TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Jaan Erik Lepp 232644IVCM

MAGIC LINK AUTHENTICATION FOR ENTERPRISE-LEVEL SAAS SOFTWARE USERS

Master's Thesis

Supervisor: Ricardo G. Lugo
PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Jaan Erik Lepp 232644IVCM

LINGIPÕHINE SISSELOGIMINE SAAS TARKVARA KASUTAJATELE ETTEVÕTETES

Magistritöö

Juhendaja: Ricardo G. Lugo
PhD

Tallinn 2025

Author’s Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Jaan Erik Lepp

18.05.2025

Abstract

Traditional password-based authentication presents numerous challenges for enterprise-level SaaS software users, including vulnerability to brute-force attacks, password reuse across multiple platforms, and the cognitive burden of remembering complex passwords. Magic link authentication emerges as a potential alternative that offers enhanced security while potentially improving user experience by eliminating the need for password management.

This research employs a mixed-methods approach to investigate end-user perceptions of magic link authentication in enterprise-level SaaS applications. The methodology combines quantitative data collected through an online survey distributed to business professionals with qualitative insights gathered from controlled usability testing sessions.

The findings reveal that while magic links offer benefits by eliminating password management and potentially improving security, they face significant practical challenges including email delivery issues, time inefficiency concerns due to application-email switching, and a knowledge gap regarding how magic link security works. The System Usability Scale assessment shows both authentication methods have excellent usability, with password authentication scoring slightly higