Revista de Sistemas de Informação da FSMA
n. 31 (2023) pp. 69-75

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TRILHA PRINCIPAL

Characteristics and Main Threats about Multi-Factor Authentication: A Survey

Wesley dos Reis Bezerra, *PhD Candidate, PPGCC/UFSC*,
Carlos Becker Westphall, *Prof. Dr. PPGCC/UFSC*,

***Abstract*—This work reports that the Systematic Literature Review process is responsible for providing theoretical support to research in the Threat Model and Multi-Factor Authentication. However, different from the related works, this study aims to evaluate the main characteristics of authentication solutions and their threat model. Also, it intends to list characteristics, threats, and related content to a state-of-art. As a result, we brought a portfolio analysis through charts, figures, and tables presented in the discussion section.**

***Index Terms*—internet of things, authentication, constrained devices, fog computing**

I. Introduction

Our work reports the Systematic Literature Review process responsible for providing theoretical support to research in the intersection of Threat Model (TM) and Multi-Factor Authentication (MFA) areas. Additionally, it aims to build a bibliographic portfolio capable of guiding the discussions in that area and being the theoretical support necessary for put forward the previously cited research areas.

Specifically, the present work focuses on multi-factor authentication. That focus is one of many sub-areas of authentication, a classical area of security that has evolved into wide-ranging sub-areas. Some related works in this sub-area range from authentication schemes [1], biometrics storage [2], the diversity between authentication factors [3]–[5]. However, different from our work, the selected documents (portfolio) evaluated the main characteristics of authentication solutions and their threat model.

This work searches for publications on threat models for multi-factor authentication. With this publication, we intend to list characteristics, threats, and related content to state-of-art research in MFA. Consequently, white papers, patents, or fewer academic documents were removed from the portfolio selection. In general, this review aims to answer the following research questions:

- Q1 what are the **main articles** in the selected research area?
- Q2 what are the **main characteristics** intended by the analyzed authentication solutions?
- Q3 what are the **main threats** listed in the threat models that appear in the selected portfolio?

As for paper organization, this work continues with the Systematic Literature Review in section II; the sequence discussed the results in III. The IV, the conclusions, and future work for this section are brought.

Autor correspondente: Wesley dos Reis Bezerra, *wesleybez@gmail.com*

TABLE I
List of Abbreviations

Abbreviation	Meaning
CR	Challenge-Response
DDoS	Distributed Denial of Service
DFD	Data Flow Diagram
MFA	Multi-Factor Authentication
OTP	One-Time Password
SLR	Systematic Literature Review
SSO	Single Sign-On
TM	Threat Model
U2F	Universal 2nd Factor
TTS	Text-To-Speech

II. Systematic Literature Review (SLR)

The systematic literature review is a process/methodology whose goals is to promote the reduction of bias in scientific research [6]. However, it is not limited to this type of research [7], [8], but expands its results to constructing didactic material, classes, and books, a solid base for building a knowledge base.

In this work, we used the adapted ProKnow-C [9] methodology for the Systematic Literature Review methodology. Such methodology consists of four macrosteps: (i) portfolio selection, (ii) systematic review, (iii) bibliometrics, and (iv) research questions. Nevertheless, the research questions were already established a priori, and the answer to the research questions replaced the last step.

In this section, the macrosteps of (i) portfolio selection and (ii) systematic review will be further explored. The portfolio was chosen through these macro-steps in a documented and replicable manner. Additionally, the lenses (points of view) were chosen, analyzed, and contributed to the successful conclusion of this study. Thus, this review phase is the most important in this work.

The search term used in this review is given by the following condition:

$$'threatmodel'\ AND\ 'multi-factor\ authentication'\ AND\ (LIMIT-TO(DOCTYPE,'ar')\ OR\ LIMIT-TO(DOCTYPE,'cp')\ ORLIMIT-TO(DOCTYPE,'re')) \quad (1)$$

The files used during the systematic review process are available at the following link[1].

A. Portfolio Selection

This macrostep is a systematic way for selecting articles that comprises this study's final portfolio of base articles. This portfolio represents well the research object, the chosen cut, and the purpose of this cut in the research. Therefore, concise but representative of the state-of-the-art in the researched area.

