Information and Software Technology 94 (2018) 30–37

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof

Authentication schemes and methods: A systematic literature review

Ignacio Velásquez, Angélica Caro*, Alfonso Rodríguez

Computer Science and Information Technologies Department, University of Bío-Bío, Chillán, Chile

ARTICLE INFO

Keywords:
Security
Authentication scheme
Multi-factor authentication method
Systematic literature review

ABSTRACT

Context: There is a great variety of techniques for performing authentication, like the use of text passwords or smart cards. Some techniques combine others into one, which is known as multi-factor authentication. There is an interest in knowing existing authentication techniques, including those aimed at multi-factor authentication, and the frameworks that can be found in literature that are used to compare and select these techniques according to different criteria.

Objective: This article aims to gather the existing knowledge on authentication techniques and ways to discern the most effective ones for different contexts.

Method: A systematic literature review is performed in order to gather existing authentication techniques proposed in literature and ways to compare and select them in different contexts. A total of 515 single-factor and 442 multi-factor authentication techniques have been found. Furthermore, 17 articles regarding comparison and selection criteria for authentication techniques and 8 frameworks that help in such a task are discussed.

Results: A great variety of single-factor techniques has been found and smart card-based authentication was shown to be the most researched technique. Similarly, multi-factor techniques combine the different single-factor techniques found and the combination of text-passwords and smart cards is the most researched technique. Usability, security and costs are the most used criteria for comparing and selecting authentication schemes, whereas the context is given an important remark as well. No framework among the ones found analyzed in detail both single-factor and multi-factor authentication techniques for the decision-making process.

Conclusion: The review shows that a vast research has been done for authentication techniques, although its use in some contexts has not been researched as much. The lack of works regarding the comparison and selection of authentication techniques is observed.

1. Introduction

One of the most serious security threats to any computing device is impersonation of an authorized user. User authentication is the first line of defense against this threat [1], and is a central component of any security infrastructure [2]. Authentication is the process of positively verifying a user's identity, device or other entity in a computer system, often as a prerequisite to allowing access to resources in the system [3].

An authentication factor is a piece of information used to authenticate or verify the identity of a user [4]. These factors can be categorized in three groups [17,18]: those based on the knowledge factor (what the client knows, like text passwords [5–7] or graphical passwords [8–10]), those based on the possession factor (what the client owns, dependent of a physical possession, like smart cards [11–13]) and those based on the inherence factor (who the client is, biometrics, like face recognition [14], fingerprints [15] and keystroke dynamics [16]). Although there are other factors proposed in literature, such as the use of a person's social networks [19] and location-based authentication [20], the three above are the most used and well-known factors.

Authentication techniques belonging to different factors can be combined to enhance security, which is known as multi-factor authentication [3]. Some examples of multi-factor authentication are the combination of the knowledge and possession factors [21,22], the combination of the knowledge and 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]. In this article, authentication techniques that belong to a single authentication factor will be referred to as authentication schemes, whereas combinations of techniques from different factors will be referred to as multi-factor authentication methods.

A Systematic Literature Review (SLR) is performed to analyze existing frameworks that help in the decision process for choosing the adequate authentication schemes or methods for different use contexts, together with identifying the most used criteria for this comparison and

* Corresponding author.
E-mail addresses: ivelasqu@alumnos.ubiobio.cl (I. Velásquez), mcaro@ubiobio.cl (A. Caro), alfonso@ubiobio.cl (A. Rodríguez).

http://dx.doi.org/10.1016/j.infsof.2017.09.012
Received 14 September 2016; Received in revised form 5 July 2017; Accepted 25 September 2017
Available online 29 September 2017
0950-5849/

