Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication

Ignacio Velásquez

University of Bío-Bío, Computer Science and Information Technologies Department,
Chillán, Chile
ignaciowl@outlook.com

Abstract

Authentication is the process of verifying the identity of a user. An authentication factor is a piece of information used for authenticating. Three well-known groups of authentication factors exist: knowledge-based (what you know), possession-based (what you have) and inherence-based (what you are). Authentication schemes from distinct factors can be combined in a multi-factor manner to increase security. Various multi-factor authentication proposals exist in literature. However, the absence of a method for their evaluation in software development contexts is observed. Thus, this research focuses on the creation of a recommendation framework that guides the comparison and selection of authentication techniques by considering the application context and its requirements. This is achieved through a knowledge base generated from an extensive systematic literature review, coupled with surveys and interviews performed to industry experts from a partnered software development company. This company has also collaborated in validating the proposal through an expert panel and the realization of case studies. Moreover, a tool prototype for using the framework was also developed. This work extends from previously published material by updating the performed systematic literature review with publications since 2017, while also providing additional information regarding the tool prototype and the planning of the case studies.

Keywords: Security, Authentication Scheme, Multi-Factor Authentication Method, Recommendation Framework.

1 Introduction

Authentication is the process of positively verifying the identity of a user, devices, or any other entity in a computational system, generally as a prerequisite for gaining access to the system's resources [1]. Thus, an authentication factor is a piece of information used for authenticating or for verifying a user's identity [2]. These factors can be categorized in three groups: those based on knowledge (something that the client knows, such as text passwords or PIN codes), those based on possession (something that the client possesses, dependent of the possession of a physical object) and those based on inherence (something that the client is, known as biometrics) [3, 4]. Authentication schemes (concrete authentication solutions) belonging to distinct factors can be combined to enhance security, which is known as multi-factor authentication [1].

To differentiate between one-factor and multi-factor proposals, from this point onwards the former will be referred as Authentication *Schemes*, whereas the later will be referred as Multi-Factor Authentication *Methods*.

Although there are multiple proposals on the use of multi-factor authentication in literature [4-6], it is possible to observe the absence of a method that helps in the decision of when to use one or another authentication scheme and how to more adequately combine them in a multi-factor modality, especially considering requirements given by software application clients. Although there are some frameworks in literature that provide an analysis of multiple features of authentication schemes [7, 8], these are centered on authentication schemes by themselves and not in their use as part of multi-factor authentication methods, without emphasizing on clients' requirements and not giving a concrete answer for every situation.

Due to the above, this proposal centers itself in the creation of a framework that guides the selection of authentication schemes and their combinations as multi-factor authentication methods, by considering distinct criteria and application contexts, which are defined by the requirements given by clients. Based both on literature and on the experience of industry experts, comparison and selection criteria are applied, complementing both viewpoints.

The entirety of this work is part of a master thesis, whose aim is to ascertain the hypothesis that “*the use of a framework that guides software application developers in the selection of authentication schemes for their combined usage systematizes and facilitates the use of the most appropriate multi-factor authentication method for the use context*”.

1.1 Objectives

The main objective of this work is to study authentication schemes and methods proposed in literature and their features. Moreover, to identify criteria used for their comparison and selection proposed either in academy or industry. Finally, based on the above, to propose a framework that allows the selection of the most appropriate multi-factor authentication methods for a particular software application development context.

To achieve this objective, several sub-objectives have been defined, namely:

- To perform a Systematic Literature Review with the purpose of finding the main authentication schemes and methods that have been proposed.
- To gather comparison and selection criteria for authentication schemes and methods both from literature and the industry.
- To create a framework that provides a guide for the comparison and selection of authentication schemes and methods, based on the knowledge base obtained from literature and the industry.
- To construct a tool prototype that allows the use of the framework in distinct software application development contexts.
- To demonstrate the proposal’s validity, as well as the tool prototype’s usefulness, through case studies.

1.2 Contributions

The main contribution of this research is the creation of a recommendation framework that allows software developers to perform an adequate comparison and selection of authentication schemes and methods when deciding which scheme or method to implement while developing applications. This framework has been created based both on knowledge acquired from the academy as well as the experience reported by industry experts. These experts helped to properly validate the framework as well.

The experience from industry experts has been obtained thanks to the collaboration with a software development company during this research’s realization. The partnered software development company (PSDC) is a multinational company that works along three different countries. These countries are the United States of America, Chile, and India.

The PSDC not only provided the experience from their industry experts, but it also helped in the validation of the research.

The importance of the performed systematic literature review is highlighted as well, as it allowed ascertaining how the treated topic has been addressed before the realization of this research.

To date, various parts of this research have already been published [9-13]. However, this work presents additional contributions with the objective of providing added value, specifically:

- The knowledge base acquired through the realization of a systematic literature has been updated. Previously, publications published until 2016 had been reviewed. For this work, publications published since 2017 were also reviewed by following the same previously applied planning. This has allowed to identify new trends in research related to authentication schemes and methods, as well as the criteria used for their comparison and selection, and the application contexts considered by the publications.
- The developed tool prototype is presented more extensively, providing both screenshots of the tool as well as details on its utilization.
- The structure of the case study methodology utilized for validating the framework has been redefined. This has been done taking in consideration the guidelines proposed in literature [14]. This way, in addition to providing the results of the case studies, both their planning and the data gathering strategies utilized have been documented in a more comprehensive manner, which allows a clearer validation of the framework.

1.3 Organization

The remainder of the article is structured as follows: the main research strategies applied during this work are briefly described in Section 2. The addressed topic’s state of the art, along with the details of the performed systematic

literature review is provided in Section 3. Section 4 presents the results of the survey and interviews performed to industry experts for this research. The Kontun Framework is described in depth in Section 5, whereas Section 6 presents its validation through a case study methodology. Finally, the research's conclusions and future work are given in section 7.

2 Work Methodology

The realization of this research contemplates a series of activities which correspond to distinct research methodologies, which are described next.

2.1 Systematic Literature Review

Based on [15], a Systematic Literature Review (SLR) has been performed to obtain knowledge on the main authentication schemes and methods and criteria for their comparison and selection.

The three main steps of a SLR are (i) the review planning, (ii) the realization of the review and (iii) the report of results [15]. The detail of each step for the performed SLR is shown in Section 3.

2.2 Surveys

Industry experts were surveyed to gather their experience regarding the criteria used in industry for the selection and differentiation of authentication schemes and methods.

To evaluate the survey's adequacy [16], a pilot study was performed prior to its application to a reduced number of people, in the modality of personal interviews.

The results obtained from the realization of the survey and interviews are shown in Section 4.

2.3 Case Studies

The results of this research have been validated through the realization of case studies.

The required information for the realization of these case studies was obtained using semi-structured interviews [17, 18] and observation with low awareness of the subject coupled with a low degree of interaction from the researcher [17] techniques.

The realization of these case studies is shown in Section 6.

2.4 Action-Research

Finally, the work performed in this research can be encompassed as part of an action-research methodology, as it fulfills the double purpose of generating relevant "research knowledge" as well as providing a benefit to the "client" of the research [19].

The following action-research roles [20] can be identified in this work:

- The researcher, which corresponds to the author of this work.
- The researched object or topic, which corresponds to the comparison and selection of authentication schemes and methods.
- The critical group of reference, which corresponds to the employees of the PSDC.
- The beneficiary, which corresponds to the PSDC, as well as software developers in general.

3 State of the Art

The state of the art regarding the topic of authentication schemes and methods, coupled with criteria for their comparison and selection, could be ascertained through the realization of a SLR. The in-depth development and results of the originally performed SLR, which covers publications published up to 2016, have been documented in [10]. However, with the objective of complementing the previously obtained results, a new SLR has been performed. This SLR followed the same planning as the previous SLR but limiting the reviewed publications to those published since 2017. The following sections describe a summary of the planning utilized for both reviews, their results and discussion derived from them, respectively.

3.1 Systematic Literature Review Planning

With the objective of learning about existing decision frameworks, together with the criteria utilized by them, for the comparison and selection of authentication schemes and methods, the SLR aims to answer the following Research Questions (RQ):

- RQ1: Which are the main authentication schemes that exist in literature?
- RQ2: What combinations of these schemes can be found for their use as multi-factor authentication methods?
- RQ3: What criteria can be used to compare and/or to select between authentication schemes or multi-factor authentication methods?
- RQ4: Are there frameworks that help to compare and/or to select authentication schemes or multi-factor authentication methods? What are their characteristics?

The SLR was performed on sources with relation to the topic at hand, namely the ACM Digital Library, IEEE Xplore, Science Direct, Scopus and Springer. Google Scholar was also used to identify potentially useful publications not indexed in the above sources.

3.1.1 Search Protocol

The Terms (T) and their Combinations (C) used for the review are shown in Table 1. As previously mentioned, the SLR has been performed in two stages. The first stage reviewed publications up to 2016, whereas the second reviewed publications since 2017. In the case of the first stage, up to the first 200 results for every performed search have been reviewed. Due to the reduced number of reviewed years, up to the first 50 results of each search were reviewed for the second stage. An online reference manager was used to maintain a record of the results.

Table 1: Terms and combinations used to perform the SLR

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

3.1.2 Review Protocol

Initially, a partial review was performed by mainly reading the abstract of every publication and, if necessary, its introduction and conclusions. This served to identify potentially useful publications. A publication was included as potentially useful if it could be observed that it had a relation with any of the RQ. On the other hand, any other publication that contained the search terms, but did not have important information regarding either of the RQ, was excluded.