In this SLR, the research object is state-of-the-art Threat Models for Multi-Factor Authentication. Thus, the object of study can be translated into the query-string (1), which is limited to articles (ar), reviews (re), and conference papers (cp).

TABLE II
INCLUSION AND EXCLUSION CRITERIA FOR SELECTION OF WORKS - IX OR EX, ARE USED FOR INDEXING THE CRITERIA, WHERE: THE PREFIX I DESIGNATES INCLUSION CRITERIA, THE PREFIX E DESIGNATES EXCLUSION CRITERIA, AND THE X MUST BE REPLACED BY THE COUNT OF THE NUMBER OF CRITERIA IN EACH CASE.

i1	documents published from 2012
i2	documents in English
e1	impact factor less than 1.0
e2	repeated work report
e3	document not available in full

The inclusion and exclusion criteria from Table II were used as a guide for selecting works. As for inclusion, criterion (i1) can be mentioned regarding the maximum age of the articles being eleven years old, and (i2) regarding the articles reporting the research in English. As for the exclusion criteria, criterion (e1) indicates removing articles in sources that have the impact factor[2] lower than 1.0, the (e2) indicates that repeated articles or that are a repeated report by the same researcher but in a different source are excluded, and (e3) evaluate works without full access to it content is removed from the analysis flow. Therefore, these criteria (Table II) helped to make a more deterministic selection and to avoid bias.

The portal chosen for the present work was SCOPUS[3] —the dl.acm[4] and ieeeXplorer[5] returned zero occurrences. This portal is accessible through the CAPES Periodic portal, and it is possible to access most of the articles published therein from the public higher education system. Furthermore, this portal allows us to download a database of research articles containing many fields relevant to the research. Which was sufficient because it incorporates many sources from different publishers in computer science.

TABLE III
DESCRIPTION OF THE ANALYZED ARTICLES DATABASE. AS FOR DATA TYPES: (I) INTEGER, (R) REAL, (T) TEXT.

field	type	description
index	i	sequential number used to identify the article in the workflow
title	t	field with document title
source	t	field with the name of the source where the document was published
citations	i	field that stores the number of citations of the work
impact factor	r	stores the impact factor value of the source where the article was published
hindex	i	stores the h-index value of the source where the article was published
year	i	stores the year of publication of the article

After the search, 35 articles were obtained for the initial database. Such articles were registered using a spreadsheet with fields already detailed in Table III. The spreadsheet management tool LibreOffice Calc[6] was used to tab the data and generate the datasets. For document management, the tool Mendeley[7] was used, which allows the organization of documents in folders and subfolders that replicate the portfolio selection steps. This tool considerably facilitated the work of organizing the documents in stages.

The inclusion and exclusion criteria were applied to the initial database, and the resulting data was the article portfolio (Table IV). Thus, at the end of the **initial phase**, 28 articles remained. Of the five excluded articles (e1), two did not have the impact factor [10], [11], four [12]–[15] had an impact factor less than 1.0, and one was not found even in Google Scholar.

Following the workflow, seven more articles [16]–[22] were removed in the **title reading phase** because their title had no relation with our research theme, leaving only 21 articles for the next phase.

Of these, another seven were excluded during the **abstracts reading phase** due to their low adherence to the desired research theme, leaving only 14 articles for the complete reading phase. The document used for the decision to exclude articles based on reading the abstracts can be seen at the link[8] of the project on GitHub.

After the **complete reading phase**, four articles were excluded, of which: one was a duplicate publication in different sources but by the same authors; the complete document was chosen [23]; the next article removed did not have free access to read the content of the work in its entirety [24]; the next one presented a very broad approach to the need for the present study [25]; and the last [26] diverged from the focus of the study, having as its specific object the study of mobile payment and not authentication. In this way, nine articles were left to compose the bibliographic portfolio of this work.

[1]https://github.com/wesleybez/mfar_tm
[2]Impact factor obtained in the Scimago Journal & Country Rank
[3]https://www.scopus.com/home.uri
[4]http://dl.acm.org/
[5]http://ieeexplore.ieee.org/
[6]https://pt-br.libreoffice.org/descubra/calc/
[7]https://www.mendeley.com/search/
[8]https://github.com/wesleybez/mfar_tm

TABLE IV
SYSTEMATIC BIBLIOGRAPHIC PORTFOLIO. THIS ARTICLE SET REPRESENTS THE SELECTION MADE AFTER THE VARIOUS STAGES OF ANALYSIS PERFORMED ON THE SET RESULTING FROM THE INITIAL SEARCH.

