SWC Software Construction

RWTH AACHEN UNIVERSITY

The present work was submitted to the Research Group Software Construction

of the Faculty of Mathematics, Computer Science, and Natural Sciences

Bachelor Thesis

A Classification Approach for Authentication Methods

Ein Klassifikationsansatz für Authentifizierungsmethoden

presented by

Vincent Schmandt

Aachen, July 28, 2025

Examiner

Prof. Dr. rer. nat. Horst Lichter

Prof. Dr. rer. nat. Bernhard Rumpe

Supervisor

Alex Mattukat, M. Sc.

Acknowledgment

First and foremost, I would like to thank my supervisor Alex Mattukat for his guidance and constructive feedback throughout the process of writing this thesis. The discussions with him and his insights have greatly improved this thesis. I would also like to thank Prof. Dr. rer. nat. Horst Lichter for the opportunity to write this thesis at the Research Group Software Construction. I am grateful to him and Prof. Dr. rer. nat. Bernhard Rumpe for reviewing my thesis. Lastly, I would like to thank my friends and family for their patience and support during the writing of this thesis.

Vincent Schmandt

Abstract

Authentication plays a critical role in modern infrastructure and everyday life. Despite its importance, however, the landscape of authentication methods suffers from fragmented terminology, inconsistent classifications and limited visibility beyond the most common methods. There exists no comprehensive framework to systematically classify and compare authentication methods across domains and applications. To investigate which authentication methods exist, what properties they have and how they can be classified, we conducted a lightweight systematic literature review. We used LLM-assisted abstract screening to screen 1256 papers from IEEE Xplore and identified 457 relevant papers, of which 24 representatives were selected through semantic clustering using BERTopic and HDBSCAN for manual full-text analysis. We identified five primary classes of authenticators (knowledge-based, possession-based, biometric, context-based and hybrid authenticators), with biometric authentication being the most prevalent among the representatives. In addition to this, we identified 12 key facets that characterize authentication methods beyond the type of authenticator. Based on these two dimensions, we propose a split classification approach that combines a hierarchical classification of authenticators with a facetted classification of authentication methods to allow for a more detailed comparison of methods. By combining these two approaches, the more rigid and abstract classification of authenticators can be complemented by a more flexible and more easily adaptable facetted classification, which allows for easy extensions and modifications through future research. By providing an extensible and general classification approach for authentication methods, we aim to aid practitioners as well as future research in this field. The proposed classification can be used to systematically compare authentication methods and their properties and serve as a foundation for research into specific areas of authentication or new authentication methods. While our lightweight approach has limitations in terms of comprehensiveness compared to a full systematic literature review, we were able to successfully identify key patterns and characteristics of authentication methods and build a novel classification approach based on them.

Contents

List of Tables

List of Figures

List of Listings

1. Introduction

Contents

1.1. Background

Over the past decades, computer systems have become an integral part of daily life and now govern access to critical infrastructure, personal data, and other valuable resources. Consequently, the need to secure these systems has also quickly gained importance. One of the most important aspects in safeguarding any environment is ensuring that only authorized entities, which can be any acting component in a system including users, devices, and services, can access it and perform actions within it. This is achieved through authentication and authorization [Tem+24a]. While authorization determines what a given entity can do, authentication is the process of verifying the identity of an entity, making it a prerequisite for authorization [Int10]. With this, authentication stands at the core of any secure system and forms the basis for any form of access control. Therefore, choosing the right authentication approach and understanding its strengths and weaknesses is of critical importance to the security of any system.

Systems ranging from smartphones to online banking to corporate infrastructure rely on authentication methods to protect them against unauthorized access. Despite these systems providing very valuable access, they are frequently protected by weak authentication methods such as simple Personal Identification Numbers (PINs), passwords or even no authentication at all [Boc23; Yub24]. While it is well-established that these methods suffer from a variety of security issues, such as their vulnerability to phishing, credential stuffing and shoulder surfing [Has+25], they are still widely used due to their simplicity and user familiarity [WZZ19]. Since the advent of passwords for digital systems, however, many new authentication methods have been proposed which can provide superior security, usability, or both while often offering additional benefits as well.

A major roadblock in the adoption of these methods, in addition to the ubiquity of existing methods, is the fact that they are frequently not well documented and that their discoverability is poor. Their benefits and drawbacks are often not well laid out and while unique benefits are usually highlighted, drawbacks are not always addressed appropriately [Bon+12]. This makes it difficult to choose a fitting authentication method for a given use-case and can lead to suboptimal choices when architecting new systems and ultimately leads to the continued use of already established methods such as password authentication. This problem is compounded by the fact that the realm of authentication itself suffers from unclear language [Gol96], for example through the reuse of terms or due to contradictory definitions [AJ10]. Even the term authentication itself is used to refer to different concepts such as entity authentication, which is the topic of this thesis, and data authenticity verification, which is sometimes referred to as data authentication or message authentication [Shi07; JSY25].

Besides the aforementioned use-cases, authentication is also a key component in emerging technologies such as the Internet of Things (IoT) [JNR24], smart homes [Wan+22], interconnected self-driving cars [Rez+21] and many more. This large variety of use-cases and their accompanying wide range of requirements and individual constraints make it hard to choose the right authentication method that balances security, usability and other requirements.

Previous attempts at providing structure in this area typically focus on small subsets of the field of authentication, bounded by use-case or technology. Some for example focus solely on biometric authentication [Mah+18], authentication in IoT [AN22] or use in the medical domain [JNR24]. These related works are explored in more detail in chapter 3. More importantly, the previous works identified in our research each utilize their own partially overlapping terminology and do not work towards a unified framework. This lack of a common representation and classification of authentication methods is a key barrier to making secure authentication methods more comparable and accessible to researchers and ultimately end-users.

1.2. Research questions

Given these current problems that make it harder to use authentication effectively and to research authentication in general, this thesis aims to answer one overarching research question in order to lay the groundwork for future research into authentication methods and to provide a framework for further research into this field:

RQ0: How can we systematically describe and classify existing and future methods of authentication?

To address this complex problem, we first need an overview of existing methods to extract common properties and classes and identify use cases. Due to this complexity, **RQ1** deals with gaining an overview of the existing authentication landscape:

RQ1: Which methods of authentication exist?

Here the aim is not to provide an exhaustive list of all authentication methods in all their variety but rather to get a broad overview of which broader methods exist to gain an understanding of commonalities and differences between them in order to extract characteristics and ultimately classes, which is the goal of the second research question:

RQ2: Which characteristics of authentication methods can be used to group them into meaningful classes for systematic comparison?

This will ultimately allow us to answer the overarching research question **RQ0** and provide a framework for future research into authentication methods.

1.3. Contributions

To answer these questions, our research makes the following contributions:

- We provide a novel classification approach for authentication methods that can easily be extended when new authentication methods emerge or once more in-depth research is completed in a specific area. This approach allows for systematic comparison of methods across different technologies and use-cases.
- To address the large variety in terminology and the lack of clearly defined properties and classes of authentication methods, we provide a well-defined set of facets and hierarchical classes of authentication methods that allow for systematic classification. This enables the effective use and modification as well as extension of the classification.
- We create a catalog of authentication methods classified based on the proposed classification approach to validate its usefulness and to provide a foundation for future research.

For example, the proposed classification in combination with the catalog of authentication methods enables systematic selection of privacy-preserving machine-to-machine authentication methods for vehicular network deployments or high-robustness or passive, continuous human-to-machine authentication methods for smart home scenarios, each based on their specific requirements. We will explore using the classification in practice in chapter 8.

This thesis focuses on the description and classification of digital authentication methods (i.e., the specific methods used to verify identity claims) across domains and does not focus on any specific use-case or technology in order to provide a broad overview of the field. We include methods for authenticating entities of all kinds, including humans and machines. Authentication protocols (communication protocols used to exchange credentials or other information to perform authentication), authenticity verification (verifying the integrity or origin of data) and other related concepts such as authorization or access control are not the focus of this thesis. However, we do provide a brief overview of these concepts in chapter 2 to establish common ground and terminology for this thesis and to avoid any confusion that may arise from overlapping terminology.

Since initial research showed that there are many existing and proposed authentication methods, we utilize an *Large Language Model (LLM)*-assisted workflow with strong human review guardrails based on a lightweight Systematic Literature Review (SLR) to extract meaningful insights from the large amount of data.

1.4. Structure of this thesis

The rest of this thesis is organized as follows. In the next chapter, we cover the concepts and terminology that will be used throughout the thesis to establish common ground. Chapter 3 discusses previous work in describing and classifying authentication methods and also references different works on whose results the methodology of this thesis was based upon. In chapter 4, the methodology of performing our research is described in detail to allow for reproducibility. Chapters 5 to 7 describe our results and the insights we gained, and lastly, they are discussed in chapter 8 before drawing a conclusion and discussing future research directions in chapter 9.

2. Foundations

Contents

In order to be able to discuss aspects of different authentication methods, we must first establish a collection of common terms and definitions. The following section lays out clear definitions for the terms used throughout the thesis. Note, however, that due to the aforementioned overlaps in terms and definitions across this field of research, other works may utilize different language for the same concepts or the same language for an entirely different concept. We do attempt to also cover common synonyms as well as potentially confusing alternative meanings in this section, but we do not aim to be exhaustive in this effort.

2.1. Definitions

2.1.1. Authentication

Authentication is commonly used to refer to two different concepts [Shi07]:

- *Entity authentication*, which is the process of verifying the claimed identity of an entity, and
- *Authenticity verification*, which is the process of verifying the integrity or origin of data (such as a message or file). This process is also known as *data authentication* or *message authentication*.

For the purposes of this thesis, we define *authentication* as the process of verifying the claimed identity of an entity (i.e., entity authentication). More specifically, we follow the definition of an authentication process defined by NIST in *Digital Identity Guidelines: Authentication and Authenticator Management* [Tem+24b], which states: During the authentication process, an entity (the *claimant*) claims a specific *identity* and proves that they are in possession and control of an *authenticator* that substantiates one or more *authentication factors* associated with the claimed *identity* to demonstrate that they are the *subscriber* associated with that *identity* [Tem+24b]. This definition will be explained and expanded upon in the rest of this chapter.

All actors in the authentication process are entities, which we define as anything capable of acting autonomously. This includes people, devices, and services. Note that this definition

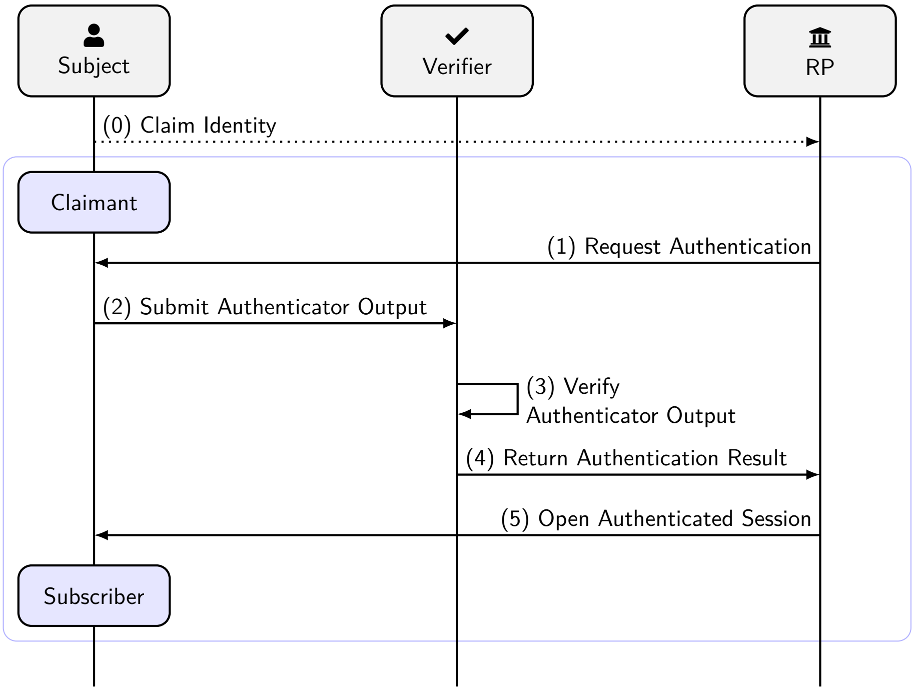

Subject
Verifier
RP
(0) Claim Identity
Claimant
(1) Request Authentication
(2) Submit Authenticator Output
(3) Verify
Authenticator Output
(4) Return Authentication Result
(5) Open Authenticated Session
Subscriber

Figure 2.1.: The authentication process, recreated based on [Tem+24b]

is intentionally broad to cover as many scenarios as possible. We distinguish between the following actors and roles they assume [Tem+24b]:

- *Subject*: The entity that is being authenticated.
- *Claimant*: The role that the subject assumes during the authentication process when they claim an identity.
- *Subscriber*: The role that the subject assumes when they have been successfully authenticated. This role is associated with the identity that the subject claimed during the authentication process. It is mostly used to refer to the subject after it has been successfully authenticated.
- *Verifier*: The entity that verifies the claimed identity of the claimant.
- *Relying Party (RP)*: The entity that relies on the authentication process to grant access to resources or services. This is usually the application the subject wants to access.

Generally, authentication occurs whenever a subject wants to access a resource or service that requires proof of their identity. This may be due to a variety of reasons such as access control or audit logging. The interaction between the actors during the authentication process is visualized in figure 2.1. Here, we can see that the subject initially claims an identity (0), thereby assuming the role of the claimant. The RP then requests the claimant to authenticate themselves (1) to prove their claimed identity. The claimant then submits the output of an authenticator that is bound to the claimed identity (2) to the verifier, which verifies the output of the authenticator (3) and informs the RP of the result of the authentication (4). If the authentication was successful, the RP can establish an authenticated session with the subject (5), which is then referred to as the subscriber and can access the resources or services provided by the RP in accordance with the permissions associated with the subscriber's identity as determined by the *authorization* process. In simpler systems, the verifier and RP are often part of the same service or application, while in more complex environments there is usually a shared verifier often called a *Single-Sign-On (SSO)* provider, which is external to the application (RP) itself.

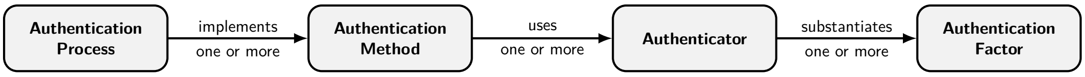


Figure 2.2.: The hierarchy of authentication concepts

Besides the actors and roles, the authentication process also involves other key concepts, also shown in figure 2.2, which we define as follows:

- *Authentication factor*: An authentication factor is a category of evidence that is used to verify a claimant's identity. The most common categories are *something the claimant knows* (knowledge), *something the claimant possesses* (possession), and *something the claimant is* (biometric) [Tem+24b], but some sources also include contextual factors such as location or time [Bar+22].

- *Authenticator*: An authenticator is something a claimant possesses and controls and that substantiates one or more authentication factors by embodying or generating evidence (which is called *authenticator output*). Examples are passwords (knowledge), hardware tokens (possession), or biometric features such as fingerprints (biometric) [Tem+24b]. Authenticators are often categorized based on the authentication factor(s) they substantiate (e.g., physical authenticator or multifactor authenticator) [Tem+24b].

- *Authentication method*: An authentication method is a specific technique used to verify a claimant's identity using one or more authenticators associated with the claimed identity. Examples include password authentication, PIN authentication, and fingerprint authentication. An authentication method that uses authenticators which cover multiple authentication factors is called a multifactor authentication method. Note that an authentication method can still be a single-factor authentication method if it uses multiple authenticators that substantiate the same authentication factors or a multifactor authentication method even if it uses only a single multifactor authenticator.

- *Authentication protocol*: An authentication protocol defines how authentication data is exchanged between claimant and verifier. It specifies the messages exchanged and cryptographic operations required. It is the concrete conceptual implementation of the authentication process [Tem+24b].

The relationship between these components is hierarchical as can be seen in figure 2.2. Each builds upon the previous one, with authentication factors being substantiated by authenticators, which are in turn used by authentication methods that are implemented in the form of authentication protocols.

2.1.2. Authentication, Identification and Authorization

In addition to the terminology discussed in the previous section, the distinction between *identification*, *authentication*, and *authorization* is not always clear and the lines between them are sometimes blurry. While these concepts are all related and all part of access control systems, they are usually distinct steps [Sye+13]:

- *Identification* determines the claimed identity of an entity, usually by asking the user to provide a unique identifier (such as a username or email address) that is associated with their account. The subject becomes a claimant when they claim an identity.
- *Authentication* verifies that claimed identity as described above. After successfully being authenticated, the subject becomes a subscriber associated with the claimed identity.
- *Authorization* determines the permissions associated with the subscriber's identity. Authorization is performed on the permissions associated with the subscriber's identity and determines what actions the subscriber may perform or what resources they may access.

While identification is often a distinct step prior to the authentication process, some authentication methods provide identification as part of the authentication process itself. The focus of this thesis lies on the authentication phase, which is the phase shown in figure 2.1, and specifically on the methods used to verify the identity of an entity, which are referred to as authentication methods.