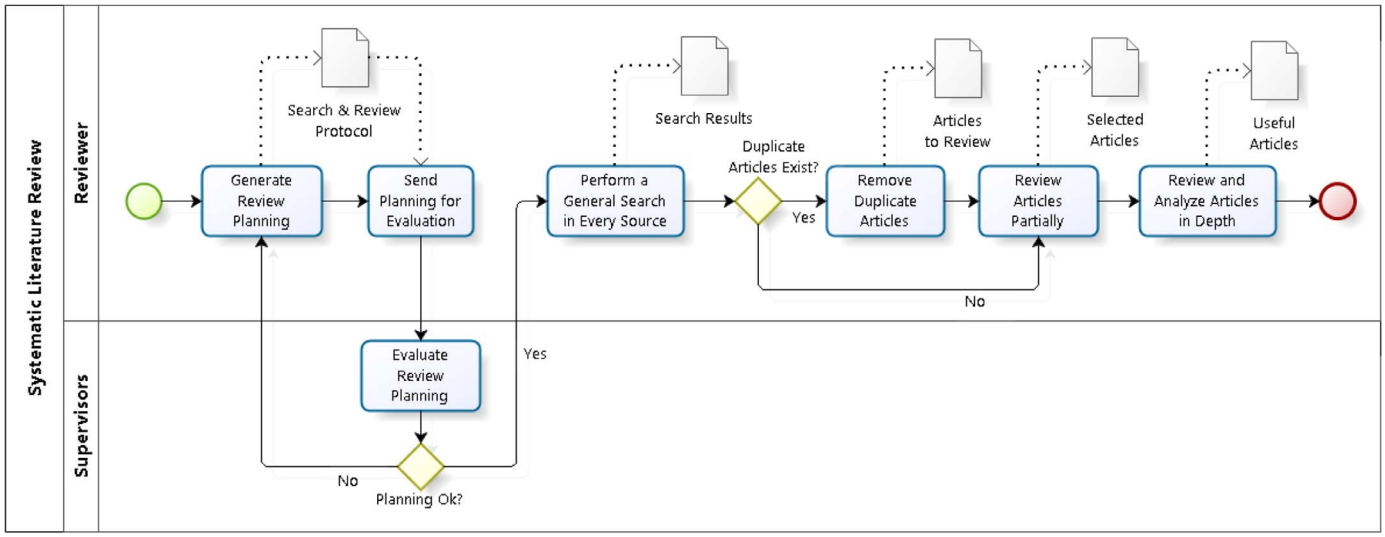

Fig. 1. Systematic literature review process applied in this research.

selection. This information could be useful for industry experts when faced with the job of selecting the most adequate authentication schemes or methods for their applications. Additionally, a detailed review of existing authentication schemes and multi-factor authentication methods is performed, in order to know the current research that has been done in this area.

The remainder of the article is organized as follows: Section 2 explains the used research methodology. In Section 3, the whole planning process of the SLR is presented, whereas its results are shown in Section 4, and a discussion about the main findings of the review is given in Section 5. Section 6 provides the article's conclusions.

2. Research methodology

A systematic literature review, based on Barbara Kitchenham's method [29], was performed in order to survey the existing knowledge about the topic of this article. The SLR process applied in this research can be seen in Fig. 1.

First, a planning of the review was performed from which, together with the identification of the need for research, the search and review protocols to be used were obtained. Two supervisors analyzed this planning to evaluate its adequacy. Afterwards, a general search was performed in different sources as specified by the review planning. From the search's results, the duplicate articles were removed, and a partial review was performed on the remaining articles, obtaining a list of selected articles that were potentially useful. The selected articles were reviewed and analyzed in depth and the list with useful articles for this research was obtained. The details of the review planning are specified in Section 3, whereas the results from performing the search and review process can be found in Section 4.

3. Review planning

The identification of the need for research, together with the search and review protocols used for the SLR are specified as follows:

3.1. Identification of the need for research

The review's objective was to identify authentication schemes proposed in literature and possible combinations of them for their use as multi-factor authentication methods, while also detecting criteria used for their comparison and selection and the existence of frameworks that handle such a task. Based on this objective, the following Questions (Q) were formulated to further define the need of investigation:

Q1. Which are the main authentication schemes that exist in the literature?
Q2. What combinations of these schemes can be found that can be used as multi-factor authentication methods?
Q3. What criteria can be used to compare and/or to select between authentication schemes or multi-factor authentication methods?
Q4. Are there frameworks that help to compare and/or to select authentication schemes or multi-factor authentication methods? What are their characteristics?

3.2. Resources for performing the systematic literature review

In order to perform the SLR, sources that are related to the topic at hand were used, specifically, Scopus (https://www.scopus.com/), Science Direct (http://www.sciencedirect.com/), IEEE (http://ieeexplore.ieee.org/Xplore/home.jsp), ACM (http://dl.acm.org/) and Springer (http://link.springer.com/).

Additionally, Google Scholar (https://scholar.google.com/) was used to deepen in the research for those potentially useful publications not indexed in the previously mentioned sources.

3.3. Search protocol

This defines the protocol that was used for performing the search in the sources defined above. Thus, the Terms (T) used for the review, as well as their Combinations (C) were defined (see Table 1).

Some general guides for the realization of the search in accordance to each of the resources specified above were defined, between them:

- In some cases, the search terms can be entered in an escalated way, restricting the results of a previous search.
- For each performed search, the first 200 results must be reviewed.
- If the search results have restricted access, the document must be searched for in alternate ways (for example, in the authors' personal sites).
- The possibility of the appearance of new terms or concepts that could help to find works of interest must be taken in consideration.

An online reference manager was used to facilitate the recording of the search results and their source. Moreover, the results of each search were recorded in a table containing the source, the combination of terms, the number of found articles and the search date for each search. For every entry in the previously described table, another table was used to record every reviewed article's reference, their acceptance or

Table 1
Terms and combinations used to perform the SLR.

Terms	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
Combinations	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			

rejection, a brief description explaining the motive of acceptance or rejection and the acceptance topic to which they belong.

3.4. Review protocol

A partial review was performed in order to obtain potentially useful articles for the research. For reviewing every article in this step, the abstract of each one was read. If needed, their introduction and conclusions were also read, while on some specific cases part of the article's body was read as well. Once every reading had been made, the decision to include or not the article as a potentially useful article was done, in accordance to this protocol's criteria. A control on the accepted and rejected articles was kept by using the tables described above.

Every article that was related to any of the following Acceptance Topics (AT), each related to one of the research questions formulated above, was included:

AT1. Authentication schemes.
AT2. Multi-factor authentication methods.
AT3. Comparison and selection criteria for authentication schemes or multi-factor authentication methods.
AT4. Frameworks that support the decision of authentication schemes or multi-factor authentication methods.

On the other hand, any article that contained the search terms or combinations of them, but did not contain relevant information on the topic at hand, was excluded.