#	Reference	Title
a01	[27]	Mobile device integration of a fingerprint biometric remote authentication scheme
a02	[28]	Unified threat model for analyzing and evaluating software threats
a05	[29]	Secure multi-factor remote user authentication scheme for Internet of Things environments
a13	[30]	Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends
a17	[31]	A survey on multi-factor authentication for online banking in the wild
a18	[32]	Two-factor authentication scheme for mobile money: A review of threat models and countermeasures
a22	[33]	Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login
a30	[23]	An Extensive Formal Analysis of Multi-factor Authentication Protocols
a31	[34]	A broad review on non-intrusive active user authentication in biometrics
a32	[35]	Securing Voice Communication Using Audio Stenography

B. The Analysis Lenses Application

The following lenses were selected in this work: (a) the perspective of the threats analyzed in each work and (b) the characteristics of each model/scheme proposed in the articles listed in the portfolio. The threat analysis (a) aims to explain the main points of vulnerability within the authentication currently used, which deserve attention during the design and construction of an authentication mechanism. On the other hand, characteristics (b) are associated with additional functionalities or problem-solving results in each work in the portfolio.

Starting with the work of Cheng, Lee, and Hsu [27] that propose a lightweight user authentication scheme, which uses few resources, adopts hash functions, and promotes integration between the biometrics of a mobile device for authentication in systems. Its authentication scheme consists of four phases: registration, login, authentication, and password change. Its threat model aims to address the following threats: insider attack, stolen-verifier attack, impersonation attack, replay attack, reflection and parallel session attack, denial-of-service attack, and password guessing attack.

In Li *et al.* [28], a unified model that derives its operation from a threat tree is proposed. According to the author, its performance is superior to traditional threat trees. Its major gains are mitigating threats in a cheaper way using mitigation already cataloged in this new proposed model. Classification through STRIDE and threat representation through a Data Flow Diagram (DFD) is also used as process tools.

As for Dhillon and Kalra [29], the solution proposed is a multi-factor and mutual authentication. Aiming to be a robust and lightweight authentication, it uses XOR and hash functions for the authentication protocol and it also uses mutual authentication. It brought as desired security features mutual authentication, confidentiality, user anonymity, availability, forward secrecy, scalability, and attack resistance. Also, the same work lists in its attack model the following items: eavesdropping attack, impersonation attack, man-in-the-middle attack, denial of service attack, parallel session attack, password change attack, gateway node bypassing attack, and offline guessing attack; The proposal takes place in four phases: registration, login, authentication, and password change.

Ferrag, Maglaras, and Derhab [30] presented an important contribution to a discussion about unusual authentication factors. Some factors can be listed, such as touch dynamics, rhythm, ear shape, and arm gestures. The psychological and behavioral factors are also discussed in the work. His contribution is based on a large amount of related work to different types of authentication. It brought to light this evolution in the acquisition and processing of human signals, albeit subjective in some cases.

Sinigaglia *et al.* [31] provides a comprehensive survey on technologies and challenges of using multi-factor authentication, specifically for banks (financial system). Although its analysis took place from the perspective of user authentication and not from the device's point of view, some evaluations can be ported between these two perspectives. As a threat model, a model is presented with the following threats listed: device theft, duplicate authenticator, shoulder surfer, eavesdropping software, social engineer, man-in-the- browser, and man-in-the-mobile. Their threats generally focus more on intended objectives than the steps needed to consolidate the attack, as in other classic models.

Ali, Dida, and Sam [32] provide a deeper analysis of authentication schemes for mobile money. This work focused on user authentication for payments through mobile devices using two-factor authentication. The authors divide the threats in their model into five groups: attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity, and attacks against availability. For the present work, only the attack group against authentication was brought, consisting of: impersonation attacks, replay attacks, masquerade attack, spoofing attack, social engineering attack, phising attack, and trojan horse attack. This work also focuses on technologies for user authentication.

