/10.

[2] Fuglerud, K. S., & Røssvoll, T. H. (2012). An evaluation of web-based voting usability and accessibility. Universal Access in the Information Society, 11(4), 359-373.

[3] Andrew, S., Watson, S., Oh, T., & Tigwell, G. W. (2020, October). A Review of Literature on Accessibility and Authentication Techniques. In The 22nd International ACM SIGACCESS Conference on Computers and Accessibility (pp. 1-4).

[4] Pedersen A. Usability of authentication in web applications. A literature review. University of Copenhagen, Tech. Rep. 2010.

[5] Bevan, N., Carter, J., Earthy, J., Geis, T., & Harker, S. (2016, July). New ISO standards for usability, usability reports and usability measures. In International conference on human-computer interaction (pp. 268-278). Springer, Cham.

[6] Yeratziotis, A., Greunen, D., Pottas, D.: A framework for evaluating usable security: the case of online health social networks. In: 6th International Symposium on Human Aspects of Information Security and Assurance (2012)

[7] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), 1-41.

[8] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.

[9] Dresch, A., Lacerda, D. P., & Antunes, J. A. V. (2015). Design science research. In *Design Science Research* (pp. 67-102). Springer, Cham.

[10] Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a framework for evaluation in design science research. European journal of information systems, 25(1), 77-89.

[11] Forget, A., Chiasson, S., & Biddle, R. (2015, September). Choose your own authentication. In Proceedings of the 2015 New Security Paradigms Workshop (pp. 1-15).

[12] Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value-based objectives. Computers in Human Behavior, 61, 656-666.

[13] Stanton, N. A., Salmon, P. M., Rafferty, L. A., Walker, G. H., Baber, C., & Jenkins, D. P. (2017). Human factors methods: a practical guide for engineering and design. CRC Press.

[14] Realpe, P. C., Collazos, C. A., Hurtado, J., & Granollers, A. (2015, September). Towards an integration of usability and security for user authentication. In Proceedings of the XVI International Conference on Human Computer Interaction (pp. 1-6).

[15] George, A. (2018). Perceptions of Internet banking users—a structural equation modelling (SEM) approach. IIMB management review, 30(4), 357-368.
[16] Altobishi, T., Erboz, G., & Podruzsik, S. (2018). E-Banking effects on customer satisfaction: The survey on clients in Jordan Banking Sector. International Journal of Marketing Studies, 10(2), 151-161.
[17] Muratovski, G. (2015). Research for designers: A guide to methods and practice. Sage.
[18] Realpe-Muñoz, P., Collazos, C. A., Granollers, T., Muñoz-Arteaga, J., & Fernandez, E. B. (2017, September). Design process for usable security and authentication using a user-centered approach. In Proceedings of the XVIII International Conference on Human Computer Interaction (pp. 1-8).
[19] Schwind, N., Magnin, M., Inoue, K., Okimoto, T., Sato, T., Minami, K., & Maruyama, H. (2016). Formalization of resilience for constraint-based dynamic systems. Journal of Reliable Intelligent Environments, 2(1), 17-35.
[20] Naqvi, B., & Seffah, A. (2018, May). A methodology for aligning usability and security in systems and services. In 2018 3rd International Conference on Information Systems Engineering (ICISE) (pp. 61-66). IEEE.
[21] Realpe PC, Collazos CA, Hurtado J, Granollers A. A set of heuristics for usable security and user authentication. InProceedings of the XVII International Conference on Human Computer Interaction 2016 Sep 13 (pp. 1-8).
[22] Coulton, P., & Lindley, J. G. (2019). More-than human centred design: Considering other things. The Design Journal, 22(4), 463-481.
[23] Morales, J., Rusu, C., Botella, F., & Quiñones, D. (2019). Programmer eXperience: A systematic literature review. IEEE Access, 7, 71079-71094.
[24] Nielsen, J. (1994). Heuristic evaluation, w: Nielsen J., Mack RL (eds.), usability inspection methods.
[25] Mohamed, M. A., Chakraborty, J., & Dehlinger, J. (2017). Trading off usability and security in user interface design through mental models. Behaviour & Information Technology, 36(5), 493-516.
[26] Abu-Salma, R., Redmiles, E. M., Ur, B., & Wei, M. (2018). Exploring user mental models of end-to-end encrypted communication tools. In 8th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 18).
[27] Guo, Y., Norziha Megat, M. Z. & Nur Azaliah, A. B. (2021). Conceptual Model on Internet Banking Acceptance in China with Social Network Influence. International Journal on Informatics Visualization, 5(2), 177-186.