An in-depth review was performed on the potentially useful publications afterwards. Distinct strategies were used based on the RQ: for RQ1 and RQ2, the key information of the publication was identified, that is, the proposed authentication scheme or method and the related authentication factors, together with the context for which it was proposed; for RQ3 and RQ4, the entire publication was read to adequately comprehend the proposals and their strengths and weaknesses, emphasizing the identification of the distinct criteria used by each of them.

3.2 Results

For the first SLR, a search was performed for every combination of terms (Table 1) in every search source, for a total of 54 distinct searches. The first 200 publications were reviewed for every search, although 15 of these searches yielded less than 200 results. Thus, a total of 8,513 publications were reviewed. After removing the repeated publications, a total of 3,910 different publications were obtained. These were partially reviewed, and a total of 1,015

potentially useful ones were selected. An in-depth analysis was performed afterwards, discarding 33 publications that were not relevant for the current research. Finally, a total of 982 useful publications were identified.

In the case of the second SLR, 54 distinct searches were also performed, and up to 50 publications were reviewed for every search, although 6 of these searches yielded less than 50 results. Thus, a total of 2,503 publications were reviewed. After removing the repeated publications, a total of 1,019 were obtained, and after partially reviewing them, 460 potentially useful publications were selected. Finally, 10 publications were discarded through the in-depth analysis, for a total of 450 useful publications.

The useful publications of each SLR were split among the four RQ, as shown in Table 2.

Table 2: Accepted publications for each research question in every SLR

Research Topic	Number of Publications		
	First SLR	Second SLR	Total
Authentication schemes	515	164	679
Multi-factor authentication methods	442	251	693
Comparison and selection criteria	17	26	43
Decision frameworks	8	9	17
<i>Total</i>	982	450	1,432

A list containing the accepted publications in the first performed review can be found in <http://colvin.chillan.ubiobio.cl/mcaro/>, whereas a list containing the accepted publications in the second performed review can be found in <http://bit.ly/3o81gA5>. A summary of the results obtained for every RQ is shown next:

3.2.1 Authentication Schemes

Nearly half, that is, 679 of the accepted publications are related to this topic. Out of these, 217 propose the use of inherence-based authentication schemes, whereas 169 propose the use of possession-based schemes and 124 the use of knowledge-based ones. The remaining 5 articles propose the use of schemes based on other authentication factors, such as the use of the user's social networks [21] and location-based authentication [22]. Table 3 shows the number of articles proposing the use of the distinct authentication schemes, split by the authentication factors to which they belong.

Table 3: Authentication schemes found in literature

Factor	Scheme	Number of Publications		
		First SLR	Second SLR	Total
Knowledge	Graphical Passwords (GP)	42	15	57
	Text Passwords (TP)	44	10	54
	Other knowledge-based schemes	38	7	45
	<i>Total</i>	124	32	156
Possession	Smart Cards (SC)	103	10	113
	One Time Passwords (OTP or Tokens)	43	9	52
	Mobile-Based authentication (MB)	21	6	27
	Other possession-based schemes	2	1	3
	<i>Total</i>	169	26	195
Inherence	Behavioral Biometrics (BB)	64	46	110
	Face Biometrics (FB)	24	7	31
	Palm Print and Fingerprints (P/F)	22	9	31
	Iris Biometrics (IB)	8	3	11
	Other/unspecified biometrics	99	38	137
	<i>Total</i>	217	103	320
Other factors		5	3	8
<i>Grand Total</i>		515	164	679

Graphical passwords with 57, smart cards with 113, and behavioral biometrics with 110 publications each, are the most proposed schemes for the knowledge, possession, and inherence factors, respectively. It is important to highlight, however, that there are 54 proposals on the use of text passwords for the knowledge-factor, that is, only three less in comparison to graphical passwords, and that until 2016 text passwords has been proposed slightly more, meaning that graphical passwords have been proposed more often in recent years. In the case of behavioral biometrics,

it must be mentioned that they encompass distinct biometrics that are specifically related to the behavior of a person; among those in this group, keystroke and touch stroke biometrics are the most commonly proposed schemes.

Additionally, the context for which every authentication scheme was proposed was recorded, as shown in Table 4. It is important to mention that 361 of the 679 proposals did not specify a context.

Table 4: Authentication schemes and their contexts

Context	Number of Publications		
	First SLR	Second SLR	Total
Mobile Environment	81	33	114
Remote Authentication	42	4	46
Healthcare / Telecare	24	11	35
Multi-Server Environment	17	4	21
Cloud Computing	9	9	18
Banking and Commerce	8	4	12
Wireless Sensor Networks	10	2	12
Smart Environment	7	4	11
Web Applications	5	3	8
Internet of Things	1	2	3
Other Contexts	29	9	38
Unspecified	282	79	361
<i>Total</i>	515	164	679

3.2.2 Multi-Factor Authentication Methods

A total of 693 publications were related to proposals of multi-factor authentication methods. Most of them (346) focus on the combination of the knowledge and possession factors. As for the others, 70 propose the combination of the knowledge and the inherence factors, 62 propose the combination of the possession and inherence factors, and 183 propose the combination of all three factors. Additionally, 22 other publications proposed not a specific authentication method, but rather a dynamic set of methods based on the circumstances. Finally, 10 publications proposed combinations including factors other than the three well-known ones. A summary on the number of publications proposing each multi-factor authentication method and the combination of factors to which it belongs can be seen in Table 5.

Table 5: Multi-factor authentication methods found in literature

Combination	Method	Number of Publications		
		First SLR	Second SLR	Total
Knowledge + Possession	Text Passwords + Smart Cards	188	41	229
	Text Passwords + Mobile-Based	37	16	53
	Text Passwords + OTP	34	10	44
	Others	11	9	20
	<i>Total</i>	270	76	346
Knowledge + Inherence	Text Passwords + Biometrics	36	18	54
	Graphical Passwords + Biometrics	4	1	5
	Others	4	7	11
	<i>Total</i>	44	26	70
Possession + Inherence	Smart Cards + Biometrics	24	7	31
	Mobile-Based + Biometrics	6	6	12
	OTP + Biometrics	9	3	12
	Others	4	3	7
	<i>Total</i>	43	19	62
Knowledge + Possession + Inherence	Text Passwords + Smart Cards + Biometrics	47	83	130
	Text Passwords + Mobile-Based + Biometrics	7	23	30
	Text Passwords + OTP + Biometrics	9	6	15
	Others	5	3	8
	<i>Total</i>	68	115	183
Other combinations		5	5	10
Dynamic methods		12	10	22
<i>Grand Total</i>		442	251	693

The most notable combination is that of text passwords and smart cards, which has been proposed in 229 distinct publications. Moreover, it can be observed that over 84% of the combinations use at least one of either text passwords or smart cards as one of the schemes for multi-factor authentication. It is also highlighted that, since 2017, proposals consisting of the combination of text passwords and smart cards have not been as common as before (42.5% of the proposals until 2016, versus 16.3% since 2017). Conversely, proposals consisting of text passwords, smart cards and biometrics have been researched more often since 2017 (10.6% of the proposals until 2016, versus 33.1% since 2017).

Similarly to authentication schemes, the context for which every authentication method was proposed was recorded as well, as shown in Table 6. In contrast to authentication schemes, where over half of the publications did not indicate a context, in the case of multi-factor authentication methods, only a 31.5% of the publications did not indicate it.

Table 6: Multi-factor authentication methods and their contexts

Context	Number of Publications		
	First SLR	Second SLR	Total
Healthcare / Telecare	48	46	94
Remote Authentication	64	20	84
Wireless Sensor Networks	33	18	51
Mobile Environment	21	28	49
Multi-Server Environment	29	20	49
Cloud Computing	17	20	37
Banking and Commerce	11	11	22
Web Applications	11	3	14
Internet of Things	0	13	13
Smart Environment	2	6	8
Other Contexts	36	18	54
Unspecified	170	48	218
<i>Total</i>	442	251	693

3.2.3 Comparison and Selection Criteria

The third objective of this SLR was to identify criteria used for the comparison and selection of the above authentication schemes and methods. A total of 43 publications that proposed one or more criteria were found.

Among the categories used for differentiating the distinct criteria, those with relation to security and usability were the most common, with a total of 27 appearances for security, and 21 for usability. Costs-related criteria come next, with 10 appearances. Instead of using criteria, a number of publications evaluated the authentication schemes and methods based on advantages and limitations [23, 24]. Other criteria categories could be ascertained, but each of them did not appear more than twice.

Similarly to the first two RQ, the contexts where these criteria were used were identified, as it can be observed in the graphic on Fig. 1.

