Identifying Comparison and Selection Criteria for Authentication Schemes and Methods

Ignacio Velásquez, Angélica Caro, and Alfonso Rodríguez, *University of Bío-Bío*

Abstract—Multiple techniques exist for performing authentication such as text passwords and smart cards. Multi-factor authentication combines two or more of these techniques in order to enhance security. It is of interest to know what the current research on these authentication techniques is and what comparison and selection criteria exist that help in the decision of these techniques. A systematic literature review is performed in order to obtain the desired knowledge. Moreover, the found comparison and selection criteria are analyzed and organized in order to generate a list of criteria that can be used to help in the decision of authentication techniques in different situations. The results of this research help to cover the gap in literature that could be observed through literature, which is the lack of works that focus on the comparison and selection of authentication techniques.

Index Terms—Authentication Scheme, Comparison and Selection Criteria, Multi-Factor Authentication Method, Security

1 Introduction

AUTHENTICATION is the central component of any security infrastructure [1], as it is the first line of defense against the impersonation of an authorized user [2], because it is often a prerequisite to allowing access to resources in the system [3]. Specifically, Authentication is the process of positively verifying the identity of a user, device or other entity in a computer system [3].

Authentication factors are pieces of information used to authenticate or verify the identity of a user [4]. These factors can be categorized in three groups [5], [6]: what the user knows (based on knowledge), what the user owns (based on possession) and who the user is (based on inherence). Although the three above are the most used and well-known factors, there are other factors proposed in literature, such as the use of a person's social networks [7] and location-based authentication [8]. In order to enhance security, multi-factor authentication combines authentication techniques belonging to different factors [3].

In this article, single-factor authentication techniques will be addressed as authentication *schemes*, whereas multi-factor authentication techniques will be addressed as multi-factor authentication *methods*. Text passwords [9], [10], [11] and graphical passwords [12], [13], [14] are examples of knowledge-based authentication schemes, whereas smart cards [15], [16], [17] are examples of possession-based schemes and face recognition [18], fingerprints [19] and behavioral biometrics [20] are of inherence-based schemes. The combination of the knowledge and possession factors [21], [22}, the combination of the knowledge and the inherence factors [23], [24], the combination of the possession and inherence factors [25], [26] and the combination of all three well-known factors [27], [28] are examples of multi-factor authentication.

A Systematic Literature Review (SLR) has been performed in order to identify the most used criteria for comparing and selecting authentication schemes and methods, together with decision frameworks that use these criteria for the same purpose. Additionally, authentication schemes and methods have been reviewed with the objective of ascertaining the existing research on this topic.

Based on the findings of this SLR, a list containing the most recurrent comparison and selection criteria for authentication schemes and methods has been prepared. The objective of this list is to present a number of criteria that help in the decision-making process of both single-factor authentication schemes and multi-factor authentication methods in any situation. This can be observed through the results of the SLR, where the research on comparison and selection criteria for authentication schemes and methods has not been extensive. In the same way, no decision framework could be found that makes use of them analyzes both authentication schemes and authentication methods in depth.

The remainder of this article is as follows: Section 2 synthethizes the SLR, including both its planning and its results. The analysis and identification of comparison and selection criteria for authentication schemes and methods is given in Section 3. Finally, the conclusions of this research are shown in Section 4.

2 Systematic Literature Review

A SLR, based on Barbara Kitchenham's method [29], was performed in order to obtain the required knowledge for this article's research. The activity diagram shown in Fig. 1 illustrates the activities taken for the realization of this SLR.

The first activity was to perform a planning of the review, which, together with the identification of the need

- *I. Velásquez is with the Computer Science and Information Technologies Department, University of Bío-Bío, Chillán, Chile. E-mail: ivelasqu@alumnos.ubiobio.cl.*
- *A. Caro is with the Computer Science and Information Technologies Department, University of Bío-Bío, Chillán, Chile. E-mail: mcaro@ubiobio.cl.*
- *A. Rodríguez is with the Computer Science and Information Technologies Department, University of Bío-Bío, Chillán, Chile. E-mail: alfonso@ubiobio.cl.*

for research, served to obtain the search and review protocols. This planning was analyzed by two supervisors, in order to evaluate its adequacy. The next activity was to perform a general search in the different sources that were specified in the search protocol. The duplicate articles were removed from this search's results. Afterwards, a partial review was performed on the remaining articles, obtaining a list of potentially useful articles. These articles were reviewed and analyzed in depth, resulting in the list of useful articles for this research. Some details of the review planning are presented in Section 2.1, whereas the main findings of this SLR are shown in Section 2.2.