Sciarretta *et al.* [33] provided a formal analysis of an MFA with Single Sign On (SSO) where two e-health scenarios are used to support the analysis. As factors, a token authentication through One Time Password (OTP) and a Challenge-Response (CR) is used. The following threats are brought up: device

thief smartphone, device thief and IDCard, social engineering, shoulder surfer, App duplicator, leaking software, and malicious application. It can be noted that the analyzed proposal aims at user authentication, and due to this, some of the threats are directly addressed as problems with human users.

Thomas and Mathew [34] also showed an approach that considers behavior-based authentication factors. As an example of authentication factors used in this article, we can mention biosignals, emotion recognition, and typing pattern. Therefore, the authors comprehensively review non-intrusive active methods for user authentication. Still, his work has presented the importance of non-intrusive methods for authentication, which can be the basis of continuous and active authentication in future research on computer systems.

Moreover, there is the work of Jacome and Kremer [23], which proposed a formal analysis of multi-factor authentication. In this work, the authors evaluated Google 2-steps and FIDO's U2F through formal methods using applied pi-calculus and the Proverif tool[9]. The work also presented a threat model composed of the following threats: compromised passwords, network control, compromised platform, human aspects, and "trust this computer mechanism- threats very specific to the analyzed MFA models.

Finally, the work of Phips and Vassilev [35] proposed using steganography to encapsulate authentication data in audio communications. As a threat model, this work showed vulnerabilities specifically for voice, such as voice impersonation (deep fake), fake skill, side-channel attacks, voice synthesis, replay attacks, and technical exploitation. As presented, the technological advances allow tools to perform some attacks, such as text-to-speech (TTS) usage, cloned voices, interference, noise, and remote injection of inaudible commands.

The attacks listed in Table (V) have a wide range of impact, target audience, and security domain. As with DDoS, some can have major financial impacts on institutions and systems. Others have the target audience focused on specific users or devices, and the impact is associated with the level of clearance of that person in the system. As for the security domain, some attacks use technology to attack the network, the fragility of a chosen password; however, others focus on less technological issues, as with shoulder surfer and social engineering. In this way, it is important to know the possible threats to the system, as explained in the portfolio.

III. Results and Discussion

Through this work, it was possible to answer the three initial questions (Q1, Q2, and Q3) that motivated it. During its development, an SLR was created and the Figure 1 depicts the process through with the ten articles were selected as the final portfolio from an initial selection of 35 articles using Table II as criteria for initial document selection and the query-string (1) during the search.

As for Q1, a portfolio of nine articles was evaluated in detail and represents the state-of-the-art at the intersection of threat model and multi-factor authentication areas. During the process, the selected criteria helped to avoid bias and improve assertiveness in the —article selection, also helping in the reproducibility of this work. Moreover, the SCOPUS database proved sufficient as it incorporated several computer science sources and publishers. Additionally, selecting tools, variables, and spreadsheet templates made the work easier.

As for the characteristics (Q2) of the selected works, we can categorize them (Figure 2) into five different ones: lightweight authentication (2 articles), threat model methodology (1 article), authentication factors (3 articles), MFA for Banks (2 articles), and formal analyzes (2 articles). From these categories, it is possible to see that there is an effort for authentication to evolve to a lighter, more diversified form and for its process to be indubitably validated through formal methods. Therefore, there is also a concern about its use in financial institutions and how to assess its threats at a lower cost. In general, low cost and resource restrictions are key factors in multi-factor authentication and threat model research.

Finally, regarding threats (Q3), four documents were used for their listing (see Table V). Among the threats listed, none appeared in all the works, and they are distributed (Figure 2) in four occurrences (8.70%), three occurrences (13.04%), two occurrences (17.39%), and one occurrence (60.87%). A total of 23 distinct threats were listed in this survey, and they range (Figure 2-c) from confidentiality threats, which have the most items (20 threats), integrity (2 threats), and availability (1 threat) —with the fewest. Consequently, we notice that some types of threats appear more frequently, such as confidentiality, which is the category of threats with the highest occurrence, adding up to 86.95% of the works listed in Table V. This result is cause by the fact that threats linked to authentication are directly associated with reliability, involving privacy, information disclosure, and secrecy - not detailed in the CIA-based classification of Stallings [36].