2.2. Reference Authentication Methods

In order to provide a common baseline for the later comparison of authentication methods, we define a small set of reference authentication methods that are already well-established and widely used. These serve as a basis for comparison and to show some benefits and drawbacks of different authentication methods.

- *Password authentication* (knowledge): Password authentication uses a secret alphanumeric string (the password) that is known only to the claimant and the verifier. The password is an authenticator that substantiates the authentication factor of knowledge. This authentication method is one of the most common methods, but suffers from security issues such as phishing, credential stuffing, and shoulder surfing [Has+25].
- *PIN authentication* (knowledge): PIN authentication is similar to password authentication but uses a shorter numeric string (the *Personal Identification Number (PIN)*)

as the authenticator. This authenticator also substantiates the authentication factor of knowledge. It suffers from the same security issues as password authentication, but usually has a smaller keyspace, which makes it easier to brute-force or observe. It is often used when the subject has to authenticate often and/or quickly, as it is faster to enter, providing better usability than passwords.

- *Fingerprint authentication* (biometric): Fingerprint authentication utilizes the unique appearance of a subject's fingerprint as the authenticator that substantiates the authentication factor of biometric. It is easy to use and difficult to forge, but can be vulnerable to spoofing attacks, and once compromised, the biometric factor cannot be changed.
- *SMS authentication* (possession): SMS authentication uses a one-time code sent to the claimant's mobile phone via SMS. The mobile phone is the authenticator that substantiates the authentication factor of possession. Its main weakness is its vulnerability to SIM swapping attacks, but it provides a basic possession factor that is often used in combination with password authentication as part of a multifactor authentication method.
- *Smart card authentication* (possession): Smart card authentication uses a physical smart card as the authenticator that substantiates the authentication factor of possession. The smart card contains a cryptographic key that can be used to authenticate the claimant. It is a very secure method, as it is highly resistant to phishing and other attacks, but requires specialized hardware and can be lost or stolen.

The definitions and terminology established in this chapter provide a foundation for the lightweight *Systematic Literature Review (SLR)* and cluster analysis presented in chapter 4 and the subsequent chapters.

3. Related Work

Contents

While the field of authentication is large and fragmented, this work builds upon a number of existing works on classifying authentication methods and providing a better foundation and understanding of the field. We also rely on much of the methodological groundwork laid out by Kitchenham and Charters [KC07] for our SLR methodology as well as the pioneering efforts done by Tingelhoff, Brugger, and Leimeister [TBL24] and Schulhoff et al. [Sch+24] to integrate LLM assistance into the SLR process to deal with the ever-growing amount of research. A lot of the terminology and basic concepts are based on the work of Temoshok et al. [Tem+24b]. It provides distinct definitions for many of the terms used and clearly distinguishes between concepts which many other works do not.

3.1. Existing Classifications of Authentication Methods

Besides the papers we reviewed as part of the literature review, our classification efforts build upon a variety of existing classifications and their ideas. Chenchev, Aleksieva-Petrova, and Petrov [CAP21] provide a hierarchical classification of authenticator types, based on the three basic authentication factors (knowledge, possession, and biometrics, though they use slightly different terminology). This classification is a good starting point, but is rather coarse as it only distinguishes between the three factors while disregarding any other properties of authenticators or authentication methods. Nonetheless, its clear and often used structure makes it a good basis for our classification.

A large amount of research has also been done in classifying authentication methods for use in specific domains. Alsaeed and Nadeem [AN22] provide a comprehensive overview of how methods of authentication can be classified for use in the medical domain and establish a set of different views on the classification. Notably, they distinguish between credentials, procedures, schemes, and other aspects of the authentication process. We build upon the idea of splitting classification into different views or perspectives to improve usability of the classification while not overloading any single view with too many properties.

Wang et al. [Wan+20] establish Two- & Multi-Factor Authentication as a distinct class of authenticators besides the three basic factors. While this work does not provide more granularity for any of the existing factors, the addition of this class allows classifying authenticators that do not cleanly fit into any of the other classes, as they are based on a combination of multiple factors.

3.2. Systematic Review Approaches

As established in the previous sections, most existing works focus on a specific aspect or use-case of authentication methods, and those which try to provide a more general classification often lack depth or granularity. This may be due to inherent limitations of reviewing a field as large and fragmented as authentication. While the systematic literature review is a well-established method, it takes considerable time and resources to conduct one at scale. To mitigate this, research into using LLMs to assist in the SLR process without compromising its integrity has been conducted.

Tingelhoff, Brugger, and Leimeister [TBL24] provide guidance on incorporating LLMs into the SLR process, noting how they can be used safely to assist in the process. On how to efficiently utilize the capabilities of LLMs, Schulhoff et al. [Sch+24] describe commonly used prompting techniques and how they can be used to get consistent and reliable results from LLMs. All of this is based on the assumption that the researcher is capable of and does validate the quality of the results produced by the LLM [TBL24].

Using LLMs for creating semantic embeddings of papers is also being studied to improve the efficiency of the literature screening process. Work in this area is, for example, contributed by Galli et al. [Gal+24] and Weißer et al. [Wei+20], who explore how to best use LLMs for this task. We use the insights from these papers and apply them to our own process to ensure our approach aligns with current best practices while allowing us to screen a much larger number of papers than what would be feasible through a classical review process within the constraints of this thesis.

4. Methodology

Contents

As we aim to gain a broad overview of a large and complex field of research, an approach similar to a structured literature review seemed appropriate to ensure valuable results. An SLR is a systematic and transparent method for gathering and evaluating existing literature to answer research questions while reducing biases by utilizing a well-documented and repeatable process [KC07]. Due to the size of the field and the limited scope of a bachelor thesis, however, a full SLR was not feasible. Therefore, we opted for a lightweight LLM assisted variant of an SLR that allows for a broad overview while remaining manageable. In this chapter we describe this methodology in detail and explain how we use it to answer our research questions.

We based our lightweight SLR on the guidelines provided by Kitchenham and Charters in *Guidelines for Performing Systematic Literature Reviews in Software Engineering* [KC07]. Therefore, our lightweight SLR shares the same sequential phases as a full SLR: planning, conducting and reporting the review. This chapter describes how we adapted the phases of an SLR to our lightweight LLM assisted approach and how the review was conducted.

With LLMs becoming increasingly capable and the emergence of guidance on effectively integrating them into systematic reviews [TBL24], we decided to utilize their capabilities to enable a review process on a larger scale than would be otherwise feasible within the constraints of a bachelor thesis. LLM assistance was specifically integrated into abstract screening and a subsequent clustering step to manage the large number of papers. In addition to the incorporation of LLMs, the main simplifications compared to a full SLR are:

- A subset of papers is selected as representatives for clusters of papers to gain a broad overview, as opposed to a full analysis of all papers.
- The focus is on the extraction of key characteristics and not on a full quality assessment of the full set of papers.
- The review is conducted by a singular reviewer, rather than a team of researchers.

4.1. Planning the Review

The primary goal of the planning phase is to establish the foundation of the review by formulating a plan for the review and defining research questions [KC07]. Prior to any further planning, the need for a review must be identified. This is typically done through an assessment of the existing literature and the identification of areas that require further exploration or clarification. These insights are then used to formulate research questions that aim to address these gaps in knowledge. In our case, the need for common ground in the authentication field quickly became apparent during initial explorations as discussed in chapter 1 and chapter 3. This led us to formulate the research questions **RQ1** and **RQ2** described in section 1.2.

Secondly, the plan for the review needs to be established to ensure a structured and unbiased approach. The following sections describe the steps of our lightweight SLR in detail and serve as our protocol for the review. The protocol was discussed with our supervisor and is also based on the guidelines provided by Kitchenham and Charters [KC07].

4.2. Conducting the Review

The conducting phase represents the core of the review process. It is where the established plan is executed to identify, select and analyze relevant literature. This phase can further be split into three steps: data aggregation, data extraction and data synthesis [KC07]. The details of each step are described in the following sections.

4.2.1. Data Aggregation

During the data aggregation step, relevant literature is identified and selected for the following steps. The goal of this step is to acquire a relevant, yet manageable set of papers that can be analyzed in detail. First, a data source must be selected. We selected IEEE Xplore as our primary and only data source due to its good coverage of the field of authentication and the sheer number of relevant papers available. The decision to use a single data source was made to simplify the search and retrieval process and to keep the review manageable within the timeframe of a bachelor thesis.

Afterwards, a search query has to be formulated. The aim here is to be as broad as possible, while excluding entirely irrelevant papers. This proved particularly challenging, however, as the term “authentication” is heavily used in different and adjacent contexts, many of which are not relevant to our research. In order not to exclude relevant papers at this stage, we decided on a broader query and aimed to filter out irrelevant papers in the next step utilizing the more advanced language modelling capabilities of LLMs. The full search query we developed is listed in listing 4.1. It is designed to include all papers that discuss novel authentication methods even if a different term is used in the title or abstract, while excluding papers that focus on concepts such as authentication protocols or existing surveys, reviews or evaluations of existing methods. In order to exclude the large number of papers on authentication protocols, which are primarily concerned with protecting the communication between the entities involved in the authentication process, we also excluded papers that focus on terms related to authentication protocols through our query, even if this may bias the query against authentication methods based in cryptography. This was a trade-off we had to make to ensure a manageable dataset and still leaves us with a large variety of papers and authentication methods to analyze.

```
("Document Title":"Authentication" OR "Abstract":"Authenticator")
AND ("Abstract":"Method" OR "Abstract":"Scheme" OR
    ↪ "Abstract":"Procedure" OR "Abstract":"Strategy" OR
    ↪ "Abstract":"Mechanism" OR "Abstract":"Tactic")
AND ("Abstract":"novel" OR "Abstract":"new" OR "Abstract":"propose*"
    ↪ OR "Abstract":"innovat*" OR "Abstract":"investigate" OR
    ↪ "Abstract":"investigates" OR "Abstract":"present*" OR
    ↪ "Abstract":"develop*" OR "Abstract":"design*" OR
    ↪ "Abstract":"introduc*")
AND ("Index Terms":"Authentication")

AND NOT ("Abstract":"Network" OR "Abstract":"Protocol" OR
    ↪ "Abstract":"Crypto*" OR "Abstract":"Authorization" OR
    ↪ "Abstract":"Encrypt*" OR "Abstract":"Performance")
AND NOT ("Index Terms":"Network" OR "Index Terms":"Protocol" OR
    ↪ "Index Terms":"Crypto*" OR "Index Terms":"Authorization" OR
    ↪ "Index Terms":"Encrypt*" OR "Index Terms":"Performance")
AND NOT ("Document Title":"Survey" OR "Document Title":"Framework" OR
    ↪ "Document Title":"Study" OR "Document Title":"Evaluation" OR
    ↪ "Document Title":"Review")
```

Listing 4.1: Search query used to collect papers from IEEE Xplore.

This search query resulted in a total of 1265 papers, with 9 of them excluded because the full-text was not accessible, leaving 1256 papers eligible for further processing. The resulting, purposefully broad set of papers then has to be filtered based on fixed selection criteria that are defined in advance and chosen to select only papers relevant to the research questions.

Papers were included if they:

- **Introduced or described a concrete, novel entity authentication method.** This was included to ensure that the chosen papers fully describe the authentication method and its properties as the paper introducing a new authentication method would likely be the best source of information on the method. Here the idea was that each method had to be novel when it was introduced and therefore for each method that exists a paper would also exist that introduces the method. A paper was determined to describe a novel and concrete authentication method if the authors claimed to introduce a new method or if the method presented was not already widely known.

- **Discussed the method in sufficient detail to allow analysis.** In order to be able to analyze any authentication method, we had to ensure that the paper discusses the method in sufficient detail. This was done to ensure that the paper provides sufficient detail as opposed to simply mentioning the method or discussing some of its properties. Here papers that include enough details on the method to fully understand it and its properties were included, even if not every aspect of the method was described in detail.

Papers were excluded if they:

- **Focused on authentication protocols, authorization or authenticity verification.** While there is a clear overlap between papers covering authentication protocols, authorization, authenticity verification and authentication methods, our focus is solely on authentication methods. Therefore, we chose to fully exclude any papers that primarily focus on any of these topics as they provide little to no information on authentication methods.

- **Did not contribute a novel authentication method, but improved, analyzed or applied existing methods.** Many papers focus on improving, analyzing or applying existing authentication methods. While there is certainly value in these papers, they do not typically provide sufficient detail on the authentication method itself to allow for meaningful analysis.

- **Were not accessible in full-text form.** As we need to analyze the full text of the papers, we excluded any inaccessible papers.

- **Were not written in English.** As our review was conducted in English, we excluded any papers that were not written in English.

This filtering was performed using a combination of manual review and LLM assistance. Tingelhoff, Brugger, and Leimeister have shown that using LLMs to assist in the SLR process can be a very effective tool if the researcher is able to assess the accuracy and reliability of the results the LLMs produce [TBL24]. In accordance with this, we first manually reviewed the relevance for a random sample of 5% of the papers (n=63) according to the inclusion and exclusion criteria defined above to establish a baseline for relevance assessment. The sample was selected randomly from the full set of 1256 papers and relevance was assessed based on the paper title and abstract. We then iteratively refined a prompt for the LLM to assess the relevance of the remaining papers until it achieved an accuracy of over 95% on the sample. The resulting prompt is available as part of the appendix in section A.1 and all iterations of the prompt are documented in the accompanying git repository, which is also linked in the appendix in section A.3.

As a basis for constructing the LLM agent, we used the `MAI-DS-R1` model, which is, among other use-cases, specifically intended for use in reasoning applications and scientific and academic problem-solving tasks [Mic25]. We utilized a zero-shot approach with chain-of-thought prompting as described by Schulhoff et al. [Sch+24]. This kind of prompting relies on a single prompt without examples which includes a detailed description of the task and instructs the LLM to reason about the task step-by-step. We chose this approach both for its simplicity and its effectiveness in achieving high accuracy on the sample. While more complex approaches can yield better results, they also require more effort to develop and introduce additional cost and complexity, which was not feasible for the scope of this thesis. The LLM was provided with definitions, concepts and the task of determining the relevance of the papers and given the paper title and abstract as input. A JSON template was also provided to ensure structured output. The LLM was prompted three times for each paper, and a majority vote was used to determine the final relevance score for each paper. This was done to make the results more stable and reproducible, as LLMs can produce different results for the same input. This process resulted in a total of 457 relevant papers according to the LLM-assisted relevance assessment. Given the large number of papers and the manually tuned prompt to ensure a high accuracy, these papers were not manually reviewed again before further processing. The data for all iterations and papers, which includes the LLM reasoning for including or excluding each paper is also available from the git repository linked in the appendix.

As the remaining set of papers was still too large to analyze in detail and critically contained many papers that were of relevance but covered very similar topics, we decided on a semantic clustering step to group the papers into thematic clusters and select representative papers for each cluster. The general idea here is to first semantically embed the papers in a high-dimensional vector space where papers of similar topics are close together and then run a clustering algorithm on the resulting numeric embeddings to group the papers into clusters. To visualize the clusters and their relationships, we utilized a dimensionality reduction algorithm to project the high-dimensional embeddings into a two-dimensional space while retaining as much of the details as possible. While this is of course a lossy process, it still allows us to get a good visual overview of the clusters and their relative positions in the embedding space. It should be noted that while the distances between embedded papers are meaningful, as they represent semantic similarity, their absolute positions are not, as the embedding space has no well-defined inherent structure and is specific to the embedding model used. We describe how we implemented this clustering step in detail in section 4.5.

As a result of the clustering, we found 25 clusters consisting of 345 papers, with 112 outliers. As the final step of data aggregation, we selected one representative paper for each cluster. The primary criterion for this selection step was simply choosing the paper with the highest citation count in the cluster as long as it matches the inclusion criteria or the next most relevant paper in the cluster. If a cluster did not contain any papers that matched the inclusion criteria, it was excluded from the review. The full selection process is visualized in figure 4.1, which shows how many papers were excluded at each step of the process.

Of those 25 clusters, 24 clusters contained at least one paper that matched the criteria. The full list of clusters – including the excluded one – and their representatives, as well as the reason for choosing the representative, is available in the appendix in section A.2. This final set of 24 papers serves as the basis for remaining analysis and is presented in detail in chapter 5.