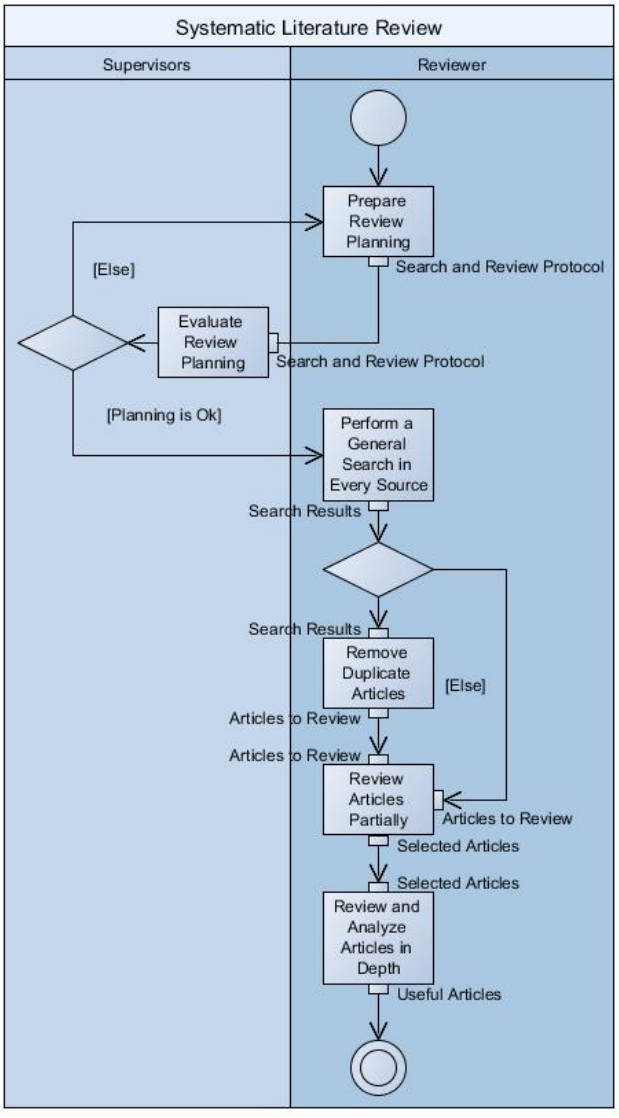

Fig. 1. Activities taken for the realization of this systematic literature review.

2.1 Review Planning

The objective of this SLR was to identify the most used criteria for comparing and selecting authentication schemes and methods. Moreover, in order to ascertain the existing research on this area, existing authentication schemes and methods proposed in literature are reviewed. Thus, the following research questions (RQ) were formulated:

RQ1. What authentication schemes (single-factor authentication) exist in literature?

RQ2. What multi-factor authentication methods that combine these schemes can be found?

RQ3. What criteria can be used to compare and/or to select between authentication schemes and/or multi-factor authentication methods?

RQ4. Are there frameworks that help in the comparison and/or selection of authentication schemes and/or methods? What criteria do they consider?

The following sources, which have a relation with the topic at hand, were used to perform the SLR: Scopus, Science Direct, IEEE, ACM and Springer. Moreover, Google Scholar was used to widen the research in order to obtain potentialy useful articles not indexed in the above sources.