In brief, we can say that by answering these three questions, it was possible to have a good representation of the state-of-the-art and the paths that research in multi-factor authentication and threat modeling has taken. Furthermore, textual items (tables and charts) and graphical items (schemes, graphs, and images) provide a set of artifacts[10] that support future research or updates of this work.

IV. Conclusion and Future Works

This work fully achieved its objectives by listing through the portfolio the main articles within the research area, bringing

[10]https://github.com/wesleybez/mfar_tm

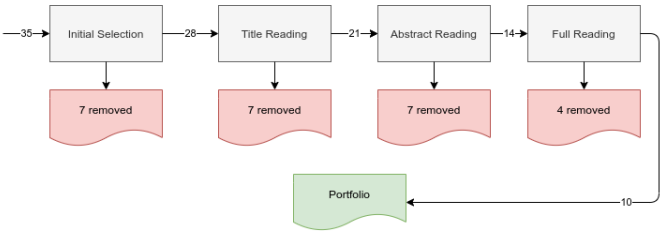

Fig. 1. Systematic Literature Review Workflow - the diagram shows in gray the processes, in red the removed documents, and in green the resulting portfolio.

[9]https://bblanche.gitlabpages.inria.fr/proverif/

TABLE V

CORRELATION BETWEEN THE SET OF ATTACKS CITED AND THE ARTICLES IN THE BIBLIOGRAPHIC PORTFOLIO. IN THE LINES IS LISTED THE SET OF ATTACKS, THE THIRD COLUMN CLASSIFIES THE ATTACK ((C)ONFIDENTIALITY, (I)NTEGRITY, AND (A)VAILABILITY), AND THE OTHER COLUMNS SHOW THE ARTICLES WHERE SUCH ATTACKS ARE MENTIONED. ALSO, • MEANS PRESENT IN THE ARTICLE, AND ¬ MEANS NOT PRESENT. FURTHER, NOT ALL ARTICLES APPEARED IN THE COLUMNS SINCE SOME DID NOT PRESENT A THREAT MODEL.

#	Attacks	CIA	[27]	[29]	[31]	[33]	[32]	[35]
01	Insider	C	•	¬	¬	¬	¬	¬
02	Stolen-Verifier	C	•	•	•	¬	¬	¬
03	Impersonation	C	•	•	¬	¬	•	•
04	Replay	I	•	¬	¬	¬	•	•
05	Reflection	C	•	¬	¬	¬	¬	¬
06	Parallel Session	C	•	•	¬	¬	¬	¬
07	Denial-of-Service	A	•	•	¬	¬	¬	•
08	Password Guessing	C	•	•	¬	¬	¬	¬
09	Eavesdropping	C	¬	•	•	•	¬	¬
10	Man-In-The-Middle	C	¬	•	•	¬	¬	¬
11	Password Change	C	¬	•	¬	¬	¬	¬
12	Gateway Node Bypassing	C	¬	•	¬	¬	¬	¬
13	Duplicate Authenticator	C	¬	¬	•	¬	¬	¬
14	Shoulder Surfer	C	¬	¬	•	•	¬	¬
15	Social Engineer	C	¬	¬	•	•	•	¬
16	Man-In-The-Browser	C	¬	¬	•	¬	¬	¬
17	Man-In-The-Mobile	C	¬	¬	•	¬	¬	¬
18	App Duplicator	C	¬	¬	¬	•	¬	¬
19	Malicious Application	C	¬	¬	¬	•	¬	¬
20	Masquerade	C	¬	¬	¬	¬	•	¬
21	Spoofing	C	¬	¬	¬	¬	•	¬
22	Phishing	C	¬	¬	¬	¬	•	¬
23	Trojan Horse	I	¬	¬	¬	¬	•	¬

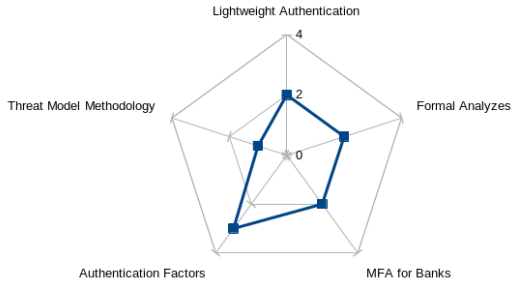

Fig. 2. Quantitative data obtained from the analysis of portfolio articles - Articles Categorization.

the main characteristics of solutions through the portfolio analysis, and presenting the main threats in the related literature. Also, it provides a quantitative analysis of the portfolio article content, discusses and comments on this, and reports it in Table V and Figure 2.