Figure 1: Considered contexts for comparison and selection criteria

3.2.4 Decision Frameworks

A total of 17 frameworks that help in the comparison and selection of authentication schemes or methods have been found in literature. A summary of each of them is given next, ordered by date, from oldest to newest:

- Various authentication schemes are evaluated in [25] regarding their pros and cons. This framework considers some topics regarding authorization as well.
- A framework with a focus on multimedia systems is proposed in [26]. This framework considers three primary criteria (security, ease of use and simplicity) and three secondary criteria (awareness, usability, and algorithms). This framework considers the perceptions of users as well.
- A framework that considers both the context and the requirements of stakeholders is proposed in [27]. This framework focuses on supporting the selection of the most suitable automatic identification between the knowledge and inference factors.
- A detailed analysis of authentication schemes and methods is done in [28]. This analysis uses costs-related criteria and is to be used by companies when switching to a new authentication scheme or method.
- An in-depth analysis of multiple web authentication schemes is performed in [7]. This analysis considers criteria related to security, usability, and costs.
- In [8], a framework oriented to researchers that evaluates knowledge-based authentication schemes is proposed. The evaluation is done based on the scheme's persuasion, memory, input and output and obfuscation features.
- The work in [29] compares the multiple two-factor authentication method proposals that utilize the combination of text passwords and smart cards. This comparison is done based on criteria related to desirable attributes, security requirements and efficiency.
- System managers are surveyed on their preferences regarding paid authentication schemes for the mobile environment in [30]. This is done based on criteria related to security, convenience, and operation costs.
- The research in [31] surveys the authentication schemes and methods utilized in telecare medical information systems while also providing a taxonomy for their classification. The study also compares the techniques regarding their advantages, properties, and limitations.
- A method for choosing biometric schemes is presented in [32]. For this, the method makes use of various usability, security, and costs criteria, as well as weighting factors.
- The work in [33] proposes a systematical evaluation framework for two-factor authentication schemes in wireless sensor networks. The evaluation is performed through various security criteria.
- A framework for critically analyzing smart card-based two factor authentication methods is presented in [34]. The framework utilizes various security criteria for performing the comparison.
- A comprehensive evaluation framework for multi-factor authentication in the mobile environment is proposed in [35]. This framework is proposed through the fishbone model and developed in the form of a universal authentication framework leveraging on user priorities such as security, usability, and pricing.
- A game-based framework is proposed by [36] to compare the usability features of authentication techniques.
- The study of [37] extends from the framework proposed in [7] by revisiting the rating process and reviewing additional authentication schemes.
- In [38], an evaluation model for knowledge-based authentication schemes is proposed. This model utilizes security and usability criteria for performing the evaluation.
- Finally, multiple one, two and three-factor authentication methods are evaluated for their use in wireless sensor networks in [39]. This evaluation is done through security and functionality criteria, providing the pros and cons of every evaluated method.

3.3 Discussion

The realization of this SLR allowed learning not only about the existing authentication schemes and methods, but also about the criteria used for their comparison and selection, as well as frameworks that utilize these criteria. Moreover, it was also possible to ascertain the amount of research performed regarding authentication in distinct application contexts.

Regarding authentication schemes, the most reviewed authentication factor is that of inherence-based schemes, whereas the least reviewed one is that of knowledge-based schemes. This is perhaps due to the paradigm that the most researched scheme of the knowledge factor (text passwords) is not too secure [7]. The use of smart cards is the most proposed authentication scheme. However, this is a declining trend, as only 10 publications were found that proposed using smart cards as a single-factor scheme since 2017. Conversely, there has been an upward trend of publications proposing the use of behavioral biometrics, with 46 such publications since 2017. A possible explanation to this is that the possession of devices that allow authenticating through biometrics has become more common in recent years [32].

The combination of the knowledge and possession factors, especially with the use of text passwords and smart cards, has been researched very often in literature. It has been observed that three-factor authentication has been proposed more often than combinations of two factors other than that of knowledge and possession, especially since 2017, where 45.8% of the proposals considered combinations of the three factors. In comparison, only 15.4% of the publications until 2016 proposed three-factor authentication methods. A four-factor authentication method proposal was also found, the fourth factor being the location-based factor [40]. The appearance of dynamic authentication methods [41-43] was an interesting find, as these methods adapt to distinct contexts.

When comparing the number of publications that proposed authentication schemes to that of publications that proposed multi-factor authentication methods, it can be observed that a similar amount of research has been performed for both. However, although until 2016 there was a higher number of single-factor proposals (515 versus 442), since 2017 the situation is the opposite (164 versus 251). Thus, an upward trend towards researching multi-factor authentication can be observed.

Regarding the application contexts that were identified from the authentication scheme and method proposals, many of these have been researched often, such as mobile environment, remote authentication, and healthcare / telecare. However, it can be observed that there is still room for further researching other less considered contexts, such as banking and commerce, and web applications. The contexts of internet of things and smart environments are highlighted as there has been an upwards trend on their research since 2017. In the case of internet of things, it is also noted that there are three publications that propose comparison and selection criteria for authentication techniques in this context [24, 44, 45].

Only 60 of the found and accepted publications tackled either comparison and selection criteria or frameworks that utilized them. The three most used criteria categories that could be observed are those of security, usability, and costs. The application context was observed to be of importance as well, since most publications either directly considered it as a criterion [1] or were oriented to a specific application context [46-49]. An important finding from the realization of the second SLR is that the comparison and evaluation of authentication schemes and methods has been increasingly researched since 2017: more than half of the publications belonging to RQ3 and RQ4 are since this year. This is a positive upward trend, as research on this subject was not wide until 2016.

It must be mentioned that the acceptance of publications for RQ1 and RQ2 was limited to those that directly proposed a new authentication scheme or an enhancement of an existing one. Moreover, due to time constraints and to the amount of potentially useful publications for these two research questions, the review of each publication was limited to extracting the information that was relevant for this review.

Summarizing, the main findings of this SLR for each of the formulated RQs are as follows:

- *RQ1: Which are the main authentication schemes that exist in literature?*

Wide research has been done over the three well-known factors. The most reviewed authentication schemes for each factor are graphical passwords for the knowledge factor, smart cards for the possession factor, and behavioral biometrics for the inherence factor.

- *RQ2: What combinations of these schemes can be found for their use as multi-factor authentication methods?*

There are multiple multi-factor authentication methods that combine the found authentication schemes. There are both two-factor and three-factor proposals, and even a four-factor proposal. Text passwords and smart cards are the most used authentication schemes for their combination as multi-factor authentication methods.

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

Criteria related to security, usability and costs are the mainly used criteria for the comparison and selection of authentication schemes and methods. The importance given to the context of the application could be observed as a possible criterion as well.

- *RQ4: Are there frameworks that help to compare and/or to select authentication schemes or multi-factor authentication methods? What are their characteristics?*

Seventeen decision frameworks were found. Each framework has distinct features and provides adequate insight for the purposes that they have been created for. However, a generic framework that allowed a detailed analysis of both authentication schemes and multi-factor authentication methods for as many contexts as possible, while also considering multiple comparison and selection criteria could not be found.

4 Survey and Interviews

A survey and interviews (S&I) strategy was used to acquire the experience of industry experts regarding authentication. The results of the S&I were then used to complement the findings from literature, thus obtaining the viewpoints from both the academy and the industry. Part of the results of the S&I has been published in [12].

The interviews were used as a pilot realization of the survey, to ascertain its adequacy. A total of 12 industry experts from the PSDC were interviewed. Moreover, 83 surveys were sent to experts from the same PSDC. A total of 46 answers were received, but one of them only contained the respondent's demographic information, so it was discarded. Thus, 45 successful responses were received, which corresponds to a response rate of 54.2%.

Out of the 45 respondents of the survey, 36 of them were from Chile, whereas 9 were from the USA. Their experience in years can be observed in Fig. 2. As for the interviewees, all 12 of them were experts from Chile with at least 3 years of experience.

To differentiate between the participants of each study, those belonging to the interviews will be referred as interviewees, whereas those belonging to the survey will be referred as respondents.

Figure 2: Experience in years of the respondents

4.1 Results

The S&I shared the same aim on each of the questions present in them. A total of four topics were covered to ascertain:

- The known authentication schemes in the industry.
- Combinations of authentication schemes known in industry for multi-factor authentication.
- Authentication schemes and methods that industry experts select to implement in their applications.
- The criteria used by these experts to compare and select the distinct authentication schemes and methods for their implementation, as well as the importance given to each of them.

The first question inquired both the interviewees and the respondents on what single-factor authentication schemes they knew. In both cases, the most known schemes are text passwords, One Time Passwords (OTP, also known as Tokens) and mobile-based authentication. The graphic shown in Fig. 3 summarizes the authentication schemes known by both the interviewees and the respondents. All 45 respondents answered this question.

Figure 3: Authentication schemes known by industry experts, adapted from [12]

Similarly, upon an explanation on authentication factors and multi-factor authentication, the experts were inquired about multi-factor authentication methods that they knew. The combination of text passwords and OTP was the most known one for both the respondents and the interviewees. Table 7 shows the number of mentions for every combination of the knowledge, possession, and inference factors. 27 out of the 45 respondents declared knowing at least one authentication method.

Table 7: Multi-factor authentication methods known by industry experts, adapted from [12]

Combination	Method	Respondents	Interviewees
Knowledge + Possession	Text Passwords + OTP	15	7
	Text Passwords + Smart Cards	8	2
	Text Passwords + Mobile-Based	6	6
	Others	1	0
	<i>Total</i>	30	15
Knowledge + Inherence	Text Passwords + Biometrics	15	0
	Others	3	0
	<i>Total</i>	18	0
Possession + Inherence	OTP + Biometrics	6	0
	Mobile-Based + Biometrics	3	0
	Smart Cards + Biometrics	3	0
	<i>Total</i>	12	0
Knowledge + Possession + Inherence	Text Passwords + Smart Cards + Biometrics	7	0
	Text Passwords + OTP + Biometrics	2	1
	Others	2	0
	<i>Total</i>	11	1
<i>Grand Total</i>		71	16

The next question ascertained the authentication schemes and methods that have been implemented by the respondents and interviewees on applications that they have developed. Moreover, the context for which these applications have been developed was identified as well. The results of this question are summarized in the graphics shown in Fig. 4 and Fig. 5. Out of the 45 respondents, 23 had implemented at least one application that required authentication.