To perform the search in the above sources, the following search terms were defined:

T1. authentication
T2. scheme
T3. method
T4. multi-factor
T5. two-factor
T6. three-factor
T7. comparison
T8. selection
T9. criteria
T10. decision
T11. Framework

Based on these terms, a total of nine different combinations were formulated, as shown in Table 1:

TABLE 1
TERM COMBINATIONS

ID	Combination
C1	T1 and (T2 or T3)
C2	(T4 or T5 or T6) and T1
C3	(T4 or T5 or T6) and T1 and (T2 or T3)
C4	T1 and (T2 or T3) and (T7 or T8 or T9 or T10)
C5	(T4 or T5 or T6) and T1 and (T7 or T8 or T9 or T10)
C6	(T4 or T5 or T6) and T1 and (T2 or T3) and (T7 or T8 or T9 or T10)
C7	T1 and (T2 or T3) and (T7 or T8 or T9 or T10) and T11
C8	(T4 or T5 or T6) and T1 and (T7 or T8 or T9 or T10) and T11
C9	(T4 or T5 or T6) and T1 and (T2 or T3) and (T7 or T8 or T9 or T10) and T11

Some general guidelines were defined as well, such as that for each performed search, the first 200 results had to be reviewed and that the possibility of the appearance of new search terms had to be taken into consideration.

Initially, a partial review was performed in order to obtain potentially useful articles for this research by reading each article's abstract. Every article that was related to any of the defined RQ was included and grouped based on the RQ that they were related to; on the other hand, any article that contained the search terms, but did not have relation to any of the defined RQ was excluded. An in-depth analysis was performed on these articles afterwards as follows: for articles related to RQ1 and RQ2, the

authentication scheme or method, the authentication factor(s) involved and, if mentioned, the target context were identified; for articles related to RQ3 and RQ4, a thorough analysis of each article's proposal, pros and cons, and considered comparison and selection criteria was performed.

2.2 Results

A total of 982 useful articles have been obtained through this SLR. A summary of the accepted articles for every RQ can be seen in Table 2.

TABLE 2
ACCEPTED ARTICLES SPLIT BETWEEN EACH RESEARCH QUESTION

Research Question	Number of Accepted Articles
RQ1	515
RQ2	442
RQ3	17
RQ4	8
Total	982

A list containing the references of all of the accepted articles in this SLR can be found in the supplementary materials (http://colvin.chillan.ubiobio.cl/mcaro/).

The main findings of this SLR, in regards to each RQ, are as shown next.

Authentication Schemes (RQ1)

Most of the found articles belonging to RQ1 focus on the inherence factor, whereas the least do on the knowledge factor. Moreover, 5 articles were found that propose the use of other authentication factors in literature. These factors are that of "someone you know" and "where you are". The number of articles related to each authentication factor can be seen in Fig. 2.

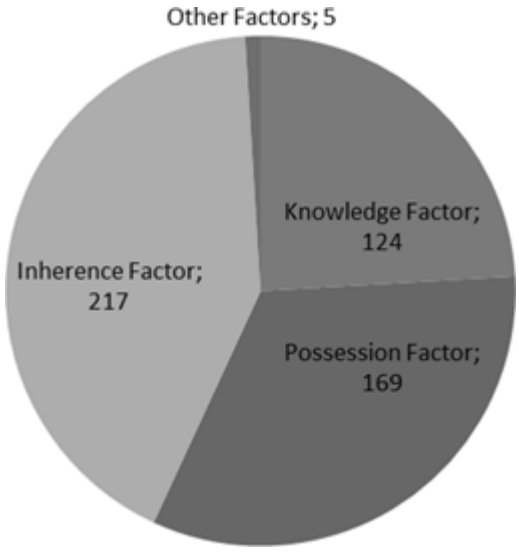

Fig. 2. Authentication schemes found in literature.

Text passwords and graphical passwords are the two knowledge-based authentication schemes with the most related articles (44 and 42, respectively). Smart cards, which belong to the possession factor, are the most proposed authentication scheme, with 103 related articles. There are multiple biometric authentication scheme proposals for the inherence factor, being face recognition and keystroke biometrics the two most proposed, with 24 related articles each.

In order to provide an additional value, the opportunity to identify the contexts for which authentication schemes were proposed the most was taken. These are 1) mobile environment, 2) remote authentication, 3) healthcare and telecare, 4) multi-server environment, 5) continuous authentication and 6) wireless sensor networks.