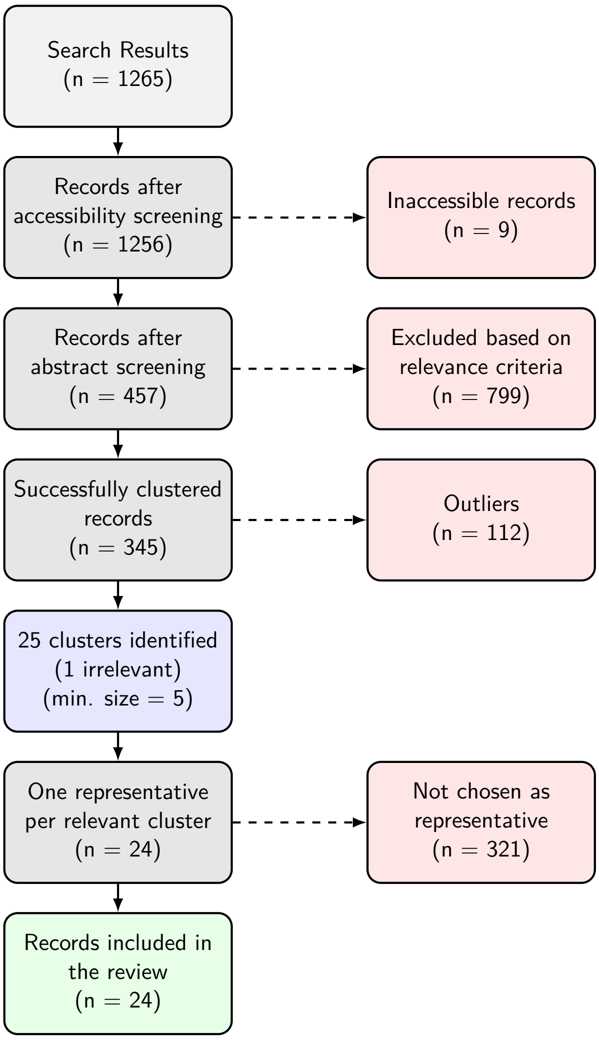


Figure 4.1.: PRISMA flow diagram of the lightweight systematic literature review adapted from [Moh+09].

4.2.2. Data Extraction

Now that we have a manageable set of papers, we can extract relevant data from them. To ensure that this was done in a structured manner, a data extraction form was defined beforehand. We extracted the following data from each paper through full-text analysis:

Field	**Description**
Chosen Cluster Name	A name that representatively describes the cluster of papers this paper belongs to.
Reason for Representativeness	A short description of why this paper is representative for the cluster it belongs to.
Summary	A short summary of the paper that includes the proposed authentication method and its primary features, weaknesses or specifically highlighted properties.
Entity Types	The entities this authentication method applies to (e.g., human-to-machine or machine-to-machine).
Use Cases	The use cases this authentication method is designed for or can be applied to (e.g., IoT, Smart Home, etc.).
Notes	Additional notes on restrictions, quality or limitations of the paper or the authentication method it describes.

Table 4.1.: Data extraction form fields

The form does not include any paper metadata as this is already provided automatically through our fully integrated workflow. The data extracted from the papers is also stored as part of the git repository and forms the basis for data synthesis in the next step as well as the results presented in chapters 5 to 7.

4.2.3. Data Synthesis

The data synthesis step forms the last step prior to reporting the review. It consists of combining the extracted data to discover patterns and insights that ultimately answer the research questions laid out in the planning phase. Kitchenham and Charters note three main types of data synthesis: descriptive, quantitative and qualitative synthesis [KC07]. As the name suggests, quantitative synthesis focuses on comparable data that can be analyzed with statistical methods, while qualitative synthesis focuses on the interpretation of natural language results. Descriptive or narrative synthesis describes the relationship between the extracted data in a structured way, highlighting similarities and differences without performing statistical analysis [KC07]. As our data is primarily qualitative in nature, we chose to perform a descriptive synthesis in order to identify patterns, properties and relationships between the authentication methods described. The results of the data synthesis are presented in chapters 5 to 7.

4.3. Reporting the Review

This thesis represents the reporting phase of the lightweight SLR, documenting both the methodology of the review and its findings. The reporting consists of this methodology chapter as well as chapters 5 to 8 and the data available in the appendix chapter A. The next chapters present the results of the review.

4.4. Catalog of Authentication Methods

To validate the classification of authentication methods we propose as part of this thesis and to provide a basis for further research, we also create a catalog of authentication methods based on the representative papers selected as part of the lightweight SLR. The catalog briefly summarizes the authentication method presented in each paper and classifies it according to the classification approach proposed in chapter 6. The creation of the catalog is based on the results of the data extraction step described in section 4.2.2. To classify the authentication methods, we use the classification approach proposed in chapter 6 and apply it to the data extracted from the representative papers. As most papers do not explicitly state all relevant properties of the proposed authentication method, we derive additional or implied properties through full-text analysis if possible and mark unknown properties as such. The resulting catalog entries follow a standardized format including the following fields:

Field	**Description**
Name	The name of the authentication method described by the paper.
Aliases	Any known aliases or alternative names for the authentication method.
Description	A brief description of the authentication method.
Requirements	A list of specific requirements for the authentication method.
Authenticator Name	The name of the authenticator used in the authentication method.
Authenticator Class	The class of authenticator used in the authentication method as defined in chapter 6.
Facets	The facetted classification of the authentication method as defined in chapter 6.
Sources	A list of sources that describe the authentication method, including the representative paper and any other relevant papers if any.

Table 4.2.: Catalog entry fields

4.5. Tooling and Implementation

We utilized a collection of well-established tools and libraries to implement the paper clustering step of our lightweight SLR described in this chapter. The full implementation of each automated step is available in the git repository linked in the appendix in section A.3. Here we briefly describe the tools and libraries, what they do and why we chose them and how we use them.

With the goal being to extract thematically similar papers as clusters, we chose to use BERTopic [Gro22], a framework designed to "extract coherent topic representations" from collections of documents using semantic embeddings and clustering. The framework is built on top of the Sentence-BERT (SBERT) framework [RG19], uses the HDBSCAN algorithm [CMS13] for clustering and the UMAP algorithm [MHM20] for dimensionality reduction.

Sentence-BERT is a framework that at its core provides a way to convert paragraphs or sentences into high-dimensional numerical vectors, referred to as embeddings, that capture the semantic meaning of the text. By doing so, similar sentences or paragraphs will be close together in the embedding vector space, with more dissimilar ones being further apart. This allows us to numerically represent the semantic meaning of papers, which can then be used for clustering. We chose the `all-mpnet-base-v2` model [NI20] for embedding, which is a pre-trained model that performs well at generating semantic embeddings [Gro22]. Since prior work has shown that embedding and clustering based on the paper titles generally provides better results than embedding and clustering based on abstracts [Wei+20], we used the titles of the papers as input for the embedding.

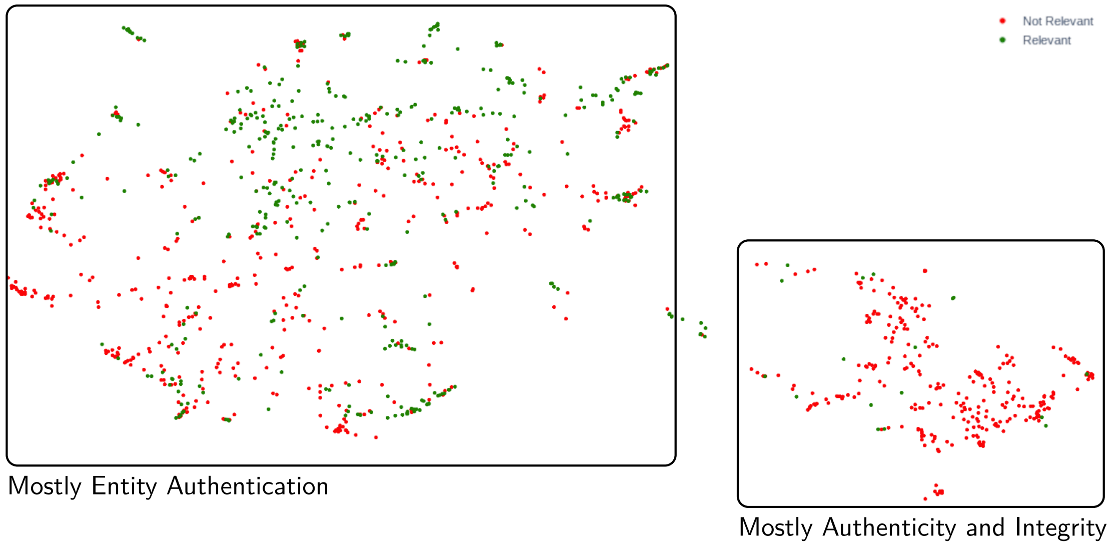
HDBSCAN is a density-based clustering algorithm that is well suited for clustering high-dimensional data such as these embeddings. Notably it does not require the user to specify the number of clusters beforehand, but instead relies on a minimum cluster size parameter to decide how large a cluster must be to be considered valid [CMS13]. This is especially useful here, since we cannot know beforehand how many clusters there will be. The purpose of this minimal cluster size is to filter out noise in the form of outliers and very small clusters. These data points will be considered outliers and not included in the final clusters. By default, BERTopic uses a minimum cluster size of 10 and recommends increasing it for larger datasets [Gro24], but we chose to lower it to 5 to ensure that we miss no relevant smaller clusters. Lowering it further would have resulted in too many small clusters with no clear underlying topic, which would have made analysis difficult.

Since the resulting embeddings are high-dimensional and can not be easily visualized as they are, BERTopic uses the UMAP algorithm [MHM20] to project the embeddings into a two-dimensional space that retains as much of the semantic meaning as possible. This allows us to visualize the clusters and their relationships relative to each other.

5. Overview of Authentication Methods

Contents

In this section we present the results of our lightweight SLR as described in chapter 4 and answer **RQ1**: Which methods of authentication exist?



Mostly Entity Authentication

Mostly Authenticity and Integrity

Figure 5.1.: Visualization of the papers before abstract screening. Each dot represents a paper and the colors represent whether the paper was deemed relevant (green) or excluded (red) during the abstract screening process. The visualization is based on a UMAP [MHM20] projection of the embeddings of the paper titles in vector space.

As discussed in the previous chapter, we screened the papers using an LLM-assisted abstract screening process to identify relevant work. When looking at the papers prior to abstract screening in figure 5.1, we can identify two large clusters: one towards the left side and one towards the bottom-right corner of the figure. By manually inspecting a sample of papers from each cluster, we found that the right cluster contains almost exclusively papers related to *authenticity* and *integrity* of data, while the larger left cluster mostly contains papers related to entity authentication. We can see this reflected in the screening results, where the right cluster is almost entirely excluded from the results. The left cluster contains a lot of relevant papers, but also includes some papers that are related to entity authentication but not relevant to our thesis, such as surveys or performance analyses of existing authentication methods.

After this screening process, the papers were clustered using HDBSCAN [CMS13] on the embeddings of the paper titles in vector space. Since the goal of this thesis is not to provide an exhaustive list of all authentication methods, a representing paper was chosen for each cluster as laid out in chapter 4.

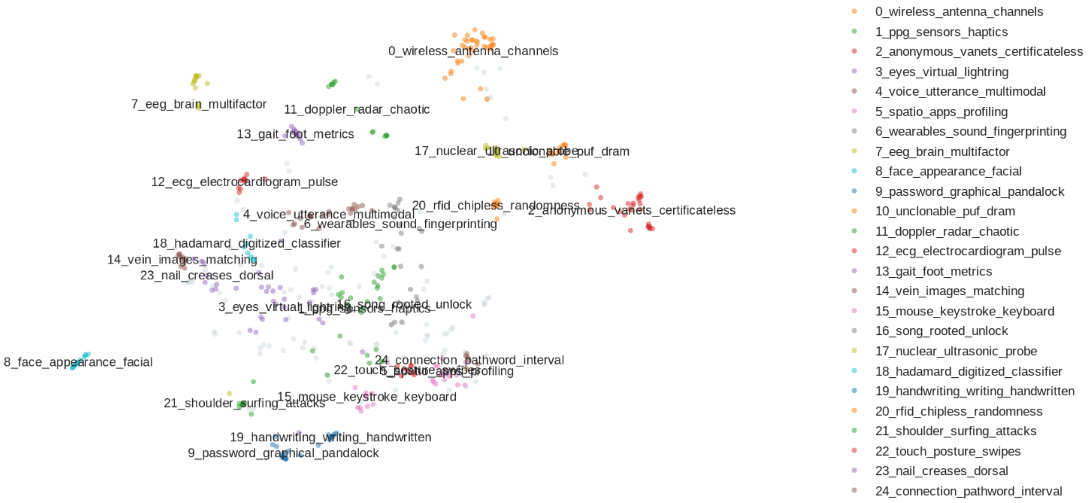


Figure 5.2.: UMAP [MHM20] projection of the embeddings of the paper titles in vector space. The colors represent the clusters of semantically similar papers identified by HDBSCAN [CMS13].

Figure 5.2 shows a visualization of a 2D UMAP [MHM20] projection after the LLM-assisted abstract screening. The clustering itself was performed in the higher dimensional vector space and the UMAP projection is only used for visualization purposes. The colors show the clusters identified by HDBSCAN [CMS13]. Each cluster is also labeled with a unique number and label, which is generated from the most frequent words in the titles of the papers in the cluster. We will refer to these clusters with their unique number as well as a chosen label that is easier to read. The raw embedding and clustering data for all included papers is available as part of our public data repository[1].

In the figure we can clearly see distinct clusters of papers that are related to each other. While the embedding does not necessarily distinguish the topics of the clusters exactly, as it only works on the titles of the papers and comes with inherent limitations, the produced clusters are still useful to gain an overview and to identify areas of interest. In the following each of the 24 clusters is briefly presented with its representative paper. Throughout this section we take note of special characteristics of the methods in the cluster, which will

[1] https://git.rwth-aachen.de/a-classification-approach-for-authentication-methods/public-data-collection/-/blob/main/data/extract-abstract-topics-output/topics_title_all-mpnet-base-v2_min_cluster_size_5_only_relevant_True.json

be discussed in more detail when we derive a classification of authentication methods in chapter 6.

5.1. Clusters and Representative Papers

In the following, we present a short description of each cluster and its representative paper. We have reordered the clusters to group them based on their characteristics in order to improve readability but kept the original numbering for easy cross-referencing. The original numbering was assigned based on cluster size, with larger clusters being assigned lower numbers.

5.1.1. Biometrics-based Authentication

Most clusters we extracted are related to biometric authentication methods. These methods utilize physiological and / or behavioral features of the user to authenticate them. We identified three subcategories of biometric authentication methods: behavioral, physiological and composite, with composite utilizing multiple biometric features which may be either behavioral or physiological. Physiological biometrics can further be divided into static and dynamic features, with static features (such as fingerprints or iris patterns) being stable over time and regardless of context and stimuli, while dynamic features (such as gait or heart rate) potentially changing over time or depending on context or stimulus. This section contains descriptions of all clusters related to biometric authentication sorted by their subcategories.

Behavioral Biometrics

Gait Authentication (Cluster 13) The papers in this cluster deal with gait-based authentication methods, which are based on the unique way a person walks. The representative paper for this cluster is "Performance of Gait Authentication Using an Acceleration Sensor" [Ter+11], which uses the vertical acceleration of the user's foot during the swing phase of the gait cycle as the basis for authentication. It does, however, find that this method alone is not robust enough for practical purposes. Other papers in this cluster also utilize different features of the user's gait, though, which may yield better results. As this authentication method is based on behavioral biometrics, it is only suitable for human-to-machine authentication. Its main use-case is in wearables. However, gait authentication can generally also be used in other scenarios such as smart homes or mobile devices in general. Gait authentication has the benefit of being passive as it occurs without requiring the user to actively participate in the process aside from walking, which is a natural activity for most people. This allows this group of methods to be used for non-intrusive continuous authentication while the user is moving. Replay attacks are possible, but they are difficult to perform, as an attacker would have to precisely mimic the gait of the victim. While the passive nature of this method makes it very easy to use, its accessibility is limited as users with mobility impairments for example may not be able to use it.

HID usage dynamics based Authentication (Cluster 15) Most papers in this cluster utilize how the user interacts with human interface devices (HIDs) such as mice or keyboards to authenticate the user. Some of these proposed methods require the user to actively enter a fixed text, while others passively observe the user's input, which results in free-text input. The passive approach allows for non-intrusive continuous authentication, while the active approach is intended for improving the security of classical point-in-time authentication methods such as passwords by adding a behavioral biometric factor. The representative paper for this cluster is "Key Classification: A New Approach in Free Text Keystroke Authentication System" [SA11]. It proposes an active free-text approach that uses the timing of keystrokes and the resulting rhythm to uniquely identify the user. The main focus of the paper is the additional constraints imposed by the free-text approach. Being based on behavioral biometrics, this method is also only suitable for human-to-machine authentication with its primary use-case being general-purpose logins with a keyboard, for example on a desktop computer or laptop (e.g., when unlocking the computer).

Biometric Authentication for Mobile Devices (Cluster 16) This cluster is less homogeneous than other clusters but generally focuses on smartphone authentication methods. Most papers in this cluster rely on biometrics for this. The representative paper, "Your Song Your Way: Rhythm-based Two-Factor Authentication for Multi-Touch Mobile Devices" [Che+15], proposes a two-factor authentication method based on knowledge of a rhythm and the biometric characteristics of inputting said rhythm on a multitouch device. The paper reports better lower-bound security and better security features than traditional login methods such as PINs or lock-screen patterns, which rely only on knowledge. The rhythm can be entered using either taps or swipes, whichever the user prefers. As with other methods in this category, it is only suitable for human-to-machine authentication, with the primary use-case being mobile devices with a touchscreen such as phones or tablets. The paper specifically notes accessibility as a goal of this authentication method, which is often neglected in other works. The method requires some musical understanding of notes, however.