An in-depth analysis of these potential articles was performed afterwards, according to the acceptance topic of each article. For the articles in AT1 and AT2, the authentication scheme or method, together with the authentication factor to which they belong and (if mentioned) the context that the scheme or method was proposed for were identified. A thorough analysis of the articles in AT3 and AT4 was realized, in order to adequately understand their proposals and to identify their pros and cons, emphasizing the criteria used in each one.

The information of the accepted articles was extracted, synthetized and stored in a table according to their acceptance topic. For authentication schemes, the reference, the proposed scheme, the authentication factor to which they belong and a brief description were stored. For multi-factor authentication methods, the reference, the combined factors, the specific schemes and a brief description were stored. For the comparison and selection criteria, the reference, the used criteria and a brief description were stored. Finally, for the decision frameworks, the reference, a brief description and observed strengths and weaknesses were stored.

4. Results

A search was performed for every combination of terms in every source specified in the search protocol, in total 54 different searches were done. For each search, 200 publications were reviewed. However 15 of these yielded less than 200 results and, among them, 5 yielded no results. This way, a total of 8153 articles were reviewed.

In order to improve the obtained results, some extra refinements were made on some of the sources: in Scopus, the subject area was limited to Computer Science, whereas in Springer the content type was refined to article and in Google Scholar patents and citations were excluded.

Out of the 8153 articles, those that were repeated were eliminated, obtaining a total of 3910 different articles. After a superficial review, 1015 of them were considered potentially useful articles. A detailed analysis was performed afterwards, and it was noticed that 33 of the potential articles were not relevant for the current research, so they were discarded, leaving a total of 982 useful and accepted articles, split between the four acceptance topics as shown in Table 2.

A list containing all of the references for the accepted articles in this SLR can be found in the supplementary materials (http://colvin.chillan.ubiobio.cl/mcaro/). The remainder of this section shows the analysis of the useful articles according to each acceptance topic.

4.1. Authentication schemes (AT1)

Over 50% of the accepted articles, 515, belong to AT1. The reason for it could be that authentication schemes are the base for the topics discussed in AT2, AT3 and AT4, so they have been addressed more often in literature. As for the results, 217 of the articles focus on the proposal of schemes pertaining to the inherence factor, whereas 169 propose the use of the possession factor and 124 the knowledge factor. The remaining 5 articles are related to other authentication factors that have been proposed in literature. Table 3 presents the authentication scheme proposals found in literature, the factor to which they belong and the number of articles that propose each of them.

The text passwords scheme, the most widely used scheme nowadays [30], is the authentication scheme that belongs to the knowledge factor with the most related articles (44), followed by the graphical passwords scheme, with 42 articles. On the other hand, the vast majority of proposals regarding to the possession factor are related to the use of smart cards, with 103 out of 169 articles, which corresponds to 60.1% of them. There are many different articles related to the use of biometrics for the inherence factor, although 48 of those do not define a specific biometric for their proposal, and 13 others only mention the use of behavioral biometrics but not a particular one.

Table 2
Accepted articles split between each acceptance topic.

Acceptance Topic	Number of accepted articles
AT1	515
AT2	442
AT3	17
AT4	8
Total	982

Table 3
Authentication schemes found in literature.

Factor	Scheme	Number of Articles
Knowledge	Text passwords	44
	Graphical passwords	42
	Cognitive authentication	25
	Personal Identification Number (PIN)	7
	Questions	4
	Other knowledge-based schemes	2
	Total	124
Possession	ID-based (Smart Cards)	103
	One Time Password (OTP) tokens	43
	Mobile-based	21
	Other possession-based schemes	2
	Total	169
Inherence	Face biometrics	24
	Keystroke biometrics	24
	Hand gestures	12
	Palmprint biometrics	12
	Touchstroke biometrics	11
	Fingerprints	10
	Iris biometrics	8
	Brainwaves	5
	Heartbeats	5
	Knuckleprint biometrics	5
	Gait biometrics	4
	Multi-modal biometrics	19
	Other biometrics	17
	Behavioral biometrics (undefined)	13
	Biometrics (undefined)	48
	Total	217
Other Factors		5
	Grand total	515

Most of the articles found have been published from 2000 onwards (505) and only 10 where published before. An increasing interest in the topic of authentication schemes can be noticed, as the number of articles related to it has been increasing over the years, with the exception of 2012, which has a notorious decrease in research compared to its prior year. 2015 is the year with the most publications related to authentication schemes, with 82 articles, whereas 2001 has the least, with only one. The oldest accepted article dates to 1974 [31], and proposes the use of text passwords. No article prior to 2000 discusses the use of schemes related to the possession factor. The graphic in Fig. 2 shows the accepted articles and the authentication factor to which they belong, split per year. It is important to mention that this review was performed between the second and third quarters of 2016, so not all of the articles of this year are present.

The context for which every authentication scheme was proposed was recorded. The mobile environment was the most common context, followed by remote authentication and healthcare/telecare. It is important to mention that more than half of the articles, 282, did not specify a particular context for their proposal. The different contexts that have been found can be seen in Table 4, along with how many schemes for each authentication factor are proposed in each of them.

Table 4
Authentication factors and their contexts.