Although it can be observed that there has been a considerable research on all three well-known authentication factors, some contexts that were expected to be widely studied, such as banking and commerce, were not found as often.

Multi-Factor Authentication Methods (RQ2)

Over 60% of the articles found for RQ2 propose the combination of the knowledge and possession factors. A number of articles were found that proposed dynamic authentication methods based on the situation. Like for RQ1, a total of 5 articles were found that proposed the use of an authentication scheme belonging to other authentication factors in combination with other schemes from among the three well-known factors. In Fig. 3, the number of articles related to each combination of authentication factors is shown.

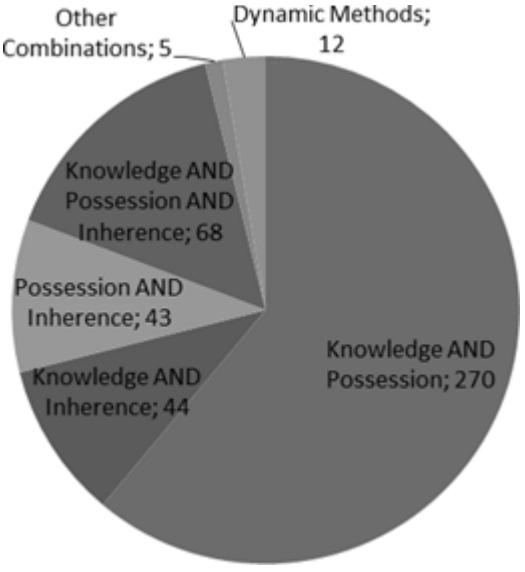

Fig. 3. Multi-Factor Authentication Methods found in literature.

Text passwords and smart cards are the two most used as one of the authentication schemes belonging to the combinations for multi-factor authentication, fol-

lowed by biometrics. In the same manner, the combination of text passwords and smart cards as a two-factor authentication method itself is proposed in 188 of the articles, whereas the combination of these two, together with biometrics, in a three-factor manner, is proposed 47 times. One article proposes the combination of the three well-known factors, together with the factor of "where you are" as a four-factor authentication method.

Like in RQ1, the most commonly found contexts for which multi-factor authentication methods are proposed could be identified. These are 1) remote authentication, 2) healthcare and telecare, 3) wireless sensor networks, 4) multi-server environment, 5) mobile environment and 6) cloud computing.

Similarly to RQ1, the absence of enough research on some contexts can be observed.

Comparison and Selection Criteria (RQ3)

A total of 11 different categories of comparison and selection criteria could be found among the articles related to RQ3. However, seven of these categories were identified only once.

Usability and security are the two most proposed categories of comparison and selection criteria, followed by costs-related criteria. Criteria related to the application's context were found twice, but it can be observed that 13 out of the 17 found articles propose the use of comparison and selection criteria for specific application contexts. The graph in Fig. 4 summarizes the number of articles that propose the use of each comparison and selection criteria. Moreover, Table 2 shows the contexts that are considered in these articles.

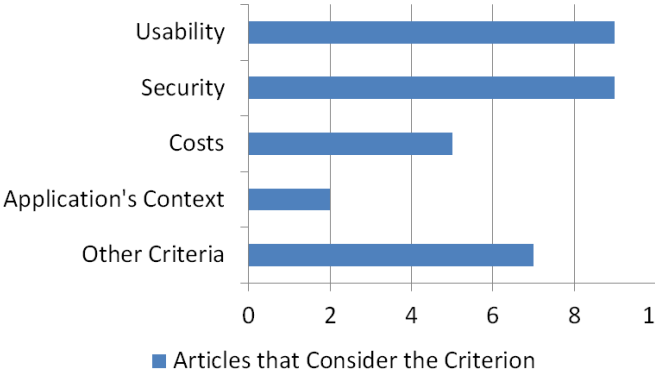

Fig. 4. Comparison and selection criteria for authentication schemes and methods found in literature.