Touch Behavior Authentication (Cluster 22) All papers in this cluster use touch interactions for authentication. The focus lies on passive (sometimes referred to as "implicit") and continuous authentication. The representative paper, "Touch-Interaction Behavior for Continuous User Authentication on Smartphones" [She+15], proposes utilizing touch interaction behavior, specifically features of swiping gestures, to continuously authenticate the user. The method is designed to be used as auxiliary continuous authentication as it currently does not meet the security requirements to be used as a primary biometric factor – its error rates are too high. The paper discusses the performance of the method and compares it to other biometric authenticators. The general idea is similar to the previous cluster, but with a distinct focus on continuous authentication to continuously ensure the security of an authenticated session.

Passive Mobile Device Authentication (Cluster 1) Especially for mobile devices, passive authentication methods are an area of interest. Given the possibility of easy data collection through the built-in sensors and the fact that users are naturally interacting with their mobile devices, these methods can be used to easily and unobtrusively authenticate the user either continuously or at points in time. The representative paper, "Please Hold on: Unobtrusive User Authentication Using Smartphone's Built-in Sensors" [BCZ17], seeks to augment existing authentication methods such as PINs with subsequent passive authentication based on hand micro-movements. It works by sampling the 3D sensors built into the smartphone for a short period of time after the phone is unlocked through conventional methods and compares the collected data to previous samples. While the method as discussed in this paper is not continuous, its passive nature makes it easy to see how it could be extended to run continuously in the background. The enrollment flow is not discussed as part of the paper, but we assume that the algorithm would either learn over time or be trained once when activating. The impact of contextual factors such as full-body movement or multiple intended users is discussed but not resolved. Notably, there is a short period during the data collection where the device is unlocked but not authenticated with this method, which is a potential security risk.

Handwriting-based Authentication (Cluster 19) The papers in this cluster generally revolve around handwriting-based authentication methods. Authentication methods based on handwriting generally ask the user to write a specific phrase and analyze the unique way the user performs the handwriting. The medium on which the user is asked to write can vary, with the representative paper, "Challenge-Response Authentication Using In-Air Handwriting Style Verification" [Xu+20], asking the user to write in the air and capturing the movements using a 3D motion sensor.

The paper proposes a challenge-response based authentication method, where the text to be written is chosen at random and the user is verified independent of the written content but purely on behavioral characteristics of the handwriting style. It discusses the performance of the method and compares it to other biometric factors. The primary use-case here is in-person authentication, for example in access control systems, as specialized hardware is required. The paper tests this method using a Leap Motion controller, which is a 3D motion sensor, but it may be possible to adapt it to regular cameras. This is not discussed in the paper, however. The authors claim that this authentication method may be more practicable than fingerprint authentication in some scenarios. A detailed attack model is provided and security is even upheld in an untrusted remote scenario due to the challenge-response approach chosen. It is noted that this method is resilient against forgery and replay attacks.

Static Physiological Biometrics

Full-Face Biometric Authentication (Cluster 8) The papers in this cluster introduce authentication methods that utilize the full face of the user. The representative paper is "Face Authentication Using the Trace Transform" [Sri+03], which presents a novel way of extracting features from faces for use in biometric authentication. Specifically, the focus is on extracting features from an image of a user's face, as generally recognizing human faces is a very hard task when looking at it as a classification problem. This is due to the fact that human faces all belong to the same class, and the differentiation must therefore occur based on comparatively small differences. By improving feature extraction, the paper aims to improve the performance of the already well-established face recognition methods. Physiological biometrics are typically unique and do not change over time, which makes them suitable for authentication. This does, however, also mean that they cannot be changed or revoked if they are ever compromised.

Biometric User Authentication (Cluster 18) This cluster contains a variety of papers that discuss different biometric authentication methods. Its representative paper is "User-Specific Iris Authentication Based on Feature Selection" [Qi+08], which proposes utilizing the iris as a unique biometric feature for user authentication. The proposed method uses a genetic algorithm to select different features for each user to maximize reliability. The iris is a unique and stable physiological biometric feature.

Vein Authentication (Cluster 14) Another physiological biometric feature that can be used for authentication is the vein pattern in the hand of the user. Like most papers in this cluster, the representative paper "Personal Authentication Using Hand Vein Triangulation and Knuckle Shape" [KP09] utilizes the pattern of veins in the hand of the user. It combines this feature with knuckle shape to achieve higher accuracy. It discusses the performance of the method and compares it to other biometric factors. Imaging is done using a near-infrared camera. As this method combines multiple biometric features, it can be considered a composite or multi-modal biometric authentication method. With hand veins being a physiological biometric, this method is only suitable for human-to-machine authentication and, due to specialized hardware requirements, is best suited for in-person authentication in access control systems or similar scenarios. A large advantage in this scenario is the ability to perform the authentication without physical contact, which may be desirable due to hygiene or other reasons. While hand veins are considered mostly stable in the age group of 20-50, the paper mentions limitations in regard to stability outside this age group and due to other physical conditions. Generally, this method appears similar to fingerprint authentication in many ways but has the advantage of being contactless.

Hand Physiology Authentication (Cluster 23) This cluster of papers also focuses on biometric authentication methods that utilize the physiology of the hand of the user. Papers in this cluster utilize the full hand shape, finger and palmar creases, vein patterns, or other features of the hand. The representative paper for this cluster is "Biometric Authentication from Low Resolution Hand Images Using Radon Transform" [Mos+09] as the most cited paper in the cluster. The features are extracted from a low-resolution image of the hand, which can be acquired using a simple document scanner. A "peg free and position invariant" method is proposed to make the method more practical. The method is designed to be used in a point-in-time authentication scenario. It uses the Radon transform to extract one-dimensional position-invariant features. Other methods utilize measurements of lengths and widths and, therefore, need pegs to fix the hand in a specific position. As with other methods that require specialized hardware, in-person authentication is the primary use case. The method still requires more testing, and finger motion remains an issue, but initial results are promising.

Dynamic Physiological Biometrics

EEG-based Authentication (Cluster 7) Another avenue for biometric authentication is the use of dynamic physiological features, such as brain activity. The papers in this cluster utilize features derived from Electroencephalography (EEG) measurements to authenticate the user. Using brain waves as an authenticator has several advantages as it is hard to replicate or even observe and can also be revoked by altering stimuli, for example by showing a different image during authentication. It also comes with significant drawbacks, however, the major one being usability.

The representative paper for this cluster is “ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System” [Klo+13]. It introduces an authentication method based on EEG signals that is primarily designed to be used in mobile devices. To accomplish this, it relies on a separate server (the verifier) to collect and analyze the EEG signals and provide the authentication result to the frontend (the RP). This is primarily done to avoid expensive processing on low-energy devices but also opens up the avenue for cross-device authentication.

Any use of this method does require specialized hardware, however, which is not generally available. It also currently requires the user to sit still and concentrate. A potential use case may be Virtual Reality (VR) or Augmented Reality (AR) applications, where the user is already required to wear a headset.

The paper also utilizes NFC Authentication to provide a second factor and claims this method is “especially suited for scenarios where there is a sudden or unexpected need to prove or authenticate an identity”, but that seems far-fetched even though the aforementioned central verifier would aid in this.

ECG-based Authentication (Cluster 12) Yet another dynamic physiological biometric is the distinct pattern of a person’s heartbeat, which can be measured using an Electrocardiogram (ECG). This cluster of papers relies on features derived from ECG traces to authenticate the user, with the representative paper being “Electrocardiogram (ECG) Biometric Authentication Using Pulse Active Ratio (PAR)” [SSP11]. The paper uses the Pulse Active Ratio (PAR) derived from ECG traces as a biometric authenticator. It discusses the performance of the factor and compares it to other ECG-derived features and other biometric authenticators. The method is proposed as a point-in-time authentication method. Use in conjunction with other factors or as continuous authentication is not discussed, but seems feasible. It does discuss solutions for temporal variability of the ECG signal for the same individual, as this is typically a problem with dynamic physiological biometrics. The heartbeat may, for example, vary due to stress or physical activity.

Radar-based Human Authentication (Cluster 11) Heartbeat and respiratory signals can also be measured using radar, which is what this cluster focuses on. The representative paper, "HeartPrint: Exploring a Heartbeat-Based Multiuser Authentication With Single mmWave Radar" [Wan+22], also utilizes a person's heartbeat to authenticate them, but extracts the data based on the skin surface vibrations caused by the heartbeat using a mmWave radar as opposed to an ECG. This identification can be used to authenticate the user even in a multi-user scenario. The method is designed to be non-contact, passive, and continuous but requires special hardware and the user must be stationary. Here, many use cases are possible with a focus on smart environments where multiple people may be present. There are some significant usability limitations but also some interesting properties.

Passive User Authentication via Wearables (Cluster 6) While the previous clusters revolved around specific biometric features, this cluster focuses on passive user authentication for wearables in general. While the representing paper, "PPGPass: Nonintrusive and Secure Mobile Two-Factor Authentication via Wearables" [Cao+20] specifically uses photoplethysmogram (PPG) signals, other papers in this cluster use other biometric features for passive mobile authentication. The paper itself does not only introduce using PPG signals as a biometric feature but also focuses on revocability and security of the factor and proposes a method of making the non-revocable PPG signal revocable through a non-invertible transformation. The factor is primarily intended as a secondary factor alongside a primary factor such as a password and is designed to be used in a point-in-time authentication. This is likely due to current limitations of the authentication method. Given this generally works with wearable devices, it has a large variety of use cases. The use of a non-invertible transformation to add a changeable layer to an otherwise non-changeable biometric feature is also interesting for other biometric features as it partially addresses the issue of revocability. If the source biometric feature is compromised however, the transformation does not provide any additional security. For dynamic, hard to replicate features this is less of a concern, however. Continuous authentication using this factor is not discussed but appears realistic as movement of the user is explicitly considered.

Context-Aware Passive User Authentication (Cluster 5) Many of the previously discussed biometric authentication methods struggle when dealing with changing conditions such as different body postures or other contextual factors. The papers in this cluster try to address this issue by incorporating context information into the authentication process. Here context is not used a secondary factor but rather to improve an existing biometric authenticator by adjusting its parameters based on the context. The representing paper, "Context-Aware Implicit Authentication of Smartphone Users Based on Multi-Sensor Behavior" [WT19], introduces a method it describes as "implicit authentication with password" which combines pin authentication with point-in-time implicit authentication based on touch dynamics and gestures. The method is designed to utilize context information (body posture) to dynamically choose the implicit authentication model to use. The authenticators used here have already been discussed in previous clusters, but this paper specifically focuses on choosing a different authentication model based on the context. This allows the method to be more robust under changing conditions.

Composite Biometrics

Composite Biometric Authentication (Cluster 3) This cluster contains papers that discuss biometric authentication methods which combine multiple biometric features. It also contains papers that only discuss a singular biometric feature. Utilizing multiple biometric features can improve accuracy and robustness and is typically referred to as composite or multi-modal biometric authentication [KH08]. Note that while this does result in a multi-modal biometric authenticator, it does not result in a multifactor authenticator, as only a biometric factor is provided. The representative paper for this cluster is "A Multi-Sample Multi-Source Model for Biometric Authentication" [PBK02] as it is the most cited paper in the cluster. It specifically discusses how multiple biometric features from different sources and samples can be combined to improve biometric authentication and does not itself introduce the use of a new feature for authentication.

Acoustics-based Biometric Authentication (Cluster 4) Most papers in this cluster focus on authenticating the user by utilizing acoustic features of the user. The representative paper is "Multimodal Biometric Authentication Using Teeth Image and Voice in Mobile Environment" [KH08], which introduces a multimodal authentication method that combines voice and teeth image features to authenticate the user. The features are captured simultaneously, combining the two features into a single authentication factor. It shows a clear improvement over single feature authentication. The paper does not discuss attacks such as replaying the voice and showing an image.

5.1.2. Knowledge-based Authentication

When thinking about authentication, most people would likely think of knowledge-based authentication methods, such as passwords first. Simple knowledge-based authenticators such as passwords or PINs are well established and widely used. However, as they come with serious limitations and drawbacks, there is research into improving them with other or derived knowledge-based methods.

Alternative password-style Authentication (Cluster 9) Papers in this cluster generally focus on improving passwords while keeping the general idea. This is usually done by changing the input method or the way the password is presented. "Neuromuscular Password-Based User Authentication" [Jia+21], the representing paper for this cluster introduces a "neuromuscular password" that combines a unique way to enter a password with the biometric features recorded during the entry. The password is entered by contracting the muscles in the fingers, which is recorded using high-density surface electromyography (HD-sEMG). As this method also uses biometrics to authenticate the user, it is considered a multifactor authentication method. In its shown implementation it can only be used for stationary devices as a point-in-time authentication method. Given that the entered password can be changed and is not visible to an observer it is both revocable and resistant to shoulder-surfing attacks.

Graphical Authentication (Cluster 24) This cluster does not have a singular topic, but the most cited paper focuses on graphical authentication methods and gives a broad overview of existing methods. “Graphical User Authentication: A Time Interval Based Approach” [URA12] proposes a graphical user authentication method that utilizes a cued recall-based approach and incorporates the time intervals between clicks or taps to authenticate users. The method is designed to be used in a point-in-time authentication scenario. By combining the graphical authentication with the timing of the clicks, it makes replay attacks harder to accomplish. The paper generally discusses that graphical authentication methods and recall-based methods are generally easier to use which leads users to choose stronger (graphic) passwords, ultimately increasing security.

Shoulder-surfing resistant Authentication (Cluster 21) Papers in this cluster focus on authentication methods that are resistant against observation attacks such as shoulder-surfing, which are a common problem with using knowledge-based authentication in public spaces. The representing paper, “DyGazePass: A Gaze Gesture-Based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attacks” [Raj+18], introduces “Dynamic Gaze Passwords” in an effort to address shortcomings of previous gaze-based authentication methods, specifically video analysis attacks and low accuracy. Previous methods already offer an improvement over PINs, passwords and patterns in regard to shoulder-surfing attacks. They show that their method is not susceptible to single video analysis attacks and even holds strong against dual video iterative attacks. The method is designed to be used in a point-in-time authentication scenario. The method is based on gaze-based color password entry by following moving circles. As such it is generally suitable for human-to-machine authentication for any application that has a screen and is capable of tracking the user’s gaze. It does have significant usability limitations however, as it takes at least eight seconds to authenticate and requires specialized eye tracking hardware. In terms of accessibility it is not suitable for users with visual impairments such as color blindness or low vision.

5.1.3. Possession-based Authentication

Possession-based authentication methods utilize something the user possesses as an authenticator. This can either be in the form of a physical or a digital token. Typical examples of digital tokens include certificates or cryptographic keys which are typically stored as files on a digital device. Physical tokens can be smart cards, tags or even physical keys.

Hardware-Possession

RFID-based Authentication (Cluster 20) This cluster contains papers that discuss authentication methods based on Radio-Frequency Identification (RFID) technology. These methods generally work by having a user or device carry an RFID tag that is then read by an RFID reader to authenticate the user or device. The representative paper for this cluster is “Ultralightweight RFID Reader-Tag Mutual Authentication” [HJ15], which describes a mutual authentication protocol for low-powered RFID tags and readers that improves upon aspects of existing protocols. While the main focus of this paper is the authentication protocol, it utilizes the RFID tag as a possession-based authenticator as part of the authentication method implemented by the protocol. As RFID tags can not only be carried by humans but also devices such as robots, this method can be used for both in-person human-to-machine and machine-to-machine authentication as part of access control systems or similar scenarios. Since the proposed authentication method ensures mutual authentication, it also provides a way to authenticate the RFID reader to the tag, which can be used to prevent replay attacks by not allowing the tag to be read by unauthorized readers.

Physical Layer Authentication (Cluster 0) The papers in this cluster focus on authenticating devices using their intrinsic physical properties. This allows for continuous authentication on devices after an initial authentication using a higher level protocol as it allows easy detection of any changes in characteristics that may occur due to tampering or replay attacks. As this validation occurs at the physical layer, it is very hard to spoof or replay, as replay attacks are typically focused on higher level protocols. The representative paper, "Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets" [Hou+14] introduces a continuous physical layer authentication method relying on the unique carrier frequency offset (CFO) induced by the hardware to continuously authenticate a device after an initial authentication using a higher level protocol. The paper discusses initialization and imitation attacks in detail. As this method only utilizes existing physical properties of IoT devices, it is very suitable for machine-to-machine authentication in IoT networks or other mobile applications.

Physically Unclonable Hardware Authentication (Cluster 10) Physically Unclonable Functions (PUFs) are a type of hardware authenticator that is very hard to clone or replicate. The papers in this cluster use PUFs to authenticate devices to take advantage of their uniqueness and clone-resistance. The representative paper, "DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication" [Teh+17], proposes using DRAM chips as PUFs as they are readily available, and their initialization behavior resembles a PUF. This allows them to be used as a collection of Challenge-Response Pairs (CRPs) to authenticate the device similar to other challenge-response based authentication methods. The paper also discusses using them as System-ID and talks about possible attacks and large scale manufacturing. Obvious use-cases include machine-to-machine authentication in IoT networks or applications where device integrity must be verified continuously.