Factor	Knowledge	Possession	Inherence	Other factors	Total
Context					
Mobile environment and touch screens	24	16	41	0	81
Remote authentication	4	33	5	0	42
Healthcare/Telecare	0	13	11	0	24
Multi server environment	2	9	6	0	17
Continuous authentication	0	0	11	0	11
Wireless sensor networks	2	7	1	0	10
Cloud computing	1	6	2	0	9
Banking and commerce	2	4	2	0	8
Smart environment	0	6	1	0	7
Session initiation protocol	1	2	2	0	5
Web applications	2	1	1	1	5
Other contexts	4	6	4	0	14
Not specified	82	66	130	4	282
Total	124	169	217	5	515

4.2. Multi-Factor authentication methods (AT2)

For the AT2, 442 articles were found. Most of the accepted articles correspond to proposals of methods that combine schemes from the knowledge and possession factors, adding up to 270 articles, which corresponds to over 60% of the articles. There are 44 proposals that combine the knowledge and inherence factors and 43 that combine the possession and inherence factors. On the other hand, 68 proposals combine the three factors. Twelve articles were found that did not propose a specific combination of factors, but rather proposed the use of different factors according to different situations. Similar to AT1, 5 articles were found that proposed multi-factor authentication methods whose factor combinations included a factor proposed in literature that was not among the three well-known ones. Table 5 presents the multi-factor authentication method proposals found in literature, the

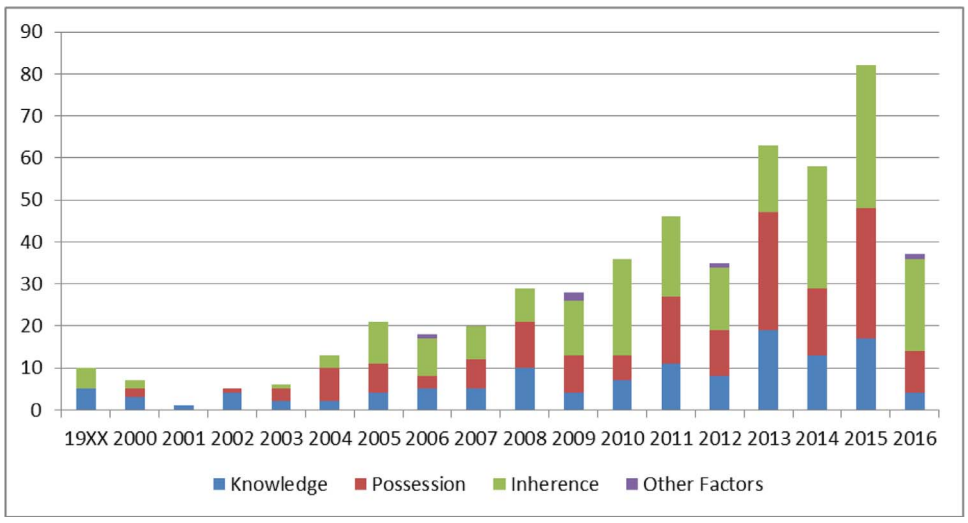

Fig. 2. Authentication factors according to publication year.

Table 5
Multi-factor authentication methods found in literature.

Combination	Method	Number of articles
Knowledge AND Possession	Text passwords AND ID-based	188
	Text passwords AND mobile-based	37
	Text passwords AND OTP	34
	Other methods	11
	Total	270
Knowledge AND Inherence	Text passwords AND biometrics	36
	Graphical passwords AND biometrics	4
	Other methods	4
	Total	44
Possession AND Inherence	ID-based AND biometrics	24
	OTP AND biometrics	9
	Mobile-based AND biometrics	6
	Other methods	4
	Total	43
Knowledge AND Possession AND Inherence	Text passwords AND ID-based AND biometrics	47
	Text passwords AND OTP AND biometrics	9
	Text passwords AND Mobile-based AND biometrics	7
	Other methods	5
	Total	68
Other combinations		5
Dynamic methods		12
	Grand total	442

combination of factors to which they belong and the number of articles that propose each of them.

The combination of text passwords and smart cards (ID-Based) is by far the one with most number of articles, with a total of 188 (69.4%) of the articles combining the knowledge and possession factors. Either text passwords and/or smart cards are seen as the most used schemes together with biometrics for every other combination of factors as well, highlighting the vast amount of research given to multi-factor authentication methods based on these schemes.

Similar to AT1, an increasing interest in the topic of multi-factor authentication can be seen, with the difference that there are no significant drops in the number of articles in any specific year. There are only 6 articles prior to 2000, and all of them propose the use of a combination between the knowledge and possession factors. Again, 2015 is the year with the most publications, 81. No articles were accepted that were published during 2000, and the oldest accepted article dates to 1991 [32]. The graphic in Fig. 3 presents the accepted articles and the combination of authentication factors to which they belong, split per year. Remind that this review was performed between the second and third quarters of 2016, so not all of the articles of said year are present.

The context for which every multi-factor authentication method was proposed was recorded as well. As opposed to authentication schemes, only a 38.7% of them did not mention the context for which they were proposed. Remote authentication and healthcare/telecare are the two most recurrent contexts, but unlike for authentication schemes, mobile environment is considerably less discussed. The different contexts that have been found can be seen in Table 6, along with how many methods for each combination of authentication factors are proposed in each of them.