TABLE 2
CONTEXTS CONSIDERED IN ARTICLES REGARDING COMPARISON AND SELECTION CRITERIA

Context	Number of Articles
Banking and Commerce	4
Mobile Environment	3
Cloud Computing	2
Wireless Sensor Networks	2
Remote Authentication	1
Web Applications	1

Although not many articles related to comparison and selection criteria could be found, it is still possible to notice that usability, security and costs are the most commonly used criteria, with an important mention on the importance of the application's context. A further analysis of comparison and selection criteria is performed in Section 3.

Decision Frameworks (RQ4)

A total of eight frameworks that help in the comparison and selection of authentication schemes and methods were found. Table 3 presents the title of each framework, together with the comparison and selection criteria considered by each of them.

TABLE 3
FRAMEWORKS THAT HELP IN THE DECISION OF AUTHENTICATION SCHEMES AND METHODS

Article Title	Considered Criteria
A criteria-based evaluation framework for authentication schemes in IMS [30]	Based in three primary criteria (Security, Ease of Use, and Simplicity) and three secondary criteria (Awareness, Usability and Algorithms). Considers users' perceptions as well.
A Framework for Choosing Your Next Generation Authentication/Authorization System [31]	Only evaluates based on pros and cons.
Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA) [32]	Selects considering the Context and Stakeholders' Requirements.
Cost and benefit analysis of authentication systems [33]	Analyses in relation to Costs.
Efficiency of Paid Authentication Methods for Mobile Devices [34]	Security, Convenience and Operation Costs are considered.
The quest to replace passwords: A framework for comparative evaluation of web authentication schemes [35]	Analyses in terms of Security, Usability and Deployability.
The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes [36]	Compares in regards to Desirable Attributes, Security Requirements and Efficiency
User-centred authentication feature framework [37]	Evaluates in regards to features related to Persuasion, Memory, Input and Output and Obfuscation

Most of the found decision frameworks either do not consider multi-factor authentication or consider it only partially. Neither framework performs a sufficently detailed analysis of both authentication schemes and multi-factor authentication methods.

3 Comparison and Selection Criteria

The most recurrent comparison and selection criteria found in literature were analyzed and filtered in order to obtain a list of criteria that could be used in most situations to analyze authentication schemes and multi-factor authentication methods. Moreover, different importance levels have been assigned to each of these criteria, in order to facilitate the comparison and selection process.

As it could be observed for RQ3 in Section 2.2, usability, securtity and costs are the three most used categories for comparison and selection criteria. As such, these three were used to categorize the criteria selected in this research.

Usability-related criteria were taken from [30], [35], [38], [39], [40], [41] and [42], whereas those related to security were taken from [1], [3], [30], [35], [36], [39], [40] and [43], and of costs from [3], [33], [35], [41] and [42].

Sections 3.1, 3.2 and 3.3 present the usability, security and costs criteria, respectively, considered by this research. In Section 3.4, further considerations on other possible comparison and selection criteria are given.

3.1 Usability Criteria

Usability criteria are related to the perception of end-users about the complexity of different aspects of the the authentication scheme or method. The considered usability criteria for this research are:

1. Ease of Use: Complexity presented by the actions to be performed by the user at the moment of authentication. Three importance levels have been considered for this criterion, namely 1) that the scheme or method *necessarily* needs to be easy to use, 2) that the scheme or method *preferably* needs to be easy to use and 3) that it is *not necessary* for the method to be easy to use.
2. Ease of Learning: Average time that takes for a user to get used to using the authentication method. Three importance levels have been considered for this criterion, namely 1) that a user should take no longer than *a day* to get used to the scheme or method, 2) that a user should take no longer than *a week* to get used and 3) that the time that it takes to get used is *not relevant*.
3. Authentication Information Recovery: Complexity presented for the user to recover his authentication information, in case that he loses or forgets it. Two importance levels have been considered for this criterion, namely 1) that the authentication information recovery process should be *simple* and 2) that the process should be *complex*.
4. Need of Using a Device: How acceptable it is that the user needs to carry a device, be it either a possession device (something unique) or a biometric device (that allows them to demonstrate their inherence information). Three importance levels have been considered for this criterion, namely 1) that the scheme or method does *not* need the use of a device, 2) that the scheme or method can use a possession *or* a biometric device (only one) and 3) that the scheme or method can use both a possession *and* a biometric device.
5. Authentication Method's Reliability: Acceptable recurrence in which the authentication method can give false negatives (that it doesn't recognize the user's authentication information and doesn't allow them access, even though the submitted information is correct, forcing them to try again). Four importance levels are considered for this criterion, namely 1) that the scheme or method should *never or hardly fail* to recognize the user during authentication, 2) that the scheme or method should *not fail occasionally* during authentication, 3) that the scheme or method *can fail occasionally* during authentication and 4) that it *does not matter* how often the scheme or method fails to recognize the user.