Software-Possession

Vehicular Authentication (Cluster 2) This cluster discusses authentication methods for vehicular networks, which is an evolving field of research due to the increase in connected vehicles and the unique requirements they pose. A unique challenge in this field is the need for privacy-preserving authentication methods, which may seem contradictory at first glance. When looking at a more abstract view of authentication however it becomes clear that in some scenarios it is sufficient to prove being part of a group-identity as opposed to proving control over a specific identity, which can for a sufficiently large group protect privacy. The representative paper for this cluster is "An Anonymous Authentication Scheme for Plug-in Electric Vehicles Joining to Charging/Discharging Station in Vehicle-to-Grid (V2G) Networks" [CZS15], which introduces a group signature based authentication method for vehicles with a focus on privacy-preservation. The method allows authentication to the charging network without revealing the vehicle identity while still proving membership in the authorized group of vehicles and allowing revocation of individual memberships. It utilizes a certificate with group signatures as the authentication factor and is specifically designed with vehicle-to-grid (V2G) networks in mind, so that vehicles can authenticate themselves to charging stations without revealing their identity, as identity information may otherwise be used to track the vehicle and its owner. In this specific implementation however, the entity is only anonymous to the charging station and the vehicle identity can still be revealed by a central authority if deemed necessary.

5.1.4. Excluded Clusters

Hardware Authenticity Verification (Cluster 17) All papers in this cluster focused solely on validating the authenticity of hardware components rather than authenticating entities. Therefore, no representative paper was chosen, and the cluster was excluded from further analysis.

Given the wide variety of authentication methods we reviewed, several key aspects can be identified, from which we can derive a novel classification approach, which we will discuss in the following chapter.

6. Classification of Authentication Methods

Contents

Now that we have an overview over existing authentication methods and how they are related to each other, we can start to look for common or unique characteristics of the methods. Some of them already become clear when looking at the clusters and their representative papers while others are less obvious and require looking at the bigger picture. In the following we will discuss characteristics extracted from the clusters and their representative papers as well as some additional characteristics that were not explicitly covered in the clusters but are still relevant to derive classes of authentication methods. Of course this framework is also intended to cover authentication methods not covered by the clusters, such as the classical authentication methods, like passwords and PINs, introduced in chapter 2.

6.1. Insights from the Clusters

Authenticator Type	Representative papers (Total cluster sizes)
Biometrics-based	15 (201)
Possession-based	4 (84)
Hybrid	3 (38)
Knowledge-based	2 (13)

Table 6.1.: Number of representative papers per authenticator type (numbers in parentheses indicate total combined size of the represented clusters).

Our analysis of the 24 clusters reveals several insights about research on authentication methods:

- **Focus on Biometric Authentication:** The majority of clusters (15/24) and by extension papers we found are related to biometric authentication methods as shown in table 6.1. This may be due to the unique properties of biometrics, such as their ease of use, ubiquity in mobile devices and resistance to different kinds of attacks or due to biases in our search strategy which we will discuss further in chapter 8. Knowledge-based authentication methods, while common in practice, only make up a small fraction of the clusters (2/24). They are, however, frequently mentioned as part of hybrid authentication methods.

- **Continuous Authentication:** With the rise of mobile devices and biometric authentication, there is also a clear interest in continuous authentication methods which can unobtrusively ensure that the user is still the same as when they first authenticated.
- **Context-Awareness:** As especially biometric authentication methods are often sensitive to contextual changes, such as changes in the environment or the posture of the user, there is also interest in improving the context-awareness of authentication methods in order to improve their robustness and usability.
- **Privacy Preservation in New Fields:** With new use cases for authentication methods such as vehicular networks, there also come new requirements such as privacy preservation. This makes it clear that while the basic concepts behind authenticators may stay the same, the requirements for authentication methods should not be seen as static but rather as evolving with the advent of new technologies and use cases.
- **Multi-Factor and Multi-Modal Authentication:** There is a growing recognition of the need for multifactor or at least multimodal authentication methods to improve security. Any single authentication factor is simply a single point of failure and therefore not sufficient for many use cases.

With the insights gained from the clusters and their representatives, we can now proceed to answer **RQ2**: Which characteristics of authentication methods can be used to group them into meaningful classes for systematic comparison?

6.2. Hierarchical Classification of Authenticators

Figure 6.1 presents our classification of authenticators based on existing work by Chenchev, Aleksieva-Petrova, and Petrov and the clusters identified by us.

It shows a hierarchical classification of the most important aspect of any authentication method, which is the authenticator used. Given that the authenticator determines what the user has to possess and control to authenticate, we look at it from the perspective of what that "thing" the user has to possess and control is. Here we can distinguish between five main classes of authenticators: Biometrics-based, Knowledge-based and Possession-based authenticators were already established as part of chapter 2 and are well established as the basis for classifying authenticators.

Definition 6.2.1 (Biometrics-based Authenticator)**.** A biometrics-based authenticator is an authenticator that is based on biometric features of the subject, such as features of their fingerprint or gait.

Definition 6.2.2 (Knowledge-based Authenticator)**.** A knowledge-based authenticator is an authenticator that is based on knowledge the subject possesses, such as a password or PIN.

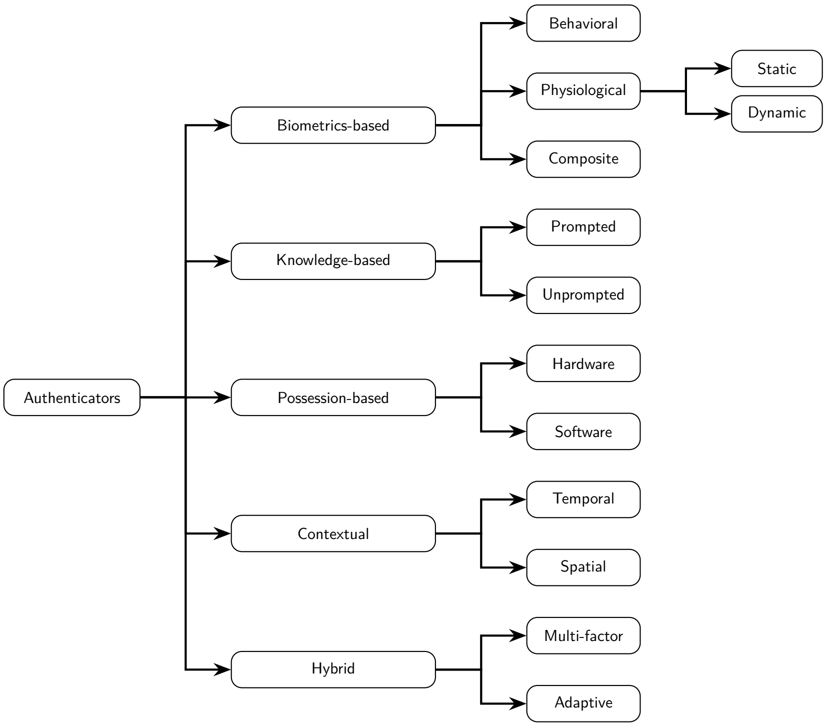


Figure 6.1.: Hierarchical classification of authenticators adapted from [CAP21].

Definition 6.2.3 (Possession-based Authenticator)**.** A possession-based authenticator is an authenticator that is based on a something the subject possesses, such as a smart card or a certificate.

We also introduce two new classes of authenticators to classify authenticators that do not fit into the existing classes:

Definition 6.2.4 (Contextual Authenticator)**.** A contextual authenticator is an authenticator that is based on context information, such as the time or location of the subject, to prove an entity's identity.

Definition 6.2.5 (Hybrid Authenticator)**.** A hybrid authenticator is an authenticator that combines multiple authentication factors into a singular authenticator.

These five classes form the basis for our hierarchical classification of authenticators. Expanding upon these main classes, we found that additional subclasses help group the authenticators into more meaningful classes for systematic comparison. Starting with authenticators based on biometrics, we can distinguish between behavioral, physiological and composite authenticators.

Definition 6.2.6 (Behavioral Biometrics-based Authenticator)**.** A behavioral biometrics-based authenticator is a biometrics-based authenticator that is based on behavioral features of the subject, such as features of their typing or gait.

Definition 6.2.7 (Physiological Biometrics-based Authenticator)**.** A physiological biometrics-based authenticator is a biometrics-based authenticator that is based on physiological features of the subject, such as features of their fingerprint or iris.

Definition 6.2.8 (Composite Biometrics-based Authenticator)**.** A composite biometrics-based authenticator is a biometrics-based authenticator that combines multiple biometric features into a single authenticator. These features can be an arbitrary combination of behavioral and physiological features.

Physiological biometric features and the authenticators that utilize them can further be split into static and dynamic subclasses. While it is assumed that physiological biometric features suitable for authentication are unique and fixed over time, dynamic physiological biometric features, such as heartbeat or brain activity, change depending on context while remaining consistent in the same context. Static physiological biometric features such as a fingerprint or an iris on the other hand are always fixed regardless of context.

Definition 6.2.9 (Static Physiological Biometrics-based Authenticator)**.** A static physiological biometrics-based authenticator is a physiological biometrics-based authenticator that is based on static physiological features of the subject, such as features of their fingerprint or iris.

Definition 6.2.10 (Dynamic Physiological Biometrics-based Authenticator)**.** A dynamic physiological biometrics-based authenticator is a physiological biometrics-based authenticator that is based on dynamic physiological features of the subject, such as features of their heartbeat or brain activity.

Knowledge-based authenticators can be split into prompted and unprompted subclasses. These are also referred to as cued and uncued respectively [URA12].

Definition 6.2.11 (Prompted Knowledge-based Authenticator)**.** A prompted knowledge-based authenticator is a knowledge-based authenticator that provides the user with additional information, so they may recognize their credentials, such as an image or a security question.

Definition 6.2.12 (Unprompted Knowledge-based Authenticator)**.** An unprompted knowledge-based authenticator is a knowledge-based authenticator that does not provide the user with any additional information and only relies on recall.

An example of a prompted authenticator is an image where the user has to click a specific point, while a password is a typical unprompted authenticator.

Possession-based authenticators can be split into hardware and software subclasses. As already discussed in the previous section, in both cases the subject must possess the authenticator to authenticate but the form of the authenticator is different.

Definition 6.2.13 (Hardware Possession-based Authenticator)**.** A hardware possession-based authenticator is a possession-based authenticator that is a physical device, such as a smart card or a unique hardware component.

Definition 6.2.14 (Software Possession-based Authenticator)**.** A software possession-based authenticator is a possession-based authenticator that is a digital file or piece of data stored on a device, such as a certificate or a cryptographic key.

In terms of contextual authenticators, we can distinguish between temporal and spatial contextual authenticators.

Definition 6.2.15 (Temporal Contextual Authenticator)**.** A temporal contextual authenticator is a contextual authenticator that is based on time, such as the time of day or the date.

Definition 6.2.16 (Spatial Contextual Authenticator)**.** A spatial contextual authenticator is a contextual authenticator that is based on location, such as the GPS coordinates of the subject or the physical network they are connected to.

Contextual authenticators are often used in conjunction with other authenticators as they provide little security on their own. An otherwise unprotected device in a restricted area can, however, for example be considered to be protected by a spatial contextual authenticator, as the device is only accessible in that area.

Finally, hybrid authenticators can be split into multifactor and adaptive authenticators.

Definition 6.2.17 (Multifactor Hybrid Authenticator)**.** A multifactor hybrid authenticator is a hybrid authenticator that simply combines multiple different authentication factors into a single authenticator.

Definition 6.2.18 (Adaptive Hybrid Authenticator)**.** An adaptive hybrid authenticator is a hybrid authenticator that may choose factors based on context or user-preference.

6.3. Facetted Classification of Authentication Methods

When comparing the hierarchical classification with the clusters presented in chapter 5, we can see, however, that this does not adequately represent all characteristics of authentication methods. It becomes clear there are two orthogonal ways to classify authentication methods: We already classified authentication methods based on the kind of authenticator they use. Some clusters, however, focused on the method of authentication and its properties rather than the authenticator itself, i.e., how the user provides the authenticator. Therefore, we also introduce a secondary facetted classification of authentication methods, that shows overarching characteristics of authentication methods which are not hierarchical. While authenticators define what the user has to provide to authenticate, authentication methods define how the user can provide this information. As this is not hierarchical but rather composed of multiple independent facets, we cannot simply extend the hierarchical classification. Instead, we present a facetted classification of authentication methods based on the clusters identified in chapter 5 as shown in figure 6.2.

It shows 12 additional facets of authentication methods which are relevant across different classes of authenticators. The facets are defined as follows:

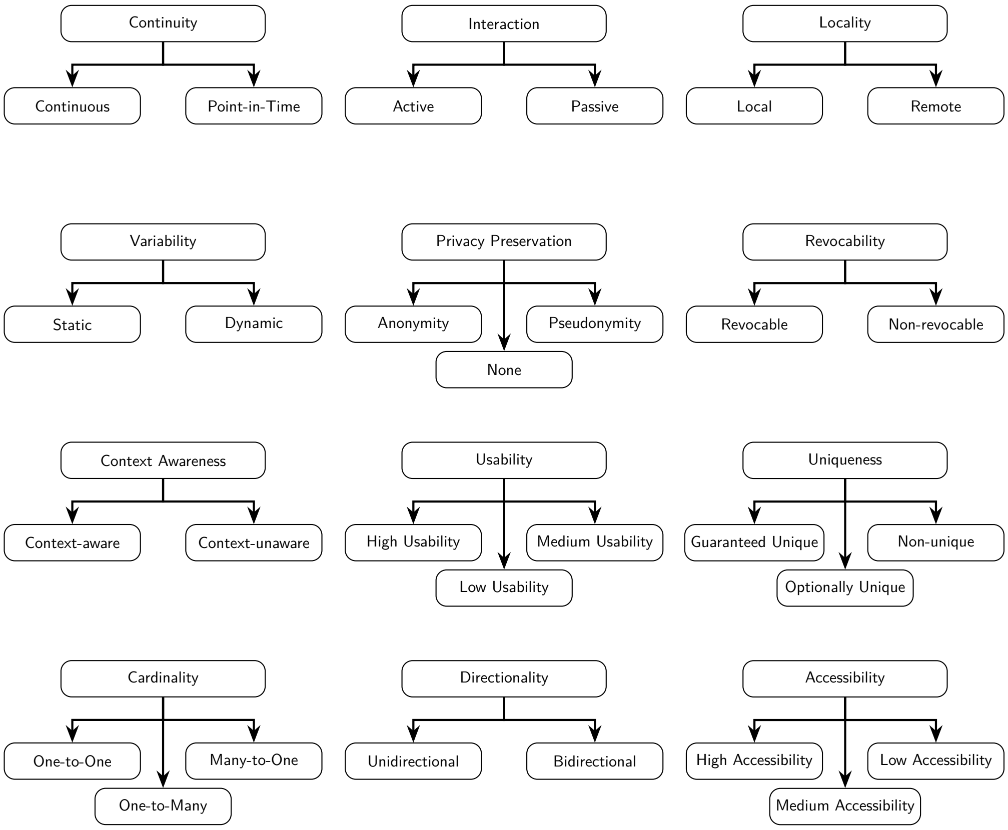


Figure 6.2.: Facetted classification of authentication methods.

Definition 6.3.1 (Interaction)**.** Interaction specifies if the authenticating entity has to actively participate in the authentication process or if it can be done passively. An authentication method is considered **active** if the authenticating entity has to actively perform an action solely to authenticate. Otherwise, it is considered **passive**. Note that we still consider an authentication method to be **passive** if it only requires an action that the authenticating entity would perform anyway, such as breathing or using their keyboard.

Passive authentication methods are usually implemented with biometric authenticators, as some biometric features can easily be measured without having the user actively perform a specific action that they would not otherwise perform.

Definition 6.3.2 (Continuity)**.** Continuity describes whether authentication occurs only once or continuously. An authentication method is considered **continuous** if the subject is continuously authenticated, for example by continuously measuring their heartbeat or prompting them to perform a specific action in regular intervals. In contrast, an authentication method is considered **point-in-time** if authentication occurs only once, usually at the beginning of a session and is assumed to be valid for the duration of the session without further checks.

Continuous authentication methods work best with passive authentication methods but can also be used with active authentication methods by continuously prompting the subject to authenticate. By continuously revalidating the subject's identity, continuous authentication provides higher security especially for long-lived sessions.

Definition 6.3.3 (Locality)**.** Locality signifies if authentication is performed locally or remotely. An authentication method is considered **local** if the subject has to be physically present at the location where the authentication is performed, such as when using a fingerprint scanner or a smart card reader. An authentication method is considered **remote** if the subject can authenticate from a different location, usually over a network connection, such as when using a password.

Some authentication methods which are not natively suitable for remote authentication due to the nature of the authenticator or due to assumptions made by the authentication method can be adapted to work remotely, but this usually involves placing additional burden on the authentication protocol to create a secure channel or similar.

Definition 6.3.4 (Variability)**.** Variability indicates if the authentication method is static or dynamic. An authentication method is considered **static** if the output of the authenticator does not change over time and considered **dynamic** if the authenticator output changes over time. An example for dynamic authentication methods are challenge-response based authentication methods, where the challenge changes for each authentication attempt.

This property is particularly relevant if replay resistance or resistance against observation attacks in general is important.