4.3. Comparison and selection criteria (AT3)

Another goal of this review was to identify different selection and comparison criteria used to decide on what authentication scheme or multi-factor authentication method to use in a given situation. 17 articles regarding this topic were found. All of these consider one or more criteria for comparing authentication schemes or methods, being usability and security criteria the two most used, each one addressed in 9 different articles.

Criteria related to the scheme or method's costs are used 5 times, and those regarding the context where the scheme or method will be used are used twice. Other seven criteria, such as future tendencies of the scheme or method or its privacy, are proposed as well among different articles, but each of them is proposed only once. It could be observed that many of the relevant articles proposed the use of two or more of the three most considered criteria [33–35].

Five of the articles consider multi-factor authentication. On the other hand, 13 of them consider a specific context. The contexts considered in these articles can be seen in Fig. 4.

4.4. Decision frameworks (AT4)

Eight decision frameworks have been found that help in the selection and comparison of authentication schemes and/or multi-factor authentication methods. A brief description of each is given through Table 7.

The oldest article found is from 2002 [37]. Most of the authentication scheme and multi-factor authentication method proposals found in this review are from years after this framework's publication, so its contents might be outdated. On the other hand, the most recent article is from 2016 [41], and most scheme and method proposals found are prior to this publication, so its contents are probably up to date.

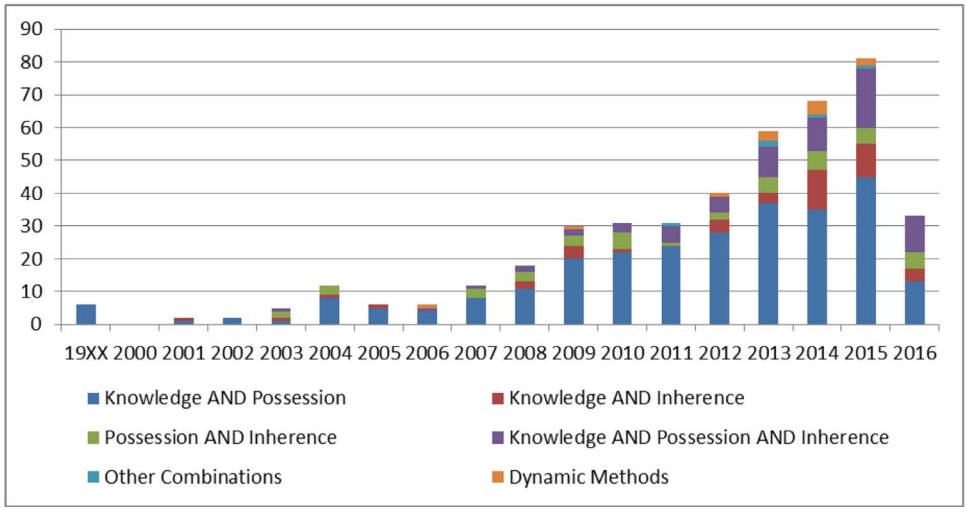

Fig. 3. Multi-factor authentication methods according to publication year.

Table 6
Multi-factor authentication methods and their contexts.

Combinations Context Context	Knowledge AND possession	Knowledge AND inherence	Possession AND inherence	Knowledge AND possession AND inherence	Other combinations	Dynamic	Total
Remote authentication	45	1	8	10	0	0	64
Healthcare/Telecare	29	3	2	14	0	0	48
Wireless sensor networks	28	0	1	4	0	0	33
Multi server environment	18	1	4	6	0	0	29
Mobile environment and touch screens	11	8	0	2	0	0	21
Cloud computing	10	2	1	3	0	1	17
Banking and commerce	8	1	1	0	0	1	11
Web applications	10	1	0	0	0	0	11
Wireless networks	7	0	0	1	0	0	8
USB devices	3	0	0	3	0	0	6
Unsafe environment	4	0	1	0	0	0	5
Other contexts	10	2	3	2	1	1	19
Not specified	87	25	22	23	4	9	170
Total	270	44	43	68	5	12	442

5. Discussion

The main findings and the limitations of this review are discussed here. This review permits us to not only know about the state of the art on authentication schemes and multi-factor authentication methods, but it also serves as a way to identify the principal contexts in which they were proposed and used, while also giving an insight on the criteria used when facing the need to decide on what scheme or method to use in different contexts and the existing frameworks that perform this task.

Among authentication schemes, out of the three well-known authentication factors, the inherence factor is the most researched one, whereas the knowledge factor is the least, perhaps due to the current paradigm that the most representative scheme of this factor (text passwords) is not very secure [30]. Nevertheless, the most reviewed scheme is smart card-based authentication, which belongs to the possession factor. While some contexts were expected to be researched often, like the mobile environment, some others were not identified as often as it was expected, like banking and commerce.

The combination of the knowledge and possession factors is very predominant in multi-factor authentication methods, especially the use of both text passwords and smart cards. Three-factor authentication is the second most researched combination of factors, although it seems to be the less widely applied one [3]. Both text passwords and smart cards are used in 259 articles each, as one of the schemes considered in the combination for multi-factor authentication. The existence of dynamic multi-factor authentication methods [43–45] is interesting, as they adapt to different environments. One multi-factor authentication method that uses four different factors (being the factor related to the user's location the fourth) was found [46].