3.2 Security Criteria

Security criteria are related to, as the name implies, security aspects of the application and its importance. The considered security criteria for this research are:

1. Importance of Security: Overall appreciation of the development team about the importance of security in the application, according to the information that has been specified either by the client or by the development team themselves. Three importance levels are considered for this criterion, namely 1) that security is a *crucial* aspect for the application, 2) that security is an *important* aspect for the application and 3) that security is a *secondary* aspect for the application.
2. Information Sensitivity: Information with which the application will work and sensitivity level that it possesses. Four importance levels have been considered for this criterion, namely 1) that there is sensitive information for the *company* and the *user*, 2) that there is sensitive information for the *company*, 3) that there is sensitive information for the *user* and 4) that there is *no* sensitive information.
3. Resistance to Observation from Third Parties: That the method is usable in environments where people that could be observing the users upon authentication time exist. Two importance levels are considered for this criterion, namely 1) that the method *should* be resistant and 2) that the method does *not* need to be resistant.
4. Resistance to Phishing: That it is difficult for an attacker to discern a user's authentication information, even if they acquire knowledge related to it through applying social engineering to the user. Two importance levels are considered for this criterion, namely 1) that the method *should* be resistant and 2) that the method does *not* need to be resistant.
5. Resistance to Replay Attacks: That the cost of trying to obtain a user's authentication information through brute force or replay attacks is higher than the profit that an attacker can obtain if they manage to obtain said information. Two im-

portance levels are considered for this criterion, namely 1) that the method *should* be resistant and 2) that the method does *not* need to be resistant.

3.3 Costs Criteria

Costs criteria are related to monetary aspects of the application and how much can be assigned to authentication. The considered costs criteria for this research are:

1. Implementation Costs: The monetary value that the client or the development team is willing to invest for the implementation of security and authentication aspects in the application to be developed. Three importance levels have been considered for this criterion, namely 1) that implementation costs should not be over *10%* of the budget, 2) that implementation costs should not be over *30%* of the budget and 3) that there can be any implementation costs *regardless* of the budget.
2. Costs per User: Willingness of the client or the development team to incur in additional costs for each user that registers in the application, be it either due to the need of delivering authentication devices or any other motive. Two importance levels have been considered for this criterion, namely 1) that the method should *not* present additional costs for each user and 2) that the method *can* present additional costs for each user.

3.4 Further Considerations

The above criteria are considered in order to allow the comparison and selection of authentication schemes and methods in as many contexts as possible. Nevertheless, some additional criteria, which could possibly not be applied to every case, can be considered, such as criteria related to specific applications, like "server compatibility" and "technology availability".

Additional costs-related criteria could be considered, namely the "need to acquire licenses", or human resources and time. However, it can be observed that ultimately all of these can be considered as implementation costs, so it was decided to keep a criterion that includes all of the implementation costs in the list.

Finally, it is important to mention the importance that could be implicitly observed in regards to the application's context as a criterion for comparing and selecting authentication schemes and methods. Thus, it would be desirable to consider the application's context as an additional aspect for performing a comparison and selection.

In order to provide insight on this topic, the most common contexts for which authentication schemes and methods, together with the respective comparison and selection criteria, have been identified. These contexts are Mobile Environment, Remote Authentication, Multi-Server Environment, Cloud Computing, Healthcare and Telecare, Wireless Sensor Networks and Banking and Commerce.

4 Conclusions

This article aims to help covering a gap that has been observed in literature, which is that of the lack of enough research in regards to comparison and selection criteria for authentication schemes and multi-factor authentication methods.