Definition 6.3.5 (Privacy Preservation)**.** Privacy Preservation describes if the authentication method preserves the privacy of the authenticating entity. Here we distinguish between full

anonymity, **pseudonymity** and **none**. An authentication method is considered **anonymous** if the authenticating entity can authenticate without revealing their identity to the verifier. If the authenticating entity can authenticate without revealing their identity but still has to reveal a persistent identifier (a pseudonym) to the verifier, the authentication method is considered **pseudonymous**. If the authenticating entity has to reveal their identity to the verifier, the authentication method is considered to have **no privacy preservation**.

Definition 6.3.6 (Revocability)**.** Revocability indicates if the credentials used in an authentication method can be revoked. **Revocable** authentication methods enable the user to revoke or change their credentials. This can be separate from the authenticator itself, i.e., a heartbeat characteristic may not be revocable, but by utilizing a non-invertible transformation, the authentication method can be made revocable. A **non-revocable** authentication method does not allow the user to change their credentials. This is usually due to the nature of the authenticator [Cao+20].

Definition 6.3.7 (Context Awareness)**.** Context Awareness indicates if the authentication method is context-aware or not. To be considered **context-aware**, an authentication method must use context information to improve the authentication process, for example by adjusting the authentication model based on context [WT19]. Otherwise, the authentication method is considered **context-unaware**.

Definition 6.3.8 (Usability)**.** Usability is a measure of how easy it is to utilize the authentication method for a user. While this can be subjective, it is still a very important metric that can be gathered from user studies or evaluations. We distinguish between **high**, **medium** and **low** usability. An authentication method is considered to have **high usability** if it is easy to use and does not require much effort from the user. If an authentication method requires some effort, cognitive load or specialized hardware, it is considered to have **medium usability**. Lastly, if an authentication method is difficult to use and requires a lot of effort from the user, it is considered to have **low usability**.

Definition 6.3.9 (Uniqueness)**.** Uniqueness describes whether the authentication method uses an authenticator that guarantees uniqueness such as a fingerprint or if it uses an authenticator that is only optionally unique such as a password or PIN. An authentication method is considered **guaranteed unique** if the authenticator is guaranteed to be unique for each subject, such as a fingerprint or an iris. This also applies if each subscriber is guaranteed to be assigned a unique authenticator, such as a unique password, even if the authenticator on its own is not guaranteed to be unique. If the subscriber is responsible for selecting a unique authenticator, the authentication method is considered to be **optionally unique**, as uniqueness is not guaranteed but depends on the subscriber's choice. Finally, if the authenticator is not unique at all, such as for a shared password or key, the authentication method is considered **non-unique**.

While non-unique authenticators are generally possible they provide less security but may be more usable in some scenarios.

Definition 6.3.10 (Cardinality)**.** Cardinality describes how many subjects authenticate to how many relying parties. The most common cardinality is **one-to-one**, but **many-to-one**

and **one-to-many** are also possible. An authentication method is considered **one-to-one** if a single subject authenticates to a single relying party, for example when simply logging in to a website with a password. If multiple subjects authenticate to a single relying party, the authentication method is considered **many-to-one**. This may be the case in physical environments where multiple subjects are continuously authenticated. If a single subject authenticates to multiple relying parties, the authentication method is considered **one-to-many**, such as when a user authenticates through a single-sign-on provider to multiple systems.

Definition 6.3.11 (Directionality)**.** Directionality indicates if an authentication method is unidirectional or bidirectional. An authentication method is **unidirectional** if only the subject authenticates to the relying party. In contrast, an authentication method is **bidirectional** if it authenticates the identity of both the subject and the relying party.

Definition 6.3.12 (Accessibility)**.** Accessibility describes how accessible the authentication method is to users with limited abilities or disabilities. This includes considerations for visual impairments, motor impairments and other factors that may otherwise exclude users from using the authentication method and thereby potentially accessing the service or system. While we think that accessibility is a very important aspect of authentication methods, it currently is not well covered in the literature. Therefore, we only provide a very coarse classification of **high**, **medium** and **low** accessibility and leave it to future work to provide a more detailed classification. An authentication method is considered to have **high accessibility** if it can be used by most or all users without any additional effort or special hardware. If an authentication method can be used by most users but requires some effort or special hardware, it is considered to have **medium accessibility**. Finally, if an authentication method is difficult to use for anyone with limited abilities or disabilities, it is considered to have **low accessibility**.

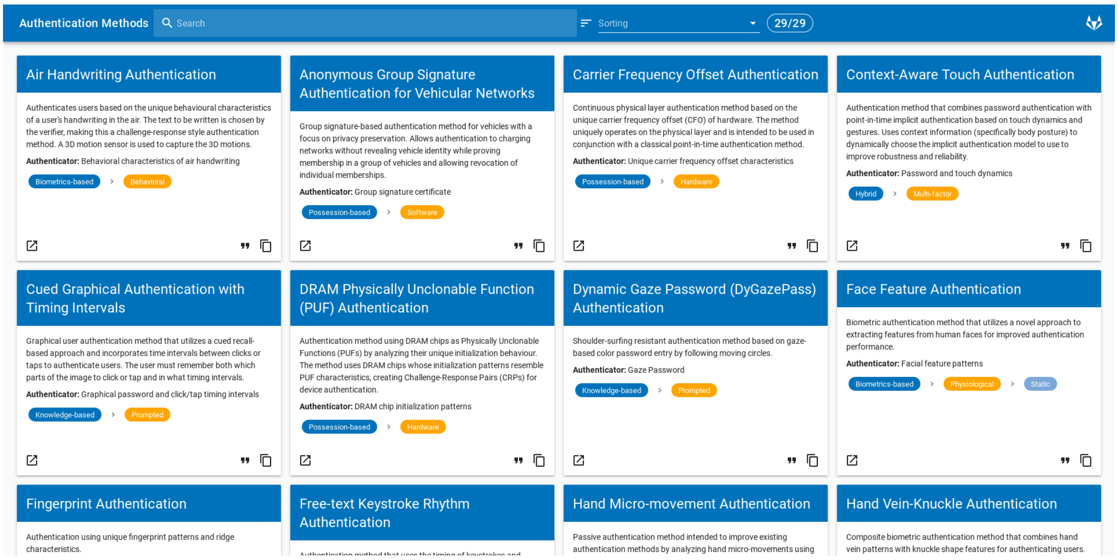
A facetted classification has the additional benefit of being easily extendable due to its orthogonal nature, which allows for the addition of new facets as needed. This is of particular importance as we have seen for example with the new requirement of privacy preservation in vehicular applications. Combining these facets with the hierarchical classification of authenticators from section 6.2 allows for a systematic comparison of authentication methods based on their unique characteristics.

7. Catalog of Authentication Methods

Contents

7.1. The Catalog Website

To validate the results of this thesis, we used our classification approach to create a publicly accessible website that contains a catalog of authentication methods. The website is available at `https://a-classification-approach-for-authentication-methods.pages.rwth-aachen.de/web-catalog/` and provides an overview of the authentication methods we analyzed in this thesis, including a full classification in accordance with the classification framework we presented in the previous chapter and the methodology described in section 4.4.



Air Handwriting Authentication

Authenticates users based on the unique behavioural characteristics of a user's handwriting in the air. The text to be written is chosen by the verifier, making this a challenge-response style authentication method. A 3D motion sensor is used to capture the 3D motions.

Authenticator: Behavioral characteristics of air handwriting

Biometrics-based › Behavioral

Anonymous Group Signature Authentication for Vehicular Networks

Group signature-based authentication method for vehicles with a focus on privacy preservation. Allows authentication to charging networks without revealing vehicle identity while proving membership in a group of vehicles and allowing revocation of individual memberships.

Authenticator: Group signature certificate

Possession-based › Software

Carrier Frequency Offset Authentication

Continuous physical layer authentication method based on the unique carrier frequency offset (CFO) of hardware. The method uniquely operates on the physical layer and is intended to be used in conjunction with a classical point-in-time authentication method.

Authenticator: Unique carrier frequency offset characteristics

Possession-based › Hardware

Context-Aware Touch Authentication

Authentication method that combines password authentication with point-in-time implicit authentication based on touch dynamics and gestures. Uses context information (specifically body posture) to dynamically choose the implicit authentication model to use to improve robustness and reliability.

Authenticator: Password and touch dynamics

Hybrid › Multi-factor

Cued Graphical Authentication with Timing Intervals

Graphical user authentication method that utilizes a cued recall-based approach and incorporates time intervals between clicks or taps to authenticate users. The user must remember both which parts of the image to click or tap and in what timing intervals.

Authenticator: Graphical password and click/tap timing intervals

Knowledge-based › Prompted

DRAM Physically Unclonable Function (PUF) Authentication

Authentication method using DRAM chips as Physically Unclonable Functions (PUFs) by analyzing their unique initialization behaviour. The method uses DRAM chips whose initialization patterns resemble PUF characteristics, creating Challenge-Response Pairs (CRPs) for device authentication.

Authenticator: DRAM chip initialization patterns

Possession-based › Hardware

Dynamic Gaze Password (DyGazePass) Authentication

Shoulder-surfing resistant authentication method based on gaze-based color password entry by following moving circles.

Authenticator: Gaze Password

Knowledge-based › Prompted

Face Feature Authentication

Biometric authentication method that utilizes a novel approach to extracting features from human faces for improved authentication performance.

Authenticator: Facial feature patterns

Biometrics-based › Physiological › Static

Fingerprint Authentication

Authentication using unique fingerprint patterns and ridge characteristics.

Free-text Keystroke Rhythm Authentication

Authentication method that uses the timing of keystrokes and

Hand Micro-movement Authentication

Passive authentication method intended to improve existing authentication methods by analyzing hand micro-movements using

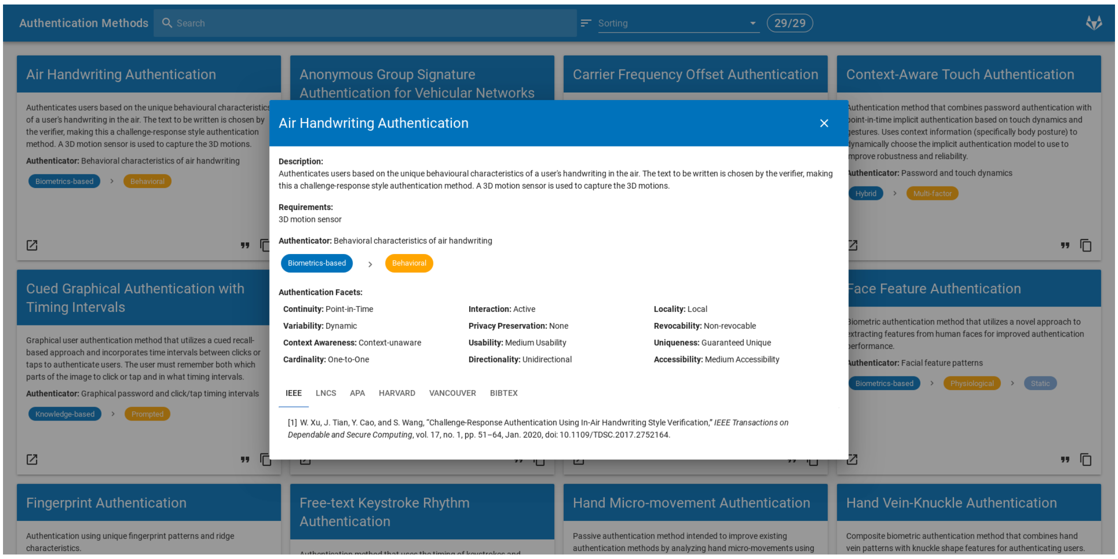
Hand Vein-Knuckle Authentication

Composite biometric authentication method that combines hand vein patterns with knuckle shape features for authenticating users.

Figure 7.1.: Screenshot of the authentication methods catalog website showing an overview of the authentication methods.

The website is based on a web application originally developed for cataloging service-based antipatterns by Bogner et al. [Bog+19] and modified to be used as a catalog of enterprise architecture refactorings by Salentin and Hacks [SH20]. We modified it to display relevant properties of authentication methods while retaining much of the original design and functionality. It is implemented in TypeScript using the Vue.js framework. Authentication methods are stored in separate JSON files and can be easily added or modified as needed. Deployment is done automatically using GitLab Pages and GitLab CI/CD pipelines.

As shown in figure 7.1, the website provides a simple user interface that allows browsing through the authentication methods. To access more details about a specific authentication method, users can click on the icon in the bottom left corner of each card to open a detail view as shown in figure 7.2. This view provides a short description of the authentication method, any specific requirements, and a full classification of the authentication method according to the classification framework presented in chapter 6. The source of each authentication method is also provided in various citation styles, including IEEE, APA, and BibTeX. By clicking on the icons in the bottom right corner of a card in the overview, users can also easily copy the bibliography entry of the authentication method or the full JSON file containing the authentication method's raw data.


Authentication Methods
Search
Sorting
29/29
Air Handwriting Authentication
Authenticates users based on the unique behavioural characteristics of a user's handwriting in the air. The text to be written is chosen by the verifier, making this a challenge-response style authentication method. A 3D motion sensor is used to capture the 3D motions.
Authenticator: Behavioral characteristics of air handwriting
Biometrics-based
Behavioral
Anonymous Group Signature Authentication for Vehicular Networks
Carrier Frequency Offset Authentication
Context-Aware Touch Authentication
Authentication method that combines password authentication with point-in-time implicit authentication based on touch dynamics and gestures. Uses context information (specifically body posture) to dynamically choose the implicit authentication model to use to improve robustness and reliability.
Authenticator: Password and touch dynamics
Hybrid
Multi-factor
Cued Graphical Authentication with Timing Intervals
Graphical user authentication method that utilizes a cued recall-based approach and incorporates time intervals between clicks or taps to authenticate users. The user must remember both which parts of the image to click or tap and in what timing intervals.
Authenticator: Graphical password and click/tap timing intervals
Knowledge-based
Prompted
Face Feature Authentication
Biometric authentication method that utilizes a novel approach to extracting features from human faces for improved authentication performance.
Authenticator: Facial feature patterns
Biometrics-based
Physiological
Static
Fingerprint Authentication
Authentication using unique fingerprint patterns and ridge characteristics.
Free-text Keystroke Rhythm Authentication
Hand Micro-movement Authentication
Passive authentication method intended to improve existing authentication methods by analyzing hand micro-movements using
Hand Vein-Knuckle Authentication
Composite biometric authentication method that combines hand vein patterns with knuckle shape features for authenticating users.
IEEE
LNCS
APA
HARVARD
VANCOUVER
BIBTEX

Air Handwriting Authentication

Description:
Authenticates users based on the unique behavioural characteristics of a user's handwriting in the air. The text to be written is chosen by the verifier, making this a challenge-response style authentication method. A 3D motion sensor is used to capture the 3D motions.

Requirements:
3D motion sensor

Authenticator: Behavioral characteristics of air handwriting

Biometrics-based › Behavioral

Authentication Facets:

Continuity: Point-in-Time
Variability: Dynamic
Context Awareness: Context-unaware
Cardinality: One-to-One
Interaction: Active
Privacy Preservation: None
Usability: Medium Usability
Directionality: Unidirectional
Locality: Local
Revocability: Non-revocable
Uniqueness: Guaranteed Unique
Accessibility: Medium Accessibility

[1] W. Xu, J. Tian, Y. Cao, and S. Wang, "Challenge-Response Authentication Using In-Air Handwriting Style Verification," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 51–64, Jan. 2020, doi: 10.1109/TDSC.2017.2752164.

Figure 7.2.: Screenshot of the authentication methods catalog website showing a detail view of an authentication method.

The website is intended to be a living document that can be easily extended and modified as soon as new research findings or authentication methods are available. By using a public git repository as the source of authentication methods, changes can easily be proposed, discussed, and tracked by anyone willing to contribute. The git repository is accessible from the website by clicking on the GitLab icon in the top right corner of the website or directly at `https://git.rwth-aachen.de/a-classification-approach-for-authentication-methods/web-catalog`.

8. Discussion

Contents

8.1. Key Findings

At the core of our findings stands the insight that classifying authentication methods purely hierarchically is not sufficient to capture the full breadth of their properties for all use cases. Given the wide variety of authentication methods and requirements for various use cases, we find that using a combination of a hierarchical classification that allows for a quick overview and a facetted classification that allows comparison of specific details between different methods is a more effective and extensible approach. It allows for a more nuanced understanding and comparison of authentication methods, which is necessary for researching and choosing authentication methods.

8.1.1. A novel split classification approach

Prior work on classifying authentication methods has primarily focused on the hierarchical classification of authentication methods based on the authenticator(s) used and which authentication factors they provide. Modern authentication methods, however, often combine multiple authenticators to provide multifactor authentication, which makes it difficult to classify them purely hierarchically. Additionally, many authentication methods have additional important characteristics, that may be partially or entirely independent of the authenticator(s) used. To address these issues, we propose to both extend the hierarchical classification of authenticators by adding a class for contextual authenticators and a class for hybrid authenticators. We also propose an additional facetted classification of authentication methods to capture additional characteristics of authentication methods that are not directly related to the authenticator(s) used. This allows for a more detailed comparison of authentication methods, by allowing a direct comparison of benefits and drawbacks, regardless of use case or domain, while retaining the benefits a hierarchical classification provides.