Not many articles related to comparison and selection criteria or decision frameworks for authentication schemes or methods were found. From the existing ones, the common use of usability, security and cost-related criteria for the comparison and selection was noticed. The context of use is also seen as an important element, as the articles either consider this as one of the decision criteria [47] or the article's proposal itself is directed to a specific context [48,49].

In regards to the decision frameworks, it can be seen that multi-factor authentication is not considered often, whereas proposals that do focus solely in some authentication aspects, leaving others aside. No framework could be found that considered both single-factor and multi-factor authentication, together with enough decision criteria for

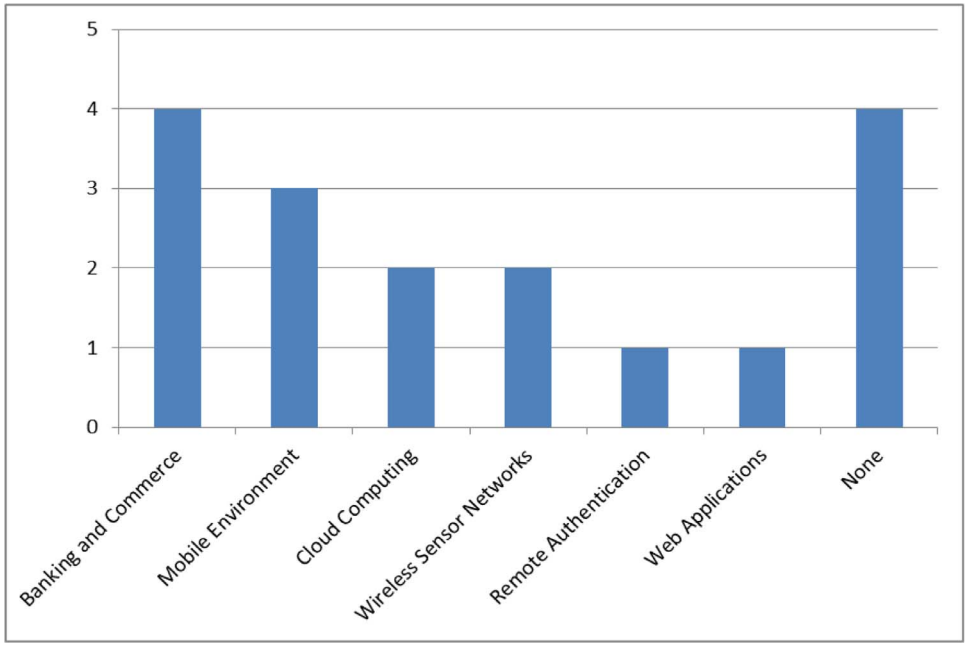

Fig. 4. Contexts considered in articles regarding comparison and selection criteria.

Table 7
Frameworks that help in the decision of authentication schemes or methods.

Article Title	Description
A criteria-based evaluation framework for authentication schemes in IMS [36]	Decision framework for multimedia systems based in three primary criteria (security, ease of use and simplicity) and three secondary criteria (awareness, usability and algorithms), and also considering users' perceptions.
A Framework for choosing your next generation authentication/ Authorization system [37]	Realizes a general evaluation of various authentication schemes in relation to their pros and cons. Also addresses some authorization-related topics.
Approach for selecting the most suitable automated personal identification mechanism (ASMSA) [38]	Supports the selection of the most suitable automated identification from either the knowledge or the inherence factors, considering both the context and stakeholders' requirements.
Cost and benefit analysis of authentication systems [39]	Thorough analysis of authentication schemes and multi-factor authentication methods in relation to cost-related criteria. Thought for its use when a company switches from an authentication scheme or method to another.
Efficiency of paid authentication methods for mobile devices [40]	Surveys system managers about their preferences on paid authentication schemes for the mobile environment. Security, convenience and operation costs are considered.
The quest to replace passwords: a framework for comparative evaluation of web authentication schemes [30]	Thorough analysis of multiple authentication schemes in terms of security, usability and costs. It provides a comparative table that eases the decision-making process. It mentions multi-factor authentication but ever so slightly.
The request for better measurement: a comparative evaluation of two-factor authentication schemes [41]	Compares the multiple existing two-factor authentication scheme proposals using text passwords and smart cards, in regards to their desirable attributes, security requirements and efficiency.
User-centred authentication feature framework [42]	A framework oriented to researchers that evaluates knowledge-based schemes in regards to features related to persuasion, memory, input and output and obfuscation.

realizing a detailed comparison and selection of existing authentication schemes or methods to be used.

The acceptance of the articles for AT1 and AT2 was limited to those that directly proposed a new authentication scheme or an improvement to an existing one. Also, due to time constraints and the number of potentially useful articles in AT1 and AT2, only the relevant information for the review was extracted.

6. Conclusions

The realization of this SLR aimed at investigating the existing decision frameworks and comparison and selection criteria related to authentication schemes and multi-factor authentication methods, together with the existing research on these schemes and methods. Through this review, a total of 982 articles were found that either discussed authentication schemes, multi-factor authentication methods or frameworks and criteria that helped on the comparison and selection of these in different environments. The main findings of this review, in relation to the formulated research questions, are as follows:

Q1. There has been considerable research on all three well-known authentication factors. Text and graphical passwords are the most researched schemes for knowledge-based authentication, whereas there are multiple different biometrics proposals for the inherence factor. The most researched scheme is smart card-based authentication from the possession factor.