Figure 4: Schemes and methods implemented by industry experts, adapted from [12]

Figure 5: Contexts where industry experts have implemented authentication schemes or methods, adapted from [12]

Finally, two distinct strategies were utilized to learn the comparison and selection criteria used by industry experts. In the case of the interviewees, the advantages of a face to face interview were utilized to obtain the criteria used by the interviewees through a guided conversation. The results of this strategy can be seen in the graphic shown in Fig. 6.

Figure 6: Comparison and selection criteria considered by the interviewees, adapted from [12]

In the case of the survey, the respondents were given a list of several comparison and selection criteria that could be identified through the realization of the SLR and the interviews. The respondents were asked to value the importance of each criteria in a scale from 1 (low importance) to 5 (high importance). The results of this strategy are shown in Table 8. A total of 29 of the respondents answered this question.

Respondents were finally given the opportunity to mention any other criteria that they considered when comparing and selecting authentication schemes or methods. Here, the ease of authentication information recovery, the registration method and the sensitivity of the information used by the application can be highlighted.

4.2 Discussion

A total of 57 answers, that is, 12 from the interview and 45 from the survey, were received through the application of this S&I. It could be observed that both strategies yielded similar results, which implies the validity of the obtained answers.

Text passwords are the most known knowledge-based authentication scheme. Unlike the results of the SLR, graphical passwords are not known as much, however.

Regarding the possession factor, results differ from those of the SLR: smart cards is the most researched authentication scheme in literature, but it is the least known possession-based scheme by the participating industry experts, whereas mobile-based authentication and OTP are widely known by the later.

Table 8: Comparison and selection criteria valued by the respondents, adapted from [12]

Category	Criteria	Value
Usability	Ease of use	3.31
	Ease of learning	3.28
	Need of using a device	3.10
	Method's reliability	4.10
Costs	Implementation costs	4.07
	Costs per user	4.00
	Server compatibility	3.69
	Need of acquiring licenses	3.86
Security	Available technologies	3.93
	Importance of security	4.41
	Resistance to well-known attacks	4.21
Others	Client's requirements	4.17
	Application context	4.41
	Norms and legislation	3.90

Some of the experts mention the existence of federated single sign-on and proxy-based authentication. However, these are implementations that support the process of authentication rather than authentication schemes themselves.

Regarding multi-factor authentication, the most knowledge from the industry experts is on the combination of text passwords coupled with a possession-based scheme. This is similar to the results of the SLR, where the combination of the knowledge and possession factors prevails. Three-factor authentication is not well-known by the industry experts, however.

Most of the applications developed by the industry experts belong to the contexts of web applications and banking and commerce. This differs from the most researched application schemes found in literature, where both contexts had not been researched as much.

It can be observed that all the proposed comparison and selection criteria were considered important by at least two thirds of the industry experts. This indicates that all these criteria are adequate to some degree for performing the comparison and selection of authentication schemes and methods.

A certain correlation can be observed between the results of the SLR and of the S&I. These are not excluding of each other and can be used together to obtain a complement from the knowledge found in the academy and the experience obtained from the industry, thus providing an added value to the results of research based on both.

5 Kontun: Framework for Recommendation of Authentication Schemes and Methods

The section presents the theoretical framework that has been devised. This framework is based on the information gathered from the academy and industry for the comparison and selection of authentication schemes and methods. The framework has been previously presented in [11].

An initial draft of the Kontun Framework consists of three stages, as shown in Fig. 7.

Figure 7: Stages of the framework's initial draft

Stage 1 consists of finding the average values of the security, usability and costs criteria that have been considered for the framework. Each criterion is given a weight and distinct possible importance levels. The average values are calculated based on the sum of the importance levels that are most adequate for the currently evaluated application for each criterion, multiplied by their respective weights.

For the second stage, the most adequate application context for the current application is identified. Based on this context, what has been denominated as the Security/Usability Value (SUV) is calculated. This value originates from the observations from the SLR, where it is observed that no existing scheme can provide maximum security and usability while also possessing minimal costs. This can be seen, for example, in [7], where none of the analyzed authentication schemes possessed every desirable feature. Rather, it is observed that the higher the importance given to usability, the lower that security will be, and vice-versa. Thus, a high SUV value will indicate that more importance is given to security over usability, whereas a low SUV value will indicate that more importance is given to usability over security. The formula for the calculation of the SUV is as shown in (1).

$$SUV = C_1 \text{Avg}_{(S)} + C_2(100 - \text{Avg}_{(U)}) \quad (1)$$

Where C_1 and C_2 are constants dependent on the defined context, whereas $\text{Avg}_{(S)}$ and $\text{Avg}_{(U)}$ correspond to the average security and usability values that have been defined in the previous stage.

The final stage corresponds to the recommendation given by the framework. This recommendation consists of the most adequate authentication schemes and methods, based on the calculated SUV and the average value of costs for the given application's requirements and context.

5.1 Expert Panel

An expert panel was performed to validate the initial draft of the framework. The expert panel consisted of four sessions with a specific objective for each of them. The expert panel was conformed of five experts from the PSDC. Fig. 8 summarizes the activities realized each day.

Figure 8: Activities for every session of the expert panel, adapted from [11]

The first session was used to familiarize the industry experts with the topic. Both the current findings of the research and the initial draft of the framework were presented to them using a deductive approach.

The comparison and selection criteria considered by the framework were reviewed on the second session. Observations emerged mainly regarding the costs-related criteria that were being considered: the experts considered that a higher level of generalization was required. The expert panel was in accordance with the weights and importance levels given to each criterion.

The contexts considered by the framework were reviewed on the third session. Through this, some of the considered contexts were grouped due to their similarities, whereas another, that is, federated single sign-on was dismissed, due to the discrepancy in the views from the academy and industry in regards to it.

The SUV was presented in the third session as well. The act of contrasting between security and usability was well received. The expert panel showed its concerns regarding the distinct weights given to security and usability, however, mentioning that further validation was required. Based on this feedback, a survey was performed to a limited number of industry experts from the PSDC in order to specifically ascertain the importance that they would give to security and to usability to every context considered by the framework. The survey was sent to 9 experts with a 100% response rate. Finally, the security and usability weights used by the framework were defined by weighing both the results of the survey and the appreciations obtained from literature.

The last session consisted of analyzing the recommendations given by the framework. No major changes were suggested to be done to the schemes and methods recommended for each context, as the expert panel considered them to be adequate.

5.2 The Proposal

The Kontun Framework is described in-depth in this section. As it was explained above, the utilization of the framework consists of three stages.

The first stage consists of the selection of the most adequate importance levels for every criterion considered by the framework. These criteria were selected based on the most recurrent criteria observed in literature. Specifically, security criteria were taken from [1, 7, 26, 29, 50-53], usability criteria were taken from [7, 26, 47, 50, 51, 54, 55], and costs criteria were taken from [1, 7, 28, 54, 55]. It is important to mention that criteria that were focused on specific technologies, such as “server compatibility”, were not considered, as the framework is not meant to be used in a single technological context. The process taken for defining these criteria has been presented in [9]. Other criteria were considered based on the results from the S&I, such as the “information authentication recovery” criterion. Each criterion was given distinct importance values and weights based on the appreciations from industry experts obtained through the S&I. Table 9 presents the criteria together with their importance levels and weights. A brief description of each criterion is given next:

Table 9: Comparison and selection criteria valued by the respondents, adapted from [11]

Category	Criteria	Importance	Value	Weight
<i>Security (S)</i>	Importance of security	Security is a crucial aspect	100	45%
		Security is an important aspect	60	
		Security is a secondary aspect	20	
	Information Sensitivity	Sensitive information for the company and user	100	25%
		Sensitive information for the company	75	
		Sensitive information for the user	45	
		No sensitive information	20	
	Resistance to observation from third parties	Method should be resistant	100	10%
		Method does not need to be resistant	20	
	Resistance to phishing	Method should be resistant	100	10%
		Method does not need to be resistant	20	
	Resistance to replay attacks	Method should be resistant	100	10%
		Method does not need to be resistant	20	
<i>Usability (U)</i>	Ease of use	Method necessarily needs to be easy to use	100	25%
		Method preferably needs to be easy to use	60	
		Not necessary for the method to be easy to use	20	
	Ease of learning	Should take no longer than a day to get used	100	25%
		Should take no longer than a week to get used	60	
		Time that it takes to get used is not relevant	20	
	Authentication information recovery	Recovery process should be simple	100	10%
		Recovery process should be complex	20	
	Need of using a device	Method does not need to use a device	100	10%
		Method can use a possession or biometric device	60	
		Method can use both kinds of devices together	20	
	Authentication method's reliability	Should never or hardly fail during authentication	100	30%
		Should not fail occasionally during authentication	75	
		Can fail occasionally during authentication	45	
<i>Costs (C)</i>	Implementation costs	Does not matter how often it fails	20	65%
		Should not be over 10% of the budget	100	
		Should not be over 30% of the budget	60	
	Costs per user	Can be any, regardless of budget	20	35%
		Should not present additional costs for each user	100	
		Can present additional costs for each user	20	

Security:

- *Importance of Security:* Importance given by the software development team to security, based on the known information about the application.
- *Information Sensitivity:* The kind of information that will be used by the application and its sensitivity.
- *Resistance to Observation from Third Parties:* Utility of the scheme or method to be used on places with the risk of onlookers at the moment of authentication.
- *Resistance to Phishing:* Difficulty for an attacker to discern the user's authentication information through the application of social engineering.
- *Resistance to Replay Attacks:* That the cost of attempting to obtain the user's authentication information through replay or brute force attacks is higher than the profit associated to a successful attack.