8.1.2. Trends and Insights

Another interesting discovery we made is the dominance of biometric authentication methods (15/24 included clusters) among the papers we reviewed. This is likely due to the increasing number of new biometric authentication methods being developed, while other kinds of authentication methods are already more mature and see less new authentication methods being introduced, but rather improvements to existing methods. Our search query and abstract screening process was also slanted in favor of novel and newly introduced authentication methods, as papers introducing new authentication methods are more likely to fully describe the authentication method itself rather than implementation details or evaluations or minor improvements of existing methods. We still saw some interesting developments in more traditional authentication methods, however, which focus on improvements to usability or security or adjusting them to new use cases.

Some major areas of research, which previous classifications did not cover, are the rising interest in passive and continuous authentication methods, which are becoming increasingly relevant in the context of mobile devices, smart environments, and the Internet of Things. Less popular yet evolving authentication factors like context-based authentication and introducing a separate class for hybrid authenticators, are also new additions to the classification approach. Introducing a secondary facetted classification while retaining the hierarchical classification also allows for a more nuanced comparison across use cases and domains, as it captures more of the details which may be relevant for specific use cases. It also allows for customization to fit a specific domain or use case by selecting the most relevant facets or extending them with additional facets. This can improve the usability of the classification approach by eliminating unnecessary complexity and focusing on more relevant facets for the specific use case.

8.2. Research Questions

Our results also allow us to fully answer the research questions we posed at the beginning of this thesis:

RQ1: Which methods of authentication exist?

We identified and analyzed 24 clusters of authentication methods, derived from the papers we reviewed. Across them, we identified five primary classes of authenticators: knowledge, possession, biometrics, context, and hybrid authenticators. While these authentication methods represent a variety of authentication methods that are currently researched, they are far from an exhaustive overview and do not represent the authentication methods currently used in practice. As discussed in previous chapters, simple classical authentication methods such as passwords and PINs are still what is most commonly used practice, while more advanced authentication methods are still establishing themselves [Yub24].

RQ2: Which characteristics of authentication methods can be used to group them into meaningful classes for systematic comparison?

In addition to the characteristics of the authenticator(s) used by an authentication method, we identified twelve other important facets of authentication methods. By combining these properties into a facetted classification, it is possible to systematically compare authentication methods to identify the most suitable method for a specific use case. The facets we identified are: continuity, interaction, locality, variability, privacy preservation, revocability, context awareness, usability, uniqueness, cardinality, directionality, and accessibility.

RQ0: How can we systematically describe and classify existing and future methods of authentication?

In summary, we propose a novel classification approach that combines an extended hierarchical classification of authentication methods based on the used authenticator(s) with a facetted classification that allows for a more detailed systematic comparison of authentication methods based on their characteristics. This approach is designed to be easily extensible and modifiable to allow for not only the classification of the existing authentication methods we reviewed, but also to cover new and emerging authentication methods and their unique properties.

8.3. Practical Applications

The classification approach we developed aims to be a practical aid in selecting the most suitable authentication method for a specific use case or evaluating existing authentication methods even across different domains. This section aims to demonstrate how it can be used in practice.

8.3.1. Selecting an Authentication Method for a Use-Case

The first step of selecting an authentication method for any given use case is to identify the requirements and constraints imposed by it. A smart home application for example, would require high accessibility and ease of use, with continuous passive authentication being ideal to ensure persistent access without repeated user interaction. On the other hand, a banking application would require high security, revocability and remote authentication capabilities and would also benefit from guaranteed uniqueness. Usability and accessibility are also very important, as users are likely to cover a wide range of technical expertise and demographics. Once the requirements have been identified, authentication methods classified within our approach can be filtered based on the selected facets and trade-offs between the characteristics can be compared. To aid in this process, the web catalog we created provides a simple user interface that shows the facets of each authentication method it contains and allows the user to gain a quick overview of the authentication methods available. As its contents are also available in machine-readable JSON format, it can easily be extended and integrated into recommender systems or other applications that aid in selecting authentication methods or building secure systems in general.

8.3.2. Domain-Specific Customization

As our framework is designed to be easily modifiable, it can be customized to better fit specific domains or use cases to, for example, serve as a guideline for future research in a specific area or as a resource for practitioners in a specific field. While the hierarchical part of the classification framework is rather fixed due to its hierarchical nature, it is also designed to already cover a wide range of use cases. The facetted classification, on the other hand, can easily be extended without modifying existing facets. Here it is only important to ensure that new facets are orthogonal to existing facets to avoid overlaps. By the same token, existing facets that are not relevant for a specific use case can be omitted to reduce complexity and thereby improve usability.

8.4. Limitations

As with any research, this work has some limitations that must be acknowledged. These limitations primarily stem from the methodological choices made to ensure the research was feasible within the timeframe and scope of a bachelor thesis. By utilizing a slimmed-down version of an SLR, we were able to rely on the structural benefits of an SLR but also lost some comprehensiveness and quality controls of a full SLR. This also includes using an LLM to assist in abstract screening and clustering of papers, which, while it proved effective, is still a relatively new method and needs further validation. Even though we performed validation of the abstract screening results using a small sample of papers, the results may still be biased by the limitations of the LLM or biases introduced due to the random selection of the sample. Additionally, it is possible that the fine-tuning of the LLM prompt resulted in overfitting to the specific set used for validation. This can lead to additional selection bias. The clustering approach is also based on existing research, but only takes paper titles into consideration, which may not fully represent the content of the paper and lead to attribution of papers to the wrong cluster or exclusion of relevant papers as outliers.

Given that the goal of this thesis was to provide a broad overview of authentication methods to derive a useful classification framework rather than create a comprehensive list of all authentication methods, we focused on selecting representatives for each cluster rather than exhaustively reviewing all papers in each cluster. This was another trade-off made to ensure feasibility and may have skewed the selection of papers towards more popular authentication methods or more active fields of research, as citation counts were used to select representative works. As authentication is also a very large and evolving field, many areas of research are certainly not covered by the selected papers, which is why the classification framework is designed to be extensible.

In general when classifying authentication methods, there are also some inherent challenges that must be acknowledged. While the goal of a classification is to provide clear and distinct classes without overlaps, the lines are often blurry in practice. As with all classification systems we have seen, the classification is based purely on the intended use of the authentication method and not on potential attacks or unintended uses. A biometric authentication method, such as fingerprint authentication for example, is obviously intended to require a fingerprint as authenticator, yet a replicated fingerprint, which would arguably be a possession authenticator, could potentially be used to also authenticate successfully. In an effort to improve the classification of authentication methods that did not fit into existing classifications, we introduced classes like the composite authenticator class, which is intended to easily classify methods that combine multiple authenticators as opposed to being forced to classify them as either knowledge-, possession-, or biometrics-based.

It should also be noted that the classification framework in its current form is not intended to be comprehensive but rather to provide a starting point for further research and development. It has not yet been validated in practice and while it is designed to be easily extensible, it may not cover all possible use cases. Validating and improving upon our classification approach, however, is a promising avenue for future research. As the classification is based on the state of research rather than common practice, it may not always be directly applicable to real-world scenarios without customization.

9. Conclusion & Future Work

Contents

9.1. Conclusion

This thesis addressed the challenge of systematically classifying and comparing authentication methods in an increasingly complex landscape. By analyzing 24 clusters of authentication methods and reviewing existing classification approaches, we developed a novel dual classification framework that combines a hierarchical classification of authenticators with a facetted classification of authentication methods across twelve key characteristics. Through extending traditional authenticator-based classes to include context-based and hybrid authenticators, we provide a more realistic representation of the current state of authentication methods. The additional facetted classification aids in a more systematic and requirements-oriented comparison of authentication methods, while also being easily extensible to accommodate future research. All of this allows for a more informed comparison and selection of authentication methods by practitioners and lays the groundwork for future research to expand on this framework. Our analysis also revealed significant trends in authentication research, particularly in the realm of biometric methods and the introduction of passive, continuous, and context-aware authentication methods to fit the needs of modern systems. By incorporating these trends into our classification framework and ensuring its extensibility, we aim to make a meaningful contribution to the field of authentication research.

9.2. Future Work

While we aim to lay a solid foundation for future research in the field of authentication, there is still a lot of research to be done. Our classification framework is extensible and customizable to allow for future research to build on it. The two major avenues for future research we see are the validation and extension of the classification framework through empirically evaluating whether it is useful in practice and by analyzing far more authentication methods than we could cover, and adding their unique characteristics to the framework. We already defined the terms we found most important to describe authentication and authentication methods. However, the field of authentication still uses many different terms and definitions, which can make it difficult to easily compare authentication methods. As ubiquitous language would improve many aspects of research in the field, this is certainly another area future research could focus on. Finally, each of the facets and classes we described in itself serves as an opportunity for future research to improve upon the level of detail within this specific facet or class.

A. Appendix

Contents

A.1. Prompt for the Abstract Screening Process

```
You will be presented with the title and abstract of a research paper.
You must decide if the paper is relevant.
Only papers that describe a **novel** and **concrete** **entity
    ↪ authentication method** as per the definitions below are
    ↪ relevant.
In particular a paper that focuses on **authenticity** or
    ↪ **authorization** as opposed to **authentication** is not
    ↪ relevant.
Applications of existing methods are not relevant, neither are
    ↪ analyses, improvements or surveys of existing methods.
Specifically only new **Authentication Factors** are of interest, not
    ↪ **Authenticators** using existing factors.
The paper must match the framework of the definitions provided.

The definitions are as follows:
**Entity**: An entity is any distinct thing or being. This includes
    ↪ people, devices or objects, etc.

**Authentication**: Authentication is the process of verifying an
    ↪ entity's identity, given its credentials.

**Authenticity**: Authenticity describes the property that data
    ↪ originated from its purported source.

**Authentication Method / Authentication Protocol**: An
    ↪ authentication method or protocol is a method used to obtain
    ↪ authentication of one or more entities to one or more other
    ↪ entities. The authentication provided may be unilateral or
```

```
mutual.

**Authentication Factor**: A factor used to prove ownership of an identity. This usually falls into one of three categories: Knowledge, Possession and Inherence. Every authenticator has one or more authentication factors.

**Authenticator**: An authenticator is something a claimant possesses and controls and that is used to authenticate a claimant's identity.

**Entity Authentication**: Entity authentication is the process by which one entity (the verifier) is assured of the identity of a second entity (the claimant) by the demonstration of possession and control of one or more authenticators associated with the claimed identity.

Take your time to analyze the title and abstract. Think step by step and make sure to provide a detailed response.
Your answer must contain your reasoning for the relevance judgement and a response in the following JSON format at the end.

<YOUR DETAILED THINKING HERE>

{
    "authentication_method": "<name of the authentication method described in the paper>",
    "authentication_factors": {
        "something you know": <0.0..1.0>,
        "something you have": <0.0..1.0>,
        "something you are": <0.0..1.0>
    },
    "use_case": ["<IoT, medical, mobile, ...>", ...],
    "entity_types: ["<user2machine, machine2user, user2user, machine2machine>"],
    "reasoning": "<reasoning for the relevance of the active entity authentication method described in the paper>",
    "relevant": <true|false>
}
```

Listing A.1: Prompt used to screen abstracts for relevance.

A.2. List of clusters with representative papers

Cluster Index	Chosen Cluster Name	Cluster Size
-1	*Outliers*	112
0	Physical Layer Authentication	37
1	Passive Mobile Device Authentication	27
2	Vehicular Authentication	27
3	Composite Biometric Authentication	24
4	Acoustics-based Biometric Authentication	21
5	Context-Aware Passive User Authentication	16
6	Passive User Authentication via Wearables	15
7	EEG-based Authentication	15
8	Full-Face Biometric Authentication	15
9	Alternative password-style Authentication	13
10	Physically Unclonable Hardware Authentication	12
11	Radar-based Human Authentication	12
12	ECG-based Authentication	11
13	Gait Authentication	11
14	Vein Authentication	10
15	HID usage dynamics based Authentication	10
16	Biometric Authentication for Mobile Devices	9
17[1]	Hardware Authenticity Verification	9
18	Biometric User Authentication	8
19	Handwriting-based Authentication	8
20	RFID-based Authentication	8
21	Shoulder-surfing resistant Authentication	8
22	Touch Behavior Authentication	7
23	Hand Physiology Authentication	7
24	Graphical Authentication	5

Table A.1.: The full list of clusters identified by the clustering algorithm, each with a chosen name to describe its contents.

[1] This cluster was excluded due to not containing any papers that match our criteria (they all focus on authenticity verification).

Cluster Index	Chosen Representative	Reason
0	"Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets," Hou et al. [Hou+14]	Most cited paper in the cluster.
1	"Please Hold on: Unobtrusive User Authentication Using Smartphone's Built-in Sensors," Buriro, Crispo, and Zhauniarovich [BCZ17]	Most cited paper in the cluster.
2	"An Anonymous Authentication Scheme for Plug-in Electric Vehicles Joining to Charging/Discharging Station in Vehicle-to-Grid (V2G) Networks," Chen, Zhang, and Su [CZS15]	Most cited paper in the cluster that matches our criteria (top 2 papers in the cluster are not related to entity authentication but rather to message authenticity).
3	"A Multi-Sample Multi-Source Model for Biometric Authentication," Poh, Bengio, and Korczak [PBK02]	Most cited paper in the cluster.
4	"Multimodal Biometric Authentication Using Teeth Image and Voice in Mobile Environment," Kim and Hong [KH08]	Most cited paper in the cluster.
5	"Context-Aware Implicit Authentication of Smartphone Users Based on Multi-Sensor Behavior," Wang and Tao [WT19]	Most cited paper in the cluster.
6	"PPGPass: Nonintrusive and Secure Mobile Two-Factor Authentication via Wearables," Cao et al. [Cao+20]	Most cited paper in the cluster.
7	"ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System," Klonovs et al. [Klo+13]	Most cited paper in the cluster.
8	"Face Authentication Using the Trace Transform," Srisuk et al. [Sri+03]	Most cited paper in the cluster.
9	"Neuromuscular Password-Based User Authentication," Jiang et al. [Jia+21]	Most cited paper in the cluster.
10	"DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication," Tehranipoor et al. [Teh+17]	Most cited paper in the cluster.
11	"HeartPrint: Exploring a Heartbeat-Based Multiuser Authentication With Single mmWave Radar," Wang et al. [Wan+22]	Most cited paper in the cluster.

continued on next page

Table A.2 – *continued from previous page*

Cluster Index	Chosen Representative	Reason
12	"Electrocardiogram (ECG) Biometric Authentication Using Pulse Active Ratio (PAR)," Safie, Soraghan, and Petropoulakis [SSP11]	Most cited paper in the cluster.
13	"Performance of Gait Authentication Using an Acceleration Sensor," Terada et al. [Ter+11]	Most cited paper in the cluster.
14	"Personal Authentication Using Hand Vein Triangulation and Knuckle Shape," Kumar and Prathyusha [KP09]	Most cited paper in the cluster.
15	"Key Classification: A New Approach in Free Text Keystroke Authentication System," Singh and Arya [SA11]	Most cited paper in the cluster.
16	"Your Song Your Way: Rhythm-based Two-Factor Authentication for Multi-Touch Mobile Devices," Chen et al. [Che+15]	Most cited paper in the cluster.
17	None	*This cluster does not contain any papers that match our criteria (they all focus on authenticity).*
18	"User-Specific Iris Authentication Based on Feature Selection," Qi et al. [Qi+08]	Most cited paper in the cluster.
19	"Challenge-Response Authentication Using In-Air Handwriting Style Verification," Xu et al. [Xu+20]	Most cited paper in the cluster.
20	"Ultralightweight RFID Reader-Tag Mutual Authentication," Huang and Jiang [HJ15]	Most cited paper in the cluster that matches our criteria (top 3 papers in the cluster are not related to entity authentication but rather to object authenticity).
21	"DyGazePass: A Gaze Gesture-Based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attacks," Rajanna et al. [Raj+18]	Most cited paper in the cluster.
22	"Touch-Interaction Behavior for Continuous User Authentication on Smartphones," Shen et al. [She+15]	Most cited paper in the cluster.

continued on next page

Table A.2 – *continued from previous page*

Cluster Index	**Chosen Representative**	**Reason**
23	"Biometric Authentication from Low Resolution Hand Images Using Radon Transform," Mostayed et al. [Mos+09]	Most cited paper in the cluster.
24	"Graphical User Authentication: A Time Interval Based Approach," Umar, Rafiq, and Ansari [URA12]	Most cited paper in the cluster.

Table A.2.: List of papers chosen as representatives for each cluster.

A.3. Paper Analysis Tooling

The tooling used to analyze the collected papers and to generate the visualizations shown in this thesis is available on the RWTH GitLab instance at `https://git.rwth-aachen.de/a-classification-approach-for-authentication-methods/public-data-collection`.

Bibliography

[AJ10] N. Ahmed and C. D. Jensen. "Definition of Entity Authentication." In: *2010 2nd International Workshop on Security and Communication Networks (IWSCN)*. May 2010, pp. 1–7. DOI: 10.1109/IWSCN.2010.5498000 (cit. on p. 2).

[AN22] N. Alsaeed and F. Nadeem. "Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues." In: *Applied Sciences* 12.15 (Jan. 2022). ISSN: 2076-3417. DOI: 10.3390/app12157487 (cit. on pp. 2, 11).