Q2. There are many different multi-factor authentication methods that combine the authentication schemes from Q1. There are both combination proposals that consider two factors and others that consider three factors, there's even a proposal that considers four factors (the fourth being location-based authentication). There's a clear prevalence in the use of text passwords and smart cards as one of the schemes used for the different combinations.

Q3. The comparison and selection of different authentication schemes or methods is done primarily through usability and security criteria, with sometimes the consideration of cost-related criteria as well. Although it is not considered as a criterion in the reviewed articles, the context is an important aspect to examine as most studies are presented for specific contexts.

Q4. Eight frameworks that help in the decision of authentication schemes or methods were found. Each framework has its own characteristics, some consider a specific context, some focus on specific schemes of methods and some are more general. No framework that realized a thorough analysis of both authentication schemes and multi-factor authentication methods could be found.

The main purpose of this SLR was to ascertain existing decision frameworks and criteria for the comparison and selection of authentication schemes or methods. However, its results could also be useful for researchers as it can help them to analyze the existing work on the different authentication schemes or methods that have been found through its realization, thus identifying spaces to perform further research on them. Some future work ideas are to research the existing authentication schemes or methods on contexts that have not been widely studied, such as social media, and to evaluate the use of these contexts as a criterion for the comparison and selection of authentication schemes or methods. The definition of a framework that helps in detail to the decision to use authentication schemes and/or multi-factor authentication methods is considered as well.

Acknowledgments

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

References

[1] W. Jansen, Authenticating users on handheld devices, Proceedings of the Canadian Information Technology Security Symposium, 2003, pp. 1–12.
[2] R. Madhusudhan, R.C. Mittal, Dynamic ID-based remote user password authentication schemes using smart cards: a review, J. Netw. Comput. Appl. 35 (2012) 1235–1248.
[3] L. O'Gorman, Comparing passwords, tokens, and biometrics for user authentication, Proc. IEEE 91 (2003) 2021–2040.
[4] C. Rathgeb, A. Uhl, Two-factor authentication or how to potentially counterfeit experimental results in biometric systems, Image Analysis and Recognition, Springer, 2010, pp. 296–305.
[5] S.K. Hafizul Islam, G.P. Biswas, Design of improved password authentication and update scheme based on elliptic curve cryptography, Math. Comput. Modell. 57 (2013) 2703–2717.
[6] A.K. Das, P. Sharma, S. Chatterjee, J.K. Sing, A dynamic password-based user authentication scheme for hierarchical wireless sensor networks, J. Netw. Comput. Appl. 35 (2012) 1646–1656.
[7] S.-Q. Wang, J.-Y. Wang, Y.-Z. Li, The web security password authentication based the single-block hash function, IERI Procedia, 4 2013, pp. 2–7.
[8] M. Mihajlov, B. Jerman-Blažič, On designing usable and secure recognition-based graphical authentication mechanisms, Interact. Comput. 23 (2011) 582–593.
[9] M.S. Umar, M.Q. Rafiq, Select-to-spawn: a novel recognition-based graphical user authentication scheme, In: 2012 IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2012, 2012.
[10] Z. Li, Q. Sun, Y. Lian, D.D. Giusto, A secure image-based authentication scheme for mobile devices, Advances in Intelligent Computing In: Lecture Notes in Computer Science, 2005, pp. 751–760.
[11] K. Cheul Shin, K. Jong Oh, Smartcard-based remote authentication scheme