We can mention as additional contributions the analysis of the most relevant threats brought into the portfolio and their occurrence in different works. The list of most relevant threats to the area (Table V) brings a large and diverse set of possible threats. Although some are specific to some areas of activity (i.e., voice), they all contribute to forming a framework of security measures for authentication in its different factors.

It is important to monitor the area and the evolution of research in threat models and multi-factor authentication in future work —until the moment of this publication, only theses [37]–[39] were found in the intended area, more recently. Also, backward and forward snowballing processes must improve the specific knowledge acquired in each category. Therefore, an important evolution of this work is the refinement of the search through terms that focus on specific technologies such as 6G, Fog Computing, or continuous authentication.

REFERÊNCIAS

[1] S. A. Chaudhry, I. L. Kim, S. Rho, M. S. Farash e T. Shon, "An improved anonymous authentication scheme for distributed mobile cloud computing services," *Cluster Computing*, v. 22, n. 1, pp. 1595–1609, 2019.

[2] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi e A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Generation Computer Systems*, v. 85, pp. 76–87, 2018.

[3] L. Loffi, C. M. Westphall, L. D. Grüdtner e C. B. Westphall, "Mutual authentication with multi-factor in IoT-Fog-Cloud environment," *Journal of Network and Computer Applications*, v. 176, p. 102 932, 2021.

[4] A. Anakath, S. Rajakumar e S. Ambika, "Privacy preserving multi factor authentication using trust management," *Cluster Computing*, v. 22, n. 5, pp. 10 817–10 823, 2019.

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen e Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, v. 2, n. 1, p. 1, 2018.

[6] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey e S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, v. 51, n. 1, pp. 7–15, 2009.

[7] D. Moher, A. Liberati, J. Tetzlaff e D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *Annals of internal medicine*, v. 151, n. 4, pp. 264–269, 2009.

[8] D. Budgen e P. Brereton, "Performing systematic literature reviews in software engineering," em *Proceedings of the 28th international conference on Software engineering*, 2006, pp. 1051–1052.

[9] L. Ensslin, C. C. Mussi, L. C. Chaves e S. N. Demetrio, "It outsourcing management: The state of the art recognition by a constructivist research process and

bibliometrics," *JISTEM-Journal of Information Systems and Technology Management*, v. 12, pp. 371–392, 2015.

[10] S. Roy e C. Khatwani, "Cryptanalysis and improvement of ECC based authentication and key exchanging protocols," *Cryptography*, v. 1, n. 1, p. 9, 2017.

[11] R. L. De Souza, M. Vigil, R. Custódio, F. Caullery, L. Moura e D. Panario, "Secret sharing schemes with hidden sets," em *2018 IEEE Symposium on Computers and Communications (ISCC)*, IEEE, 2018, pp. 00 713–00 718.

[12] W. R. Simpson e K. E. Foltz, "Enterprise level security: insider threat counter-claims," em *Proceedings of the World Congress on Engineering and Computer Science*, vol. 1, 2017, pp. 1–6.

[13] W. R. Simpson e K. E. Foltz, "Insider Threat Metrics in Enterprise Level Security.," *IAENG International Journal of Computer Science*, v. 45, n. 4, 2018.

[14] P. J. Hawrylak, G. Louthan, J. Hale e M. Papa, "Practical Cyber-Security Solutions for the Science DMZ," em *Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning)*, 2019, pp. 1–6.

[15] B. C. Kara e C. Eyüpoğlu, "Sağlık 4.0'da Mahremiyet ve Güvenlik Sorunları Privacy and Security Problems in Healthcare 4.0," em *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, IEEE, 2020, pp. 1–12.

[16] C. Johansen e A. Jøsang, "Probabilistic modelling of humans in security ceremonies," em *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, Springer, 2014, pp. 277–292.

[17] W. Ma, K. Sartipi, H. Sharghigoorabi, D. Koff e P. Bak, "OpenID Connect as a security service in cloud-based medical imaging systems," *Journal of Medical Imaging*, v. 3, n. 2, p. 026 501, 2016.