Usability:

- *Ease of Use:* Complexity presented by the actions required for a user to authenticate.
- *Ease of Learning:* The time required for a user to get accustomed to using the authentication scheme or method.
- *Authentication Information Recovery:* Complexity presented by the actions required for a user to recover their authentication information, in case of loss.

- *Need of Using a Device*: Acceptability of the user having to possess a possession device (something unique), a biometric device (for demonstrating their inherent information), or both.
- *Authentication Scheme or Method's Reliability*: Acceptable recurrence of false negatives (that the scheme or method does not recognize a user's legitimate authentication information).

Costs:

- *Implementation Costs*: Monetary value that the client is willing to spend on the implementation of security aspects in the application.
- *Costs per User*: Willingness of the client to incur in additional costs for every user that registers in the application.

Once every assessment of importance for the above criteria has been defined in regards to the evaluated application, the average Security (S), Usability (U) and Costs (C) values can be calculated using (2), (3) and (4) respectively.

$$Avg_{(S)} = \sum_{\text{for each S criterion}} \text{Value} \cdot \text{Weight} \quad (2)$$

$$Avg_{(U)} = \sum_{\text{for each U criterion}} \text{Value} \cdot \text{Weight} \quad (3)$$

$$Avg_{(C)} = \sum_{\text{for each C criterion}} \text{Value} \cdot \text{Weight} \quad (4)$$

Once the above have been calculated, the context for which the application belongs can be defined. Based on the findings both from literature and industry, the most studied and/or known contexts (Ct) have been selected as common contexts in the framework. Based on the selected context, the SUV can then be calculated by using (1). The values of the constants used for calculating SUV (C_1 and C_2) for each context are presented in Table 10. As it has been explained above, the SUV determines the importance of security and usability for the given application: the higher the SUV, the higher the importance given to security will be, whereas the lower the SUV, the higher the importance to usability will be. Thus, a high SUV will indicate that the framework will recommend more secure authentication methods, whereas a low SUV will indicate that the framework will recommend more usable authentication schemes.

Table 10: Values of C_1 and C_2 for the calculation of the SUV on every context, adapted from [11]

ID	Context	C_1	C_2
Ct1	Mobile environment	0.45	0.55
Ct2	Remote authentication, multi-server environment, cloud computing	0.65	0.35
Ct3	Healthcare / telecare	0.50	0.50
Ct4	Wireless sensor networks	0.60	0.40
Ct5	Banking and commerce	0.75	0.25
Ct6	Common web applications	0.30	0.70
	Other contexts	0.50	0.50

A brief description of every context considered by the framework is given next:

- *Mobile Environment*: Applications whose end user makes use of them mainly from a mobile device, and whose emphasis is not in cash transactions.
- *Remote Authentication, Multi-Server Environment and Cloud Computing*: Applications through which users authenticate to a network remotely, whose information is stored through more than one server and/or based in the use of Internet for providing services or storage.
- *Healthcare / Telecare*: Applications directed to medical or health-related environments.
- *Wireless Sensor Networks*: Applications that monitor and register physical or environmental conditions.
- *Banking and Commerce*: Applications with an emphasis on cash transactions, regardless of the platform that they have been built for.
- *Common Web Applications*: Simple applications that can be found on internet, such as blogs or news sites.

Once all the above has been defined, it is possible for the framework to provide a recommendation. This recommendation is given based on Table 11, where each cell indicates the recommended authentication schemes or methods for the corresponding column (the Context) and row (where both the calculated SUV and $Avg_{(C)}$ make the respective relations true).

To define what authentication scheme or method to recommend for each situation, their approximate security, usability, and costs values were calculated based on the features reported by [7] that every authentication scheme possessed. Next, based on the findings of the SLR and S&I, the most studied and/or implemented schemes and methods for every considered context were identified. These schemes and methods were divided in three groups based on the number of factors that they considered (single-factor, two-factor, and three-factor). This is because it can be implied that the more factors that an authentication method considers, the more secure and less usable.

Every level was divided once again between more expensive and cheaper schemes and methods. This way, a total of six distinct levels were defined.

The recommended schemes or methods for every cell are ordered from the most recommended to the least, based on how often the scheme or method was reported in literature and/or industry for the given context.

Table 11: Schemes and methods recommended by the framework, adapted from [11]

	SUV and Costs	Ct1	Ct2	Ct3	Ct4	Ct5	Ct6	Other Context
Level 1	SUV $\geq$ 65 C < 60	GP+SC+BB	GP+SC+P/F	TP+SC+BB	TP+SC+BB	TP+OTP+BB	TP+OTP+BB	TP+OTP+BB
		TP+OTP+BB	GP+SC+BB	TP+OTP+BB		GP+SC+BB	TP+OTP+P/F	GP+SC+BB
		GP+OTP+BB	TP+OTP+BB	TP+OTP+P/F		GP+OTP+BB	TP+OTP+FB	GP+OTP+BB
		GP+OTP+FB	GP+OTP+P/F	TP+OTP+FB			TP+OTP+IB	GP+MB+BB
	SUV $\geq$ 65 C $\geq$ 60	TP+SC+BB	TP+SC+BB	TP+SC+BB	TP+SC+BB	TP+MB+BB	TP+SC+BB	TP+SC+BB
		TP+FC+FB	TP+MB+P/F TP+MB+BB	TP+MB+BB TP+MB+P/F		TP+SC+BB	TP+MB+BB	TP+MB+BB
Level 2	35 < SUV < 65 C < 60	GP+BB	SC+P/F	SC+BB	SC+BB	TP+OTP	TP+OTP	TP+OTP
		OTP+BB	SC+BB	OTP+BB	SC+P/F	MB+BB	MB+BB	OTP+BB
		TP+P/F	GP+SC	OTP+P/F		OTP+BB		MB+BB
		GP+OTP	TP+OTP OTP+BB TP+MB	OTP+FB OTP+IB MB+BB MB+P/F				GP+OTP GP+MB
	35 < SUV < 65 C $\geq$ 60	TP+BB	TP+SC	TP+SC	TP+SC	TP+MB	TP+SC	TP+SC
		TP+SC	SC+BB GP+SC TP+MB		SC+BB	TP+SC	TP+MB	GP+BB TP+MB
Level 3	SUV $\leq$ 35 C < 60	BB	SC	FB	FB	BB	FB	BB
		GP	P/F	BB	BB	FB	BB	GP
		FB	FB	P/F	P/F	P/F	P/F	P/F
		P/F	BB IB	IB	IB	IB	IB	FB
	SUV $\leq$ 35 C $\geq$ 60	BB	TP	BB	TP	TP	TP	BB
		TP GP	BB		BB	BB	BB	TP GP

Finally, a brief description of every authentication scheme considered by the framework is given:

Knowledge-Based Schemes:

- *Text Passwords (TP)*: A user inputs a known username (such as their email or identification number) and a password (a secret string that only they know) to demonstrate their identity.
- *Graphical Passwords (GP)*: Like text passwords, but instead of memorizing a string, the user must memorize an image-based pattern.

Possession-Based Schemes:

- *Smart Cards (SC)*: A magnetic card with incorporated circuits. A user must demonstrate possession of the smart card to authenticate.

- *One Time Passwords (OTP)*: Also known as Tokens. These come in distinct manners, such as: Hardware Tokens, that consist of a device that generates a randomized password; Software Tokens, which generate this random number through an application; and Paper Tokens, which consist of grids with coordinates that possess random numbers. To authenticate, the user must submit the randomized number provided by the OTP.
- *Mobile-Based Authentication (MB)*: The user's smartphone is used to authenticate. This can be done, for example, through SMS or through an application installed in the smartphone.

Inherence-Based Schemes:

- *Face Biometrics (FB)*: Authentication is done through the analysis of the user's facial features.
- *Behavioral Biometrics (BB)*: Unlike other biometrics that focus on physical features, behavioral biometrics authenticate a user based on their behavior. For example, the way they press the keyboard's keys.
- *Palm Print and Fingerprints (P/F)*: Either the user's palm print or fingerprints are used to recognize the identity of the user.
- *Iris Biometrics (IB)*: The user is authenticated through the recognition of their iris.

5.3 Tool Prototype

A tool prototype has been developed to ease the use of the Kontun Framework on software development processes. This tool can be found in the supplementary materials (<http://colvin.chillan.ubiobio.cl/mcaro/>).

This is a Web application that facilitates the recommendation of the best authentication scheme or method by automatically calculating the mathematical formulae, thus simplifying the usage process of the Kontun Framework. Although anyone can individually use the tool prototype, it has been especially designed for its use on software development companies, as it provides a simple user login system to maintain a registry of its usage, together with additional options for companies to adapt the tool prototype based on their own preferences.

The tool prototype was developed using the Model View Controller design pattern, based on the Spring Framework for Java, and using PostgreSQL as the database manager for storing the required information.