Through the realization of the SLR, it could be observed that there has been a vast research over authentication schemes and methods, but that only a total of 25 articles could be found that cover comparison and selection criteria or decision frameworks for these schemes and methods. Moreover, none of these frameworks allows evaluating both single-factor authentication schemes and multi-factor authentication methods in every situation. Regardless, recurrent comparison and selection criteria could be identified, which allowed to generate a list of common criteria that can be used to decide what authentication scheme or method to use.

The objective of the proposed list of comparison and selection criteria for authentication schemes and methods is to help in this decision-making process, and to provide the groundwork for the creation of a framework that could make use of them in order to provide an adequate analysis of both single-factor authentication schemes and multi-factor authentication methods.

4.1 Future Work

A number of activities can be listed as future work for this research, such as:

1. To create a decision framework that uses these criteria in order to properly help in the comparison and selection of authentication schemes and methods.
2. To analyze the use of the application's context as a complementary factor for deciding what authentication scheme or method to implement in a specific application.
3. To identify a method for scoring the proposed importance levels of each criteria in order to determine a value to each of them. It could be possible to weight each critieria differently as well, and this information could be used as part of the decision framework considered as future work above.
4. To validate the findings in this research. This could be done through the use of the case study methodology over existing applications in the industry.

Acknowledgments

This research is part of the following projects: DIUBB 144319 2/R and BuPERG (DIUBB 152419 G/EF).

REFERENCES

[1] R. Madhusudhan and R. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review," *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1235-1248, 2012.

[2] W. Jansen, "Authenticating users on handheld devices," in *Proceedings of the Canadian Information Technology Security Symposium*, 2003, pp. 1-12.

[3] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021-2040, 2003.

[4] C. Rathgeb and A. Uhl, "Two-factor authentication or how to potentially counterfeit experimental results in biometric systems," *Image Analysis and Recognition*, pp. 296-305, 2010.

[5] H. Al-Assam, H. Sellahewa, and S. Jassim, "On security of multi-factor biometric authentication," in *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*, 2010, pp. 1-6: IEEE.

[6] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 8, pp. 1390-1397, 2011.

[7] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 168-178: ACM.

[8] S. Choi and D. Zage, "Addressing insider threat using "where you are" as fourth factor authentication," in *Security Technology (ICCST), 2012 IEEE International Carnahan Conference on*, 2012, pp. 147-153: IEEE.

[9] S. H. Islam and G. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," *Mathematical and Computer Modelling*, vol. 57, no. 11, pp. 2703-2717, 2013.

[10] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646-1656, 2012.

[11] S.-Q. Wang, J.-Y. Wang, and Y.-Z. Li, "The Web Security Password Authentication based the Single-Block Hash Function," *IERI Procedia*, vol. 4, pp. 2-7, 2013.

[12] M. Mihajlov and B. Jerman-Blažič, "On designing usable and secure recognition-based graphical authentication mechanisms," *Interacting with Computers*, vol. 23, no. 6, pp. 582-593, 2011.

[13] M. S. Umar and M. Q. Rafiq, "Select-to-Spawn: A novel recognition-based graphical user authentication scheme," in *Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on*, 2012, pp. 1-5: IEEE.

[14] Z. Li, Q. Sun, Y. Lian, and D. D. Giusto, "A secure image-based authentication scheme for mobile devices," in *International Conference on Intelligent Computing*, 2005, pp. 751-760: Springer.

[15] K. C. Shin and K. J. Oh, "Smartcard-Based Remote Authentication Scheme Preserving User Anonymity," *Journal of Information Processing and Management*, vol. 4, no. 2, pp. 10-18, 2013.

[16] Z.-Y. Cheng, Y. Liu, C.-C. Chang, and S.-C. Chang, "A smart card based authentication scheme for remote user login and verification," *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 8, pp. 5499-5511, 2012.

[17] W. Jeon, Y. Lee, and D. Won, "An efficient user authentication scheme with smart cards for wireless communications," *International Journal of Security & Its Applications*, vol. 7, no. 4, pp. 1-5, 2013.

[18] H. Imtiaz and S. A. Fattah, "A face recognition scheme using wavelet-based local features," in *Computers & Informatics (ISCI), 2011 IEEE Symposium on*, 2011, pp. 313-316: IEEE.