[Bar+22] M. Bartłomiejczyk et al. "User Authentication Protocol Based on the Location Factor for a Mobile Environment." In: *IEEE Access* 10 (2022), pp. 16439–16455. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3148537 (cit. on p. 7).

[BCZ17] A. Buriro, B. Crispo, and Y. Zhauniarovich. "Please Hold on: Unobtrusive User Authentication Using Smartphone's Built-in Sensors." In: *2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*. Feb. 2017, pp. 1–8. DOI: 10.1109/ISBA.2017.7947684 (cit. on pp. 27, 58).

[Boc23] M. Bock. "Measuring Adoption of Phishing-Resistant Authentication Methods on the Web." MA thesis. Stuttgart, Germany: Stuttgart Media University, 2023. URL: https://hdms.bsz-bw.de/frontdoor/index/index/docId/7038 (cit. on p. 1).

[Bog+19] J. Bogner et al. "Towards a Collaborative Repository for the Documentation of Service-Based Antipatterns and Bad Smells." In: *2019 IEEE International Conference on Software Architecture Companion (ICSA-C)*. Hamburg, Germany: IEEE, Mar. 2019, pp. 95–101. ISBN: 978-1-7281-1876-5. DOI: 10.1109/ICSA-C.2019.00025 (cit. on p. 45).

[Bon+12] J. Bonneau et al. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes." In: *2012 IEEE Symposium on Security and Privacy*. May 2012, pp. 553–567. DOI: 10.1109/SP.2012.44 (cit. on p. 1).

[Cao+20] Y. Cao et al. "PPGPass: Nonintrusive and Secure Mobile Two-Factor Authentication via Wearables." In: *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*. July 2020, pp. 1917–1926. DOI: 10.1109/INFOCOM41043.2020.9155380 (cit. on pp. 30, 42, 58).

[CAP21] I. Chenchev, A. Aleksieva-Petrova, and M. Petrov. “Authentication Mechanisms and Classification: A Literature Survey.” In: *Intelligent Computing*. Ed. by K. Arai. Cham: Springer International Publishing, 2021, pp. 1051–1070. ISBN: 978-3-030-80129-8. DOI: 10.1007/978-3-030-80129-8_69 (cit. on pp. 11, 36, 37).

[Che+15] Y. Chen et al. “Your Song Your Way: Rhythm-based Two-Factor Authentication for Multi-Touch Mobile Devices.” In: *2015 IEEE Conference on Computer Communications (INFOCOM)*. Apr. 2015, pp. 2686–2694. DOI: 10.1109/INFOCOM.2015.7218660 (cit. on pp. 26, 59).

[CMS13] R. J. G. B. Campello, D. Moulavi, and J. Sander. “Density-Based Clustering Based on Hierarchical Density Estimates.” In: *Advances in Knowledge Discovery and Data Mining*. Ed. by J. Pei et al. Berlin, Heidelberg: Springer, 2013, pp. 160–172. ISBN: 978-3-642-37456-2. DOI: 10.1007/978-3-642-37456-2_14 (cit. on pp. 21, 24).

[CZS15] J. Chen, Y. Zhang, and W. Su. “An Anonymous Authentication Scheme for Plug-in Electric Vehicles Joining to Charging/Discharging Station in Vehicle-to-Grid (V2G) Networks.” In: *China Communications* 12.3 (Mar. 2015), pp. 9–19. ISSN: 1673-5447. DOI: 10.1109/CC.2015.7084359 (cit. on pp. 34, 58).

[Gal+24] C. Galli et al. “Embeddings for Efficient Literature Screening: A Primer for Life Science Investigators.” In: *Metrics* 1.1 (Dec. 2024), p. 1. ISSN: 3042-5042. DOI: 10.3390/metrics1010001 (cit. on p. 12).

[Gol96] D. Gollmann. “What Do We Mean by Entity Authentication?” In: *Proceedings 1996 IEEE Symposium on Security and Privacy*. May 1996, pp. 46–54. DOI: 10.1109/SECPRI.1996.502668 (cit. on p. 2).

[Gro22] M. Grootendorst. *BERTopic: Neural Topic Modeling with a Class-Based TF-IDF Procedure*. Mar. 2022. DOI: 10.48550/arXiv.2203.05794. arXiv: 2203.05794 [cs] (cit. on p. 21).

[Gro24] M. Grootendorst. *BERTopic Documentation*. 2024. URL: https://maartengr.github.io/BERTopic/ (visited on 07/24/2025) (cit. on p. 21).

[Has+25] S. S. U. Hasan et al. “A Review on Secure Authentication Mechanisms for Mobile Security.” In: *Sensors* 25.3 (Jan. 2025), p. 700. ISSN: 1424-8220. DOI: 10.3390/s25030700 (cit. on pp. 1, 8).

[HJ15] Y.-C. Huang and J.-R. Jiang. “Ultralightweight RFID Reader-Tag Mutual Authentication.” In: *2015 IEEE 39th Annual Computer Software and Applications Conference*. Vol. 3. July 2015, pp. 613–616. DOI: 10.1109/COMPSAC.2015.106 (cit. on pp. 32, 59).

[Hou+14] W. Hou et al. “Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets.” In: *IEEE Transactions on Communications* 62.5 (May 2014), pp. 1658–1667. ISSN: 1558-0857. DOI: 10.1109/TCOMM.2014.032914.120921 (cit. on pp. 33, 58).

[Int10] International Organization for Standardization and International Electrotechnical Commission. *Information Technology — Security Techniques — Entity Authentication — Part 1: General*. International Standard ISO/IEC 9798-1:2010. July 2010 (cit. on p. 1).

[Jia+21] X. Jiang et al. "Neuromuscular Password-Based User Authentication." In: *IEEE Transactions on Industrial Informatics* 17.4 (Apr. 2021), pp. 2641–2652. ISSN: 1941-0050. DOI: `10.1109/TII.2020.3001612` (cit. on pp. 31, 58).

[JNR24] A. B. A. Julaihi, M. A. Ngadi, and R. Z. B. R. M. Radzi. "A Comprehensive Authentication Taxonomy and Lightweight Considerations in the Internet-of-Medical-Things (IoMT)." In: *International Journal of Advanced Computer Science and Applications* 15.8 (2024). ISSN: 21565570, 2158107X. DOI: `10.14569/IJACSA.2024.01508100` (cit. on p. 2).

[JSY25] S. Jajodia, P. Samarati, and M. Yung, eds. *Encyclopedia of Cryptography, Security and Privacy*. Cham: Springer Nature Switzerland, 2025. ISBN: 978-3-030-71520-5 978-3-030-71522-9. DOI: `10.1007/978-3-030-71522-9` (cit. on p. 2).

[KC07] B. Kitchenham and S. Charters. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Tech. rep. EBSE 2007-001. Keele University and Durham University Joint Report, July 2007 (cit. on pp. 11, 13, 14, 19).

[KH08] D.-S. Kim and K.-S. Hong. "Multimodal Biometric Authentication Using Teeth Image and Voice in Mobile Environment." In: *IEEE Transactions on Consumer Electronics* 54.4 (Nov. 2008), pp. 1790–1797. ISSN: 1558-4127. DOI: `10.1109/TCE.2008.4711236` (cit. on pp. 31, 58).

[Klo+13] J. Klonovs et al. "ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System." In: *IEEE Vehicular Technology Magazine* 8.1 (Mar. 2013), pp. 81–89. ISSN: 1556-6080. DOI: `10.1109/MVT.2012.2234056` (cit. on pp. 29, 58).

[KP09] A. Kumar and K. V. Prathyusha. "Personal Authentication Using Hand Vein Triangulation and Knuckle Shape." In: *IEEE Transactions on Image Processing* 18.9 (Sept. 2009), pp. 2127–2136. ISSN: 1941-0042. DOI: `10.1109/TIP.2009.2023153` (cit. on pp. 28, 59).

[Mah+18] N. A. Mahadi et al. "A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication." In: *Recent Advances in Cryptography and Network Security*. IntechOpen, Oct. 2018. ISBN: 978-1-78984-346-0. DOI: `10.5772/intechopen.76685` (cit. on p. 2).

[MHM20] L. McInnes, J. Healy, and J. Melville. *UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction*. Sept. 2020. DOI: `10.48550/arXiv.1802.03426`. arXiv: `1802.03426 [stat]` (cit. on pp. 21, 23, 24).

[Mic25] Microsoft AI. *Microsoft/MAI-DS-R1 [Large Language Model]*. 2025. URL: `https://huggingface.co/microsoft/MAI-DS-R1` (cit. on p. 16).

[Moh+09] D. Moher et al. “Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement.” In: *PLoS medicine* 6.7 (July 2009), e1000097. ISSN: 1549-1676. DOI: 10.1371/journal.pmed.1000097 (cit. on p. 18).

[Mos+09] A. Mostayed et al. “Biometric Authentication from Low Resolution Hand Images Using Radon Transform.” In: *2009 12th International Conference on Computers and Information Technology*. Dec. 2009, pp. 587–592. DOI: 10.1109/ICCIT.2009.5407305 (cit. on pp. 28, 60).

[NI20] Nils Reimers and Iryna Gurevych. *Sentence-Transformers/All-Mpnet-Base-v2 [Large Language Model]*. 2020. URL: https://huggingface.co/sentence-transformers/all-mpnet-base-v2 (cit. on p. 21).

[PBK02] N. Poh, S. Bengio, and J. Korczak. “A Multi-Sample Multi-Source Model for Biometric Authentication.” In: *Proceedings of the 12th IEEE Workshop on Neural Networks for Signal Processing*. Sept. 2002, pp. 375–384. DOI: 10.1109/NNSP.2002.1030049 (cit. on pp. 31, 58).

[Qi+08] M. Qi et al. “User-Specific Iris Authentication Based on Feature Selection.” In: *2008 International Conference on Computer Science and Software Engineering*. Vol. 1. Dec. 2008, pp. 1040–1043. DOI: 10.1109/CSSE.2008.1060 (cit. on pp. 28, 59).

[Raj+18] V. Rajanna et al. “DyGazePass: A Gaze Gesture-Based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attacks.” In: *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*. Jan. 2018, pp. 1–8. DOI: 10.1109/ISBA.2018.8311458 (cit. on pp. 32, 59).

[Rez+21] M. A. Rezazadeh Baee et al. “Authentication Strategies in Vehicular Communications: A Taxonomy and Framework.” In: *EURASIP Journal on Wireless Communications and Networking* 2021.1 (Dec. 2021), pp. 1–50. ISSN: 1687-1499. DOI: 10.1186/s13638-021-01968-6 (cit. on p. 2).

[RG19] N. Reimers and I. Gurevych. *Sentence-BERT: Sentence Embeddings Using Siamese BERT-Networks*. Aug. 2019. DOI: 10.48550/arXiv.1908.10084. arXiv: 1908.10084 [cs] (cit. on p. 21).

[SA11] S. Singh and K. V. Arya. “Key Classification: A New Approach in Free Text Keystroke Authentication System.” In: *2011 Third Pacific-Asia Conference on Circuits, Communications and System (PACCS)*. July 2011, pp. 1–5. DOI: 10.1109/PACCS.2011.5990168 (cit. on pp. 26, 59).

[Sch+24] S. Schulhoff et al. *The Prompt Report: A Systematic Survey of Prompt Engineering Techniques*. June 2024. URL: https://arxiv.org/abs/2406.06608v6 (visited on 05/09/2025) (cit. on pp. 11, 12, 16).

[SH20] J. Salentin and S. Hacks. “Towards a Catalog of Enterprise Architecture Smells.” In: *WI2020 Community Tracks*. GITO Verlag, Mar. 2020, pp. 276–290. ISBN: 978-3-95545-336-7. DOI: 10.30844/wi_2020_y1-salentin (cit. on p. 45).

[She+15] C. Shen et al. “Touch-Interaction Behavior for Continuous User Authentication on Smartphones.” In: *2015 International Conference on Biometrics (ICB)*. May 2015, pp. 157–162. DOI: 10.1109/ICB.2015.7139046 (cit. on pp. 26, 59).

[Shi07] R. W. Shirey. *Internet Security Glossary, Version 2*. Request for Comments RFC 4949. Internet Engineering Task Force, Aug. 2007. DOI: 10.17487/RFC4949 (cit. on pp. 2, 5).

[Sri+03] S. Srisuk et al. “Face Authentication Using the Trace Transform.” In: *2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings*. June 2003. DOI: 10.1109/CVPR.2003.1211368 (cit. on pp. 27, 58).

[SSP11] S. I. Safie, J. J. Soraghan, and L. Petropoulakis. “Electrocardiogram (ECG) Biometric Authentication Using Pulse Active Ratio (PAR).” In: *IEEE Transactions on Information Forensics and Security* 6.4 (Dec. 2011), pp. 1315–1322. ISSN: 1556-6021. DOI: 10.1109/TIFS.2011.2162408 (cit. on pp. 29, 59).

[Sye+13] S. Z. Syed Idrus et al. “A Review on Authentication Methods.” In: *Australian Journal of Basic and Applied Sciences* 7.5 (Mar. 2013), pp. 95–107. URL: https://hal.science/hal-00912435 (cit. on p. 8).

[TBL24] F. Tingelhoff, M. Brugger, and J. M. Leimeister. *A Guide for Structured Literature Reviews in Business Research: The State-of-the-Art and How to Integrate Generative Artificial Intelligence*. 2024. DOI: 10.1177/02683962241304105. (Visited on 05/09/2025) (cit. on pp. 11–13, 16).

[Teh+17] F. Tehranipoor et al. “DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication.” In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 25.3 (Mar. 2017), pp. 1085–1097. ISSN: 1557-9999. DOI: 10.1109/TVLSI.2016.2606658 (cit. on pp. 33, 58).

[Tem+24a] D. Temoshok et al. *Digital Identity Guidelines*. Tech. rep. NIST Special Publication (SP) 800-63-4 2pd. National Institute of Standards and Technology, 2024. URL: https://doi.org/10.6028/NIST.SP.800-63-4.2pd (cit. on p. 1).

[Tem+24b] D. Temoshok et al. *Digital Identity Guidelines: Authentication and Authenticator Management*. Tech. rep. NIST Special Publication (SP) 800-63B-4 2pd. National Institute of Standards and Technology, 2024. URL: https://doi.org/10.6028/NIST.SP.800-63b-4.2pd (cit. on pp. 5–7, 11).

[Ter+11] S. Terada et al. “Performance of Gait Authentication Using an Acceleration Sensor.” In: *2011 34th International Conference on Telecommunications and Signal Processing (TSP)*. Aug. 2011, pp. 34–36. DOI: 10.1109/TSP.2011.6043780 (cit. on pp. 25, 59).

[URA12] M. S. Umar, M. Q. Rafiq, and J. A. Ansari. “Graphical User Authentication: A Time Interval Based Approach.” In: *2012 IEEE International Conference on Signal Processing, Computing and Control*. Mar. 2012, pp. 1–6. DOI: 10.1109/ISPCC.2012.6224343 (cit. on pp. 32, 38, 60).

[Wan+20] C. Wang et al. “User Authentication on Mobile Devices: Approaches, Threats and Trends.” In: *Computer Networks* 170 (Apr. 2020), p. 107118. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2020.107118 (cit. on p. 11).

[Wan+22] Y. Wang et al. “HeartPrint: Exploring a Heartbeat-Based Multiuser Authentication With Single mmWave Radar.” In: *IEEE Internet of Things Journal* 9.24 (Dec. 2022), pp. 25324–25336. ISSN: 2327-4662. DOI: 10.1109/JIOT.2022.3196143 (cit. on pp. 2, 30, 58).

[Wei+20] T. Weißer et al. “A Clustering Approach for Topic Filtering within Systematic Literature Reviews.” In: *MethodsX* 7 (Jan. 2020), p. 100831. ISSN: 2215-0161. DOI: 10.1016/j.mex.2020.100831 (cit. on pp. 12, 21).

[WT19] R. Wang and D. Tao. “Context-Aware Implicit Authentication of Smartphone Users Based on Multi-Sensor Behavior.” In: *IEEE Access* 7 (2019), pp. 119654–119667. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2936034 (cit. on pp. 30, 42, 58).

[WZZ19] K. Wang, L. Zhou, and D. Zhang. “User Preferences and Situational Needs of Mobile User Authentication Methods.” In: *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. July 2019, pp. 18–23. DOI: 10.1109/ISI.2019.8823274 (cit. on p. 1).

[Xu+20] W. Xu et al. “Challenge-Response Authentication Using In-Air Handwriting Style Verification.” In: *IEEE Transactions on Dependable and Secure Computing* 17.1 (Jan. 2020), pp. 51–64. ISSN: 1941-0018. DOI: 10.1109/TDSC.2017.2752164 (cit. on pp. 27, 59).

[Yub24] Yubico. *State of Global Authentication Survey: A Holistic Approach to Combating Cyber Threats at Work and Home*. 2024. URL: https://resources.yubico.com/53ZDUYE6/at/fwps3xrj77fwfbnh46frs9x/Yubico_State_of_Global_Authentication_Survey_2024_White_Paper.pdf (visited on 07/20/2025) (cit. on pp. 1, 48).