5.3.1 Utilizing the Tool Prototype

The utilization of the tool prototype for obtaining recommendations is a linear process that, based on the user input, automatizes the framework's mathematical calculations. Since the tool is planned for its use in a software development company's context, the user first needs to have created an account. Moreover, before utilizing the tool, it is important that the user has acquired an adequate knowledge of the application to develop that will be evaluated by the tool. This is necessary so that the user knows the application's usability and security features, as well as the acceptable costs and the target context. This information can be acquired, for example, through requirements gathering meetings.

Having logged in, the user needs to go to the Select Method button in the top menu of the application. Then, the user will be prompted with the screen for selecting the importance values for the usability, security, and costs criteria, as shown in Fig. 9. The user needs to select these using the radio buttons presented. In case of requiring the definition of a criterion, the user can hover through the hint buttons next to each of them.

After selecting all importance levels, the user can proceed to the next screen, where they will be prompted with the selection of the context most suited to the application to develop, as shown in Fig. 10. The context must be selected through the provided radio buttons. The weights of usability and security given to that context are also shown in a simplified manner, by using the *low*, *medium*, and *high* keywords. Similarly to the previous screen, the user is provided with hint buttons for obtaining definitions of every context.

FRAMEWORK FOR THE COMPARISON AND SELECTION OF AUTHENTICATION SCHEMES AND METHODS

Logged in as ivelasqu@alumnos.ubiobio.cl

Index Select Method Options Log out

DEFINE CRITERIA

Usability - Security - Costs

Importance of Security	☐ Security is a crucial aspect for the application. ☒ Security is an important aspect for the application. ☐ Security is a secondary aspect for the application.
Information Sensitivity	☒ The application works with sensitive information for both the company and the user. ☐ The application works with sensitive information for the company. ☐ The application works with sensitive information for the user. ☐ The application does not work with sensitive information.
Resistance to Observation from Third Parties	☐ The method should be resistant. ☐ The method does not need to be resistant. ☒ That the method is usable in environments where people that could be observing the users upon authentication time exist.
Resistance to Phishing	☐ The method should be resistant. ☐ The method does not need to be resistant.
Resistance to Replay Attacks	☐ The method should be resistant. ☒ The method does not need to be resistant.

Cancel Next

IGNACIO VELÁSQUEZ, ANGÉLICA CARO, ALFONSO RODRÍGUEZ - 2016

Figure 9: Selection of the importance levels of criteria in the tool prototype

FRAMEWORK FOR THE COMPARISON AND SELECTION OF AUTHENTICATION SCHEMES AND METHODS

Logged in as ivelasqu@alumnos.ubiobio.cl

Index Select Method Options Log out

SELECT CONTEXT

Context	Usability Weight	Security Weight
☐ Mobile Environment		
☐ Remote Authentication, Multi Server Environment and Cloud Computing	Medium	Medium
☐ Healthcare / Telecare	Low	High
☐ Wireless Sensor Networks	Medium	Medium
☐ Banking and Commerce	Low	High
☐ Simple Web Applications	High	Low
☐ Other Context	Medium	Medium

Return Next

IGNACIO VELÁSQUEZ, ANGÉLICA CARO, ALFONSO RODRÍGUEZ - 2016

Figure 10: Selection of the application context in the tool prototype

Once the context has been selected, the next screen provides a summary of the user's selections, thus acting as a confirmation screen. After confirming his selections, the user can proceed to the recommendation screen, which provides the framework's recommendations for the evaluated application, as shown in Fig. 11. The recommendations are provided in order from the most recommended to the least, while also indicating the importance given to security, usability and costs based on the user's input (shown as *low*, *medium*, or *high*), and the selected context. If the user requires definitions of the recommended authentication schemes, they can follow the link presented below the recommendations, which will redirect them to a screen with definitions for all the possibly proposed authentication schemes.

Figure 11: Recommendation of the tool prototype

In addition to the above, though the Options button in the top menu, a user with the adequate permissions can modify the weights given to the criteria and contexts by the application. This is provided so that the tool can be adapted according to the needs of specific companies or to update the knowledge base through the years, based on possible new trends or technologies that may appear. Fig. 12 shows the screen utilized for modifying the usability and security weights of the application contexts.

Figure 12: Recommendation of the tool prototype

6 Validation

The Case Study methodology was used to validate that the recommendations given by the framework were adequate in the reality of software development. The PSDC collaborated with the relevant information of some of their existing projects to perform the case studies. The results of the case studies have already been shown in [11] and [12]. However, with the objective of providing the validation of the research in a more comprehensive manner, this work also presents the design and planning of the case studies. Thus, the design and planning of the case studies is presented next, followed by their application and discussion of results.

6.1 Design and Planning

The planning of the case studies has been done following the guidelines of [14]. Thus, the following elements have been defined:

- *Objective:* To validate the adequacy of the authentication scheme and method recommendations of the Kontun Framework, when applied in software development environments.
- *The Case:* Two kinds of cases are studied. Firstly, five existing applications belonging to projects from the PSDC are used to compare the authentication schemes or methods implemented in them against the ones that the Kontun Framework would recommend. Secondly, four hypothetically defined cases are utilized to compare the authentication scheme or method that experts from the PSDC would implement for them against the one that the Kontun Framework would recommend. Moreover, half of the hypothetical case studies were devised considering the features of two of the existing application case studies, which allows for further comparisons.
- *Theory:* The knowledge base acquired through the SLR and S&I, as well as the Kontun Framework itself, were used as the frame of reference for the case studies.
- *Research Questions:* Based on the previously stated objective, the following research questions were defined: (i) are the recommendations of the Kontun Framework adequate to the reality of software development environments? (ii) do the recommendations of the Kontun Framework coincide with the implemented authentication techniques of existing applications? (iii) are the recommendations of the Kontun Framework in line with those given by industry experts?
- *Methods:* The data of the case studies was collected through observations and semi-structured interviews. These are described in-depth in the following sub-section.
- *Selection Strategy:* The data for the realization of these case studies was obtained through the PSDC, which provided the cases to study, as well as the experts to interview.

6.2 Data Gathering

Data for the realization of the case studies has been obtained through a first degree approach. This means that the researcher has been in direct contact with the subjects to collect data in real time [14]. Specifically, strategies of observations and interviews were utilized for collecting the data. These are described next. Secondly, interviews were performed to the experts of the PSDC for evaluating the hypothetically defined case studies.

6.2.1 Observations

Observations were used for identifying the relevant information of the existing projects of the PSDC. This was done through direct conversations with the people in charge of every project, who provided insight on the general usability and security features of the developed application, as well as the average budget available for implementing authentication techniques and its target context.

The observations of this research used a low degree of interaction by the researcher and low awareness of being observed of the subject approach [14]. This is because, although the information was obtained through direct conversations, the researcher did not have an involvement in the development of the studied applications.

6.2.2 Interviews

Interviews were used for obtaining input from experts of the PSDC regarding their authentication technique recommendations for the hypothetically defined case studies. These interviews were performed in a semi-structured

manner, utilizing a mix of open and closed questions, as well as possessing a descriptive and explanatory objective [18].

A total of 10 industry experts were interviewed and each of them gave their appreciations on each of the four hypothetical case studies, for a total of 40 answers.

6.3 Case Studies Based on Existing Applications (CSEA)

Having defined the protocol used for performing the validation, the realization of the case studies based on existing applications is provided next. It was possible to access a total of five applications that have been developed or that are on development by the PSDC. Some of these belong to projects for external clients, whereas others are internal projects. In the case of the external projects, the privacy of the clients of the PSDC was ensured.

6.3.1 CSEA1

This was an internal web application to be used by the PSDC's employees, which did not consider sensitive information as it was developed mainly for informal events. Thus, the importance given to *security* was *low*, whereas it required a *high usability* as well as *low costs*.

The implemented authentication method for this application was two-factor authentication by combining text passwords and OTP. On the other hand, the Kontun Framework would recommend the implementation of text passwords or biometrics in a single-factor manner. This discrepancy is partially explained, however, as employees utilized this internal project as a means for learning and practicing new technologies, thus not considering the application's requirements when deciding what authentication scheme or method to implement.

6.3.2 CSEA2

This is a system used for physically maintaining sensitive information of an external client protected from unwanted intruders. Due to this, *usability is not important*, but the *importance of security is high*. There was *no restriction regarding costs*.

The implemented authentication method was that of two-factor authentication combining text passwords and smart cards. On the other hand, the Kontun Framework would recommend the use of one of the following three-factor combinations: TP+OTP+BB, GP+SC+BB, GP+OTP+BB, GP+MB+BB and GP+OTP+P/F. Due to the system's features, the framework's answer tries to maximize security, which is the reason that three factors are considered instead of two.

6.3.3 CSEA3

This is an internal project used for generating reports that contain sensitive information of the PSDC. Additionally, this application is to be used by people that are not experts in computing. Due to the above, *both security and usability are important*. Moreover, since it is an internal project with low priority, *costs must be kept low* as well.

At the time of applying the case studies, the application was still in development. The authentication scheme that was being considered for implementation was that of text passwords, although it was not a final decision yet. On the other hand, the Kontun Framework would recommend the use of one of the following two-factor combinations: TP+SC, GP+BB and TP+MB.

6.3.4 CSEA4

This is an external project that consists of an application that works as a point of sale, thus working with sensitive commercial information and requiring *high security*. On the other hand, the application requires to be quickly available for use by the vendors while interacting with clients, thus *usability is important* as well. Although the budget for the application is high, only a small part of it is considered towards the implementation of authentication, thus also requiring *low costs*.