[19] P. Wang, C.-C. Ku, and T. C. Wang, "A new fingerprint authentication scheme based on secret-splitting for enhanced cloud security," *Recent Application in Bio-metrics*, pp. 183-96, 2011.

[20] X. Wang, F. Guo, and J.-F. Ma, "User authentication via keystroke dynamics based on difference subspace and slope correlation degree," *Digital Signal Processing*, vol. 22, no. 5, pp. 707-712, 2012.

[21] G. Yang, D. S. Wong, H. Wang, and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," *Journal of Computer and System Sciences*, vol. 74, no. 7, pp. 1160-1172, 2008.

[22] T. CAO and S. HUANG, "Two-factor Authentication Schemes Based Smart Card and Password with User Anonymity⋆," *Journal of Computational Information Systems*, vol. 9, no. 21, pp. 8831-8838, 2013.

[23] J. Kang, D. Nyang, and K. Lee, "Two-factor face authentication using matrix permutation transformation and a user password," *Information Sciences*, vol. 269, pp. 1-20, 2014.

[24] Y. Zheng, J. Xia, and D. He, "Trusted user authentication scheme combining password with fingerprint for mobile devices," in *Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on*, 2008, pp. 1-8: IEEE.

[25] H. Tang, Z. Zhu, Z. Gao, and Y. Li, "A secure biometric-based authentication scheme using smart card," in *Cyberspace Technology (CCT 2013), International Conference on*, 2013, pp. 39-43: IET.

[26] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication," in *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, 2003, pp. 45-52: ACM.

[27] M. Zhang, J. Zhang, and Y. Zhang, "Remote three-factor authentication scheme based on Fuzzy extractors," *Security and Communication Networks*, vol. 8, no. 4, pp. 682-693, 2015.

[28] J. Yu, G. Wang, Y. Mu, and W. Gao, "An efficient generic framework for three-factor authentication with provably secure instantiation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2302-2313, 2014.

[29] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, no. 2004, pp. 1-26, 2004.

[30] C. Eliasson, M. Fiedler, and I. Jørstad, "A criteria-based evaluation framework for authentication schemes in IMS," in *Availability, Reliability and Security, 2009. ARES'09. International Conference on*, 2009, pp. 865-869: IEEE.

[31] M. D. Guel, "A Framework for Choosing Your Next Generation Authentication/Authorization System," *Information Security Technical Report*, vol. 7, no. 1, pp. 63-78, 2002.

[32] A. J. Palmer, "Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA)," *computers & security*, vol. 29, no. 7, pp. 785-806, 2010.

[33] K. Altinkemer and T. Wang, "Cost and benefit analysis of authentication systems," *Decision Support Systems*, vol. 51, no. 3, pp. 394-404, 2011.

[34] J. Y. Kim, "Efficiency of Paid Authentication Methods for Mobile Devices," *Wireless Personal Communications*, pp. 1-9.

[35] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Security and Privacy (SP), 2012 IEEE Symposium on*, 2012, pp. 553-567: IEEE.

[36] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, pp. 475-486: ACM.

[37] A. Forget, S. Chiasson, and R. Biddle, "User-centred authentication feature framework," *Information & Computer Security*, vol. 23, no. 5, pp. 497-515, 2015.

[38] M. Anwar and A. Imran, "A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication," in *MAICS*, 2015, pp. 13-18.

[39] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks*, vol. 27, pp. 159-194, 2015.

[40] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 61, pp. 59-80, 2016.

[41] M. Zviran and Z. Erlich, "Identification and authentication: technology and implementation issues," *Communications of the Association for Information Systems*, vol. 17, no. 1, p. 4, 2006.

[42] K. C. Park, J. W. Shin, and B. G. Lee, "Analysis of Authentication Methods for Smartphone Banking Service using ANP," *TIIS*, vol. 8, no. 6, pp. 2087-2103, 2014.

[43] S. Choksi, "Comparative Study on Authentication Schemes for Cloud Computing," *International Journal of Engineering Development and Research*, vol. 2, no. 2, 2014.