[18] A. González-Burgueño e P. C. Ölveczky, "Formalizing and Analyzing Security Ceremonies with Heterogeneous Devices in ANP and PDL," em *International Conference on Fundamentals of Software Engineering*, Springer, 2019, pp. 129–144.

[19] J. Chen, "Risk communication in cyberspace: a brief review of the information-processing and mental models approaches," *Current opinion in psychology*, v. 36, pp. 135–140, 2020.

[20] R. Gupta, S. Tanwar, S. Tyagi e N. Kumar, "Machine learning models for secure data analytics: A taxonomy and threat model," *Computer Communications*, v. 153, pp. 406–440, 2020.

[21] Z. Lu, S. Yang, J. Liu, X. Wang e Y. Li, "Efficient FPGA implementation of high-speed true random number generator," *Review of Scientific Instruments*, v. 92, n. 2, p. 024 706, 2021.

[22] A. González-Burgueño e P. C. Ölveczky, "Formalizing and analyzing security ceremonies with heterogeneous devices in ANP and PDL," *Journal of Logical and Algebraic Methods in Programming*, v. 122, p. 100 685, 2021.

[23] C. Jacomme e S. Kremer, "An extensive formal analysis of multi-factor authentication protocols," *ACM Transactions on Privacy and Security (TOPS)*, v. 24, n. 2, pp. 1–34, 2021.

[24] F. Sinigaglia, R. Carbone, G. Costa e S. Ranise, "Mufasa: A tool for high-level specification and analysis of multi-factor authentication protocols," em *International Workshop on Emerging Technologies for Authorization and Authentication*, Springer, 2019, pp. 138–155.

[25] M. Mahbub, "Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics," *Journal of Network and Computer Applications*, p. 102 761, 2020.

[26] S. Bojjagani, V. Sastry, C.-M. Chen, S. Kumari e M. K. Khan, "Systematic survey of mobile payments, protocols, and security infrastructure," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–46, 2021.

[27] C.-L. Chen, C.-C. Lee e C.-Y. Hsu, "Mobile device integration of a fingerprint biometric remote authentication scheme," *International Journal of Communication Systems*, v. 25, n. 5, pp. 585–597, 2012.

[28] X. Li, K. He, Z. Feng e G. Xu, "Unified threat model for analyzing and evaluating software threats," *Security and Communication Networks*, v. 7, n. 10, pp. 1454–1466, 2014.

[29] P. K. Dhillon e S. Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments," *International Journal of Communication Systems*, v. 30, n. 16, e3323, 2017.

[30] M. A. Ferrag, L. Maglaras e A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Security and Communication Networks*, v. 2019, 2019.

[31] F. Sinigaglia, R. Carbone, G. Costa e N. Zannone, "A survey on multi-factor authentication for online banking in the wild," *Computers & Security*, v. 95, p. 101 745, 2020.

[32] G. Ali, M. Ally Dida e A. Elikana Sam, "Two-factor authentication scheme for mobile money: a review of threat models and countermeasures," *Future Internet*, v. 12, n. 10, p. 160, 2020.

[33] G. Sciarretta, R. Carbone, S. Ranise e L. Viganò, "Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login," *ACM Transactions on Privacy and Security (TOPS)*, v. 23, n. 3, pp. 1–37, 2020.

[34] P. A. Thomas e K. P. Mathew, "A broad review on non-intrusive active user authentication in biometrics," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–22, 2021.

[35] A. Phipps, K. Ouazzane, V. Vassilev et al., "Securing voice communications using audio steganography," *International Journal of Computer Network and Information Security (IJCNIS)*, 2022.

[36] W. Stallings, L. Brown, M. D. Bauer e M. Howard, *Computer security: principles and practice*. Pearson Upper Saddle River, 2012, vol. 2.

[37] R. Kumar, "Exploiting App Differences for Security Analysis of Multi-Geo Mobile Ecosystems," tese de dout., 2023.

[38] S. Jones, "SenderKeys Identified Mail," tese de dout., New Mexico Institute of Mining e Technology, 2022.

[39] K. Lee, "The Research-Practice Gap in User Authentication," tese de dout., Princeton University, 2022.