The implemented authentication method was that of two-factor authentication combining text passwords and mobile-based authentication. The Kontun Framework would recommend the use of TP+MB or TP+SC. In this case, the implemented and recommended authentication methods coincide.

6.3.5 CSEA5

This is an application for an external client that allows its users to maintain non-sensitive records of their information. Since the information is not sensitive, *security is not as important*. *Usability should be important*, but the client is not willing to invest in anything that could make them modify their policies, thus forcing the need of *low costs* as well.

The implemented authentication scheme is that of OTP. However, this OTP is used in many applications in the client's company and is hard to change for a single application, thus forcing the need to implement this authentication

scheme. On the other hand, the Kontun Framework would recommend the implementation of behavioral biometrics, text passwords or graphical passwords in a single-factor manner.

6.4 Case Studies Based on Hypothetical Applications (CSHA)

After realizing the case studies based on existing applications, the hypothetical case studies were performed. As previously stated, this considered the realization of interviews to experts from the PSDC for comparing the recommendations given by them against those of the Kontun Framework.

6.4.1 CSHA1

The first hypothetical case study considers an application with *high usability*, *low security*, and *limited budget* for the context of common web applications. This case study was devised based on CSEA1.

When asked, all ten industry experts mentioned that they would recommend the implementation of text passwords for this case study, which aligns with one of the recommendations that would be given by the Kontun Framework.

When they were informed that the framework's second recommendation was that of behavioral biometrics, only 40% of the interviewees were in agreeance with such a suggestion. However, through the first half of the interviews, it could be observed that the interviewees did not fully grasp how behavioral biometrics worked. Thus, for the second half of interviewees, these were trained about them. This proved to be useful, as for the latter half the acceptance rate of this recommendation was notably higher in comparison to the former half (60% versus 20%, respectively).

Finally, when asked if they would implement a two-factor authentication method for this application, 80% of the industry experts said that they would not implement such a method.

6.4.2 CSHA2

The second hypothetical case study considers an application with *low usability*, *high security*, and *no limits in budget* for the context of banking and commerce.

When asked, half of the industry experts mentioned that they would recommend the implementation of a two-factor authentication method. The other half mentioned that they would recommend the implementation of a three-factor authentication method. The Kontun Framework would also recommend the implementation of a three-factor authentication method, thus aligning with half of the experts. However, when they were informed that the framework's recommendation was that of three-factor authentication, all ten experts coincided that it was an adequate recommendation. Some even commented that it was more adequate than their two-factor recommendation.

6.4.3 CSHA3

The third hypothetical case study considers an application with *high usability*, *high security*, and a *limited budget* for an application for generating reports (this would be considered in the category of Other Context for the Kontun Framework). This case study was devised based on CSEA3.

When asked, four of the industry experts mentioned that they would recommend the implementation of either text passwords or graphical passwords for this case study. The other six experts mentioned that they would recommend the implementation of a two-factor authentication method, which aligns with the recommendation that would be given by the Kontun Framework.

When they were informed of the framework's recommendations, 90% of the interviewees agreed with at least one of the two-factor recommendations given by the framework.

Finally, when asked if they would implement text passwords as a single-factor authentication scheme for this application, 60% of the industry experts said that they would consider that such a scheme would be unsuited for this application.

6.4.4 CSHA4

The fourth hypothetical case study considers the extreme case of a client requiring an application that *does not need a high security*, *does not need a high usability*, and *does not have budget limitations* for a cloud computing context.

When asked, nine out of the ten industry experts mentioned that they would recommend the implementation of text passwords for this case study. This does not align to the Kontun Framework's recommendation, as its recommendation would be to implement a two-factor authentication method.

Regardless of the above, when they were informed that the framework's logic for this recommendation was that a two-factor solution would be one that values neither security nor usability as high, 80% of the interviewees agreed to such logic, mentioning that a more adequate answer would require human intervention to analyze the problem properly.

6.5 Discussion

To synthesize the above information, Table 12 presents the information regarding CSEA, showing, for each of them, the involved case study, the implemented authentication method and the framework's recommendation, whereas Table 13 presents the information regarding CSHA, showing, for each of them, the involved case study, the most recommended authentication method by industry experts, the framework's recommendation and the acceptance rate of the framework's recommendation. Additionally, Table 14 presents once more the CSEA that have been used as a base for a CSHA, showing, for each of them, the involved case study, the implemented authentication method, the experts' recommendation, the framework's recommendation, and the acceptance rate of the framework's recommendation. In these tables, 2FA stands for two-factor authentication, whereas 3FA stands for three-factor authentication.

Table 12: Summary of case studies based on existing applications, adapted from [11]

Involved Case Study	Implemented Authentication Method	Framework's Recommendation
CSEA1	2FA (TP + OTP)	TP
CSEA2	2FA (TP + SC)	3FA (TP + OTP + BB)
CSEA3	TP	2FA (TP + SC)
CSEA4	2FA (TP + MB)	2FA (TP + MB)
CSEA5	OTP	BB

Table 13: Summary of case studies based on hypothetical applications, adapted from [11]

Involved Case Study	Experts' Recommendation	Framework's Recommendation	Acceptance Rate
CSHA1	TP	TP	100%
CSHA2	2FA / 3FA	3FA	100%
CSHA3	2FA	2FA (TP + SC)	90%
CSHA4	TP	2FA	80%

Table 14: Summary of case studies based on existing applications with a hypothetical counterpart, adapted from [11]

Involved Case Study	Implemented Authentication Method	Experts' Recommendation	Framework's Recommendation	Acceptance Rate
CSEA1 and CSHA1	2FA (TP + OTP)	TP	TP	100%
CSEA3 and CSHA3	TP	2FA	2FA (TP + SC)	90%

In general, the recommendations given by the Kontun Framework align with those given by industry experts. On the other hand, although the coincidence rate is low for the CSEA, most of these discrepancies were due to specific situations involving the specific projects, such as the client demanding the use of a determined authentication scheme.

The most discrepancies on the CSHA come from CSHA1 and CSHA4. As for CSHA1, the reason lies mainly on behavioral biometrics, which can be attributed to the certain lack of knowledge or experience regarding this authentication scheme that could be observed in the interviewees. After training the second half of interviewees on this authentication scheme, it was possible to observe that the acceptance rate increased considerably.

For CSHA4, although no expert considered the use of two-factor authentication, most of them agreed to the framework's recommendation when they were notified about it. From the realization of the interviews, it can be inferred that the problem lies mainly in that the framework can only give an answer based on the received information, thus requiring a human to obtain this information in order to recommend a more adequate scheme or method.

When asked if they would implement the authentication methods considered in CSEA1 and CSEA3, most of the interviewees align with the framework's answer by mentioning that they would implement said authentication methods in those contexts.

7 Conclusions and Future Work

The main objective of this research was to cover the observed gap in literature regarding an adequate method for the comparison and selection of authentication schemes and methods. As a result, the Kontun Framework has been created, which allows the selection of the most appropriate multi-factor authentication methods for multiple contexts.

The existence of this framework will be of use for software developers to adequately select the authentication techniques that they should implement in their applications, strongly reducing the bias when taking this decision. This also helps to obtain more robust applications, as they would have the adequate levels of security and usability that they require.

On the other hand, this framework is valuable to the academia as it provides insight in the topic of decision criteria for authentication techniques. Moreover, based on the results of the performed SLR, no other framework that considered as many comparison and selection criteria, both single-factor and multi-factor authentication, and multiple possible application contexts, could be found, making the Kontun Framework of interest both for the industry and the academia.

The existence of a tool prototype allows easy use of the presented framework, as it simplifies the need of performing the mathematical calculations associated to it. The average time for obtaining a recommendation using the tool prototype is no longer than 5 minutes, preventing software developers from having to invest a long amount of time deciding what authentication technique to implement.

The framework's validity has been demonstrated through the realization of case studies in collaboration with the PSDC. The results of these case studies have been favorable, which allows trusting the recommendations given by the framework. There is added value in the fact that this validation has been done in collaboration with the industry, as the framework is meant for its use both in academic and industrial environments.

In line with the above, the knowledge base used for the definition of the framework has also been obtained not only from the academia, but also from the industry. In the case of the latter, a S&I strategy has been utilized for obtaining the perspectives of industry experts regarding authentication techniques and criteria for their comparison and selection. In the case of the former, an extensive SLR was performed to identify existing authentication schemes and multi-factor authentication methods, as well as the documented criteria used for their comparison and selection.

The realization of the SLR is especially highlighted, as it provides a vast knowledge base on the topic of authentication schemes and methods, while also identifying possible topics that have not been sufficiently covered, such as application contexts that have not often been considered.

Specifically for this work, the previously performed SLR, which covered publications until 2016, has been updated with publications since 2017 to date. This has allowed to update the previously obtained knowledge base while also identifying trends in publications from recent years. Namely, there has been an increasing amount of research on the comparison and selection of authentication techniques, as well as three-factor authentication, while on the other hand, research on single-factor authentication has been declining in favor of researching multi-factor authentication.

When analyzing the application contexts reviewed in literature in recent years, smart environments and the internet of things are highlighted. These two contexts had not been considered by the Kontun Framework since there were not many publications proposing authentication techniques for them until 2016. However, since 2017 there have been various publications tackling these contexts, especially in the case of internet of things, as there are even three publications that address the evaluation of authentication techniques for this context. Thus, it would be feasible to incorporate these contexts to the knowledge base utilized by the Kontun Framework. However, doing so would require realizing an adequate validation of the recommended schemes and methods through, for example, more case studies.