preserving user anonymity, Int. J. Inf. Process. Manag. 4 (2013) 10–18.
[12] Z.Y. Cheng, Y. Liu, C.C. Chang, S.C. Chang, A smart card based authentication scheme for remote user login and verification, Int. J. Innov. Comput. Inf. Control 8 (2012) 5499–5511.
[13] W. Jeon, Y. Lee, D. Won, An efficient user authentication scheme with smart cards for wireless communications, Int. J. Secur. Appl. 7 (2013) 1–16.
[14] H. Imtiaz, S.A. Fattah, A face recognition scheme using wavelet-based local features, Computers & Informatics (ISCI), 2011 IEEE Symposium on, 2011, pp. 313–316.
[15] P. Wang, C.-C. Ku, T.C. Wang, A new fingerprint authentication scheme based on secret-splitting for enhanced cloud security, Recent Appl. Bio-metrics (2011) 183–196.
[16] X. Wang, F. Guo, J.-f. Ma, User authentication via keystroke dynamics based on difference subspace and slope correlation degree, Dig. Sig. Process. 22 (2012) 707–712.
[17] H. Al-Assam, H. Sellahewa, S. Jassim, On security of multi-factor biometric authentication, Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, IEEE, 2010, pp. 1–6.
[18] X. Huang, Y. Xiang, A. Chonka, J. Zhou, R.H. Deng, A generic framework for three-factor authentication: preserving security and privacy in distributed systems, IEEE Trans. Parallel Distrib. Syst. 22 (2011) 1390–1397.
[19] J. Brainard, A. Juels, R.L. Rivest, M. Szydlo, M. Yung, Fourth-factor authentication: somebody you know, Proceedings of the 13th ACM conference on Computer and Communications Security, ACM, Alexandria, Virginia, USA, 2006.
[20] S. Choi, D. Zage, Addressing insider threat using “where you are” as fourth factor authentication, Security Technology (ICCST), 2012 IEEE International Carnahan Conference on, 2012, pp. 147–153.
[21] G. Yang, D.S. Wong, H. Wang, X. Deng, Two-factor mutual authentication based on smart cards and passwords, J. Comput. Syst. Sci. 74 (2008) 1160–1172.
[22] T. Cao, S. Huang, Two-factor authentication schemes based smart card and password with user anonymity, J. Comput. Inf. Syst. 9 (2013) 8831–8838.
[23] J. Kang, D. Nyang, K. Lee, Two-factor face authentication using matrix permutation transformation and a user password, Inf. Sci. 269 (2014) 1–20.
[24] Z. Yu, X. Jingchun, H. Dake, Trusted user authentication scheme combining password with fingerprint for mobile devices, Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on, 2008, pp. 1–8.
[25] H.B. Tang, Z.J. Zhu, Z.W. Gao, Y. Li, A secure biometric-based authentication scheme using smart card, International Conference on Cyberspace Technology (CCT 2013), 2013, pp. 39–43.
[26] T.C. Clancy, N. Kiyavash, D.J. Lin, Secure smartcardbased fingerprint authentication, Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, ACM, Berkley, California, 2003.
[27] M. Zhang, J. Zhang, Y. Zhang, Remote three-factor authentication scheme based on Fuzzy extractors, Secur. Commun. Netw. 8 (2015) 682–693.
[28] J. Yu, G. Wang, Y. Mu, W. Gao, An efficient generic framework for three-factor authentication with provably secure instantiation, IEEE Trans. Inf. Forensic. Secur. 9 (2014) 2302–2313.
[29] B. Kitchenham, Procedures for Performing Systematic Reviews Joint Technical Report, Keele University, 2004, pp. 1–26. TR/SE-0401 and NICTA 0400011T.1.
[30] J. Bonneau, C. Herley, P.C. Van Oorschot, F. Stajano, The quest to replace passwords: a framework for comparative evaluation of web authentication schemes, Security and Privacy (SP), 2012 IEEE Symposium on, IEEE, 2012, pp. 553–567.
[31] J. Arthur Evans, W. Kantrowitz, E. Weiss, A user authentication scheme not requiring secrecy in the computer, Commun. ACM 17 (1974) 437–442.
[32] C.-C. Chang, T.-C. Wu, Remote password authentication with smart cards, IEEE Proc. E-Comput. Digit. Techniques 138 (1991) 165–168.
[33] K.C. Park, J.W. Shin, B.G. Lee, Analysis of authentication methods for smartphone banking service using ANP, TIIS, 8 2014, pp. 2087–2103.
[34] S. Kumari, M.K. Khan, M. Atiquzzaman, User authentication schemes for wireless sensor networks: a review, Ad Hoc Netw. 27 (2015) 159–194.
[35] S. Kiljan, H. Vranken, M. van Eekelen, Evaluation of transaction authentication methods for online banking, Future Gener. Comput. Syst. (2016).
[36] C. Eliasson, M. Fiedler, I. Jørstad, A criteria-based evaluation framework for authentication schemes in IMS, Proceedings - International Conference on Availability, Reliability and Security, ARES, 2009 2009, pp. 865–869.
[37] M.D. Guel, A framework for choosing your next generation authentication/authorization system, Inf. Secur. Technical Rep. 7 (2002) 63–78.
[38] A.J. Palmer, Approach for selecting the most suitable automated personal identification mechanism (ASMSA), Comput. Secur. 29 (2010) 785–806.
[39] K. Altinkemer, T. Wang, Cost and benefit analysis of authentication systems, Decis. Support Syst. 51 (2011) 394–404.
[40] J.Y. Kim, Efficiency of paid authentication methods for mobile devices, Wirel. Personal Commun. (2016) 1–9.
[41] D. Wang, Q. Gu, H. Cheng, P. Wang, The request for better measurement: a comparative evaluation of two-factor authentication schemes, Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ACM, Xi'an, China, 2016.
[42] A. Forget, S. Chiasson, R. Biddle, User-centred authentication feature framework, Inf. Comput. Secur. 23 (2015) 497–515.
[43] A.K. Nag, D. Dasgupta, K. Deb, An adaptive approach for active multi-factor authentication, 9th Annual Symposium on Information Assurance (ASIA’14), 2014, p. 39.
[44] A.K. Nag, D. Dasgupta, An adaptive approach for continuous multi-factor authentication in an identity eco-system, ACM International Conference Proceeding Series, 2014, pp. 65–68.
[45] L.H.F.M. Miranda, Context-aware Multi-Factor Authentication, Faculdade de Ciências e Tecnologia, 2009.
[46] G.J.W. Kathrine, E. Kirubakaran, Four-factor based privacy preserving biometric authentication and authorization scheme for enhancing grid security, Int. J. Comput. Appl. 30 (2011) 13–20.
[47] L. O'Gorman, Comparing passwords, tokens, and biometrics for user authentication, Proc. IEEE 91 (2003) 2021–2040.
[48] A. Bruun, K. Jensen, D. Kristensen, Usability of single-and multi-factor authentication methods on tabletops: a comparative study, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8742, 2014, pp. 299–306.
[49] M. Anwar, A. Imran, A comparative study of graphical and alphanumeric passwords for mobile device authentication, CEUR Workshop Proceedings, 2015, pp. 13–18.