Regarding future research for this work, a short-term topic would be to realize the mentioned validation for incorporating smart environments and the internet of things as contexts considered by the framework. This could also be done through collaborations with other software development companies that focus on other application contexts. In the long term, it would be of interest to adapt the framework for it to work as a recommendation system. The main quality of these systems is that the answers given by them adapt by themselves based on the framework's usage through time, thus providing more precise recommendations. In the case of industry, it would be useful that the framework not only recommends what scheme or method to implement, but also a possible implementation of said scheme or method in distinct programming languages. Additionally, the topic covered by the framework could possibly be expanded to other security-related topics, such as authorization. Finally, the tool prototype can be refined to obtain a complete software product for applying the framework.

Acknowledgements

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

References

The list containing the references of the 982 accepted publications from the first stage of the systematic literature review can be found in <http://colvin.chillan.ubiobio.cl/mcaro/>, whereas the list containing the references of the 450 accepted publications from the second stage of the systematic literature review can be found in <http://bit.ly/3o81gA5>. The following is the bibliography that has been directly referenced on the article. Publications in this bibliography may or may not be included in the previous links as well.

- [1] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021-2040, 2003.
- [2] C. Rathgeb and A. Uhl, "Two-factor authentication or how to potentially counterfeit experimental results in biometric systems," in *International Conference Image Analysis and Recognition*, 2010: Springer, pp. 296-305.
- [3] H. Al-Assam, H. Sellahewa, and S. Jassim, "On security of multi-factor biometric authentication," in *2010 International Conference for Internet Technology and Secured Transactions*, 2010: IEEE, pp. 1-6.
- [4] 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.
- [5] D. Pointcheval and S. Zimmer, "Multi-factor authenticated key exchange," in *International Conference on Applied Cryptography and Network Security*, 2008: Springer, pp. 277-295.
- [6] D. Stebila, P. Udupi, and S. Chang, "Multi-factor password-authenticated key exchange," in *Proceedings of the Eighth Australasian Conference on Information Security-Volume 105*, 2010: Australian Computer Society, Inc., pp. 56-66.
- [7] 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 *2012 IEEE Symposium on Security and Privacy*, 2012: IEEE, pp. 553-567.
- [8] A. Forget, S. Chiasson, and R. Biddle, "User-centred authentication feature framework," *Information & Computer Security*, vol. 23, no. 5, pp. 497-515, 2015.
- [9] I. Velásquez, A. Caro, and A. Rodríguez, "Identifying Comparison and Selection Criteria for Authentication Schemes and Methods," in *Simposio Argentino de Ingeniería de Software (ASSE)-JAIIO 46 (Córdoba, 2017)*. 2017.
- [10] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," *Information and Software Technology*, vol. 94, pp. 30-37, 2018.
- [11] I. Velásquez, A. Caro, and A. Rodríguez, "Kontun: A Framework for recommendation of authentication schemes and methods," *Information and Software Technology*, vol. 96, pp. 27-37, 2018.
- [12] I. Velásquez, A. Caro, and A. Rodríguez, "Multifactor Authentication Methods: A Framework for Their Comparison and Selection," *Computer and Network Security*, p. 87, 2019.
- [13] I. Velásquez *et al.*, "How Developers Tackle Authentication in Their Applications," Nisum Technologies, 2017. <http://insights.nisum.com/2017/10/09/white-paper-how-developers-tackle-authentication-in-their-applications/>.
- [14] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," *Empirical software engineering*, vol. 14, no. 2, pp. 131-164, 2009.
- [15] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.
- [16] M. S. Litwin and A. Fink, *How to measure survey reliability and validity*. Sage, 1995.
- [17] M. Genero Bocco, J. Cruz Lemus, and M. Piattini Velthuis, *Métodos de investigación en ingeniería del software*. Ra-Ma Editorial, 2014.
- [18] C. Robson, *Real world research: A resource for social scientists and practitioner-researchers*. Wiley-Blackwell, 2002.
- [19] N. Kock and F. Lau, "Information systems action research: serving two demanding masters," *Information Technology & People*, vol. 14, no. 1, 2001.
- [20] Y. Wadsworth, *What is participatory action research?* Action Research Issues Association, 1993.
- [21] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," presented at the Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2006.
- [22] S. Choi and D. Zage, "Addressing insider threat using "where you are" as fourth factor authentication," in *2012 IEEE International Conference on Security Technology (ICCST)*, 2012: IEEE, pp. 147-153.
- [23] T. S. Algaradi and B. Rama, "Big Data Security: A Progress Study of Current User Authentication Schemes," in *2018 4th International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 2018: IEEE, pp. 68-75.
- [24] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of multi-factor authentication for securing advanced IoT applications," *IEEE Network*, vol. 33, no. 2, pp. 82-88, 2019.
- [25] 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.

- [26] C. Eliasson, M. Fiedler, and I. Jørstad, "A criteria-based evaluation framework for authentication schemes in IMS," in *2009 International Conference on Availability, Reliability and Security*, 2009: IEEE, pp. 865-869.
- [27] A. J. Palmer, "Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA)," *computers & security*, vol. 29, no. 7, pp. 785-806, 2010.
- [28] K. Altinkemer and T. Wang, "Cost and benefit analysis of authentication systems," *Decision Support Systems*, vol. 51, no. 3, pp. 394-404, 2011.
- [29] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes," presented at the Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 2016.
- [30] J. Y. Kim, "Efficiency of Paid Authentication Methods for Mobile Devices," *Wireless Personal Communications*, vol. 93, no. 2, pp. 543-551, 2017.
- [31] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems," *Journal of Network and Computer Applications*, vol. 87, pp. 1-19, 2017.
- [32] V. Borodavka and M. Tsuranov, "Biometrics: analysis and multi-criterion selection," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2018: IEEE, pp. 320-325.
- [33] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081-4092, 2018.
- [34] K. Hussain, N. Jhanjhi, H. Mati-ur-Rahman, J. Hussain, and M. H. Islam, "Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes," *Journal of King Saud University-Computer and Information Sciences*, 2019.
- [35] D. Korać and D. Simić, "Fishbone model and universal authentication framework for evaluation of multifactor authentication in mobile environment," *Computers & Security*, vol. 85, pp. 313-332, 2019.
- [36] J.-B. Subils *et al.*, "A Dual-Task Interference Game-Based Experimental Framework for Comparing the Usability of Authentication Methods," in *2019 12th International Conference on Human System Interaction (HSI)*, 2019: IEEE, pp. 95-100.
- [37] V. Zimmermann, N. Gerber, P. Mayer, M. Kleboth, A. von Preuschen, and K. Schmidt, "Keep on rating—on the systematic rating and comparison of authentication schemes," *Information & Computer Security*, 2019.
- [38] S. Z. Nizamani, S. R. Hassan, and R. A. Shaikh, "TQ-Model: A New Evaluation Model for Knowledge-Based Authentication Schemes," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2763-2778, 2020.
- [39] D. Singh, B. Kumar, S. Singh, and S. Chand, "Evaluating Authentication Schemes for Real-Time Data in Wireless Sensor Network," *Wireless Personal Communications*, vol. 114, no. 1, pp. 629-655, 2020.
- [40] G. J. W. Kathrine and E. Kirubakaran, "Four-factor based privacy preserving biometric authentication and authorization scheme for enhancing grid security," *International Journal of Computer Applications*, vol. 30, no. 5, 2011.
- [41] A. K. Nag and D. Dasgupta, "An adaptive approach for continuous multi-factor authentication in an identity eco-system," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, 2014: ACM, pp. 65-68.
- [42] Z. Cui, Y. Zhao, C. Li, Q. Zuo, and H. Zhang, "An Adaptive Authentication Based on Reinforcement Learning," in *2019 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, 2019: IEEE, pp. 1-2.
- [43] K. Matsuo, A. Kanai, T. Hatashima, and S. Tanimoto, "Dynamic Authentication Method Dependent on Surrounding Environment," in *2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)*, 2018: IEEE, pp. 855-857.
- [44] N. Al-Taleb and R. Zagrouba, "Authentication Scheme for IoT," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, 2020: IEEE, pp. 1-5.
- [45] W. Li and P. Wang, "Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new construction," *Future Generation Computer Systems*, vol. 101, pp. 694-708, 2019.
- [46] A. Bruun, K. Jensen, and D. Kristensen, "Usability of Single-and Multi-factor Authentication Methods on Tabletops: A Comparative Study," in *International Conference on Human-Centred Software Engineering*, 2014: Springer, pp. 299-306.
- [47] M. Anwar and A. Imran, "A comparative study of graphical and alphanumeric passwords for mobile device authentication," in *CEUR Workshop Proceedings*, 2015, vol. 1353, pp. 13-18.
- [48] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," *Computers & Security*, vol. 95, p. 101745, 2020.

- [49] M. U. Aslam *et al.*, "A survey of authentication schemes in telecare medicine information systems," *Journal of medical systems*, vol. 41, no. 1, pp. 1-26, 2017.
- [50] 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.
- [51] 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.
- [52] R. Madhusudhan and R. C. 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.
- [53] S. Choksi, "Comparative Study on Authentication Schemes for Cloud Computing," *International Journal of Engineering Development and Research*, vol. 2, no. 2, 2014.
- [54] 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.
- [55] K. C. Park, J. W. Shin, and B. G. Lee, "Analysis of authentication methods for smartphone banking service using ANP," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 8, no. 6, pp. 2087-2103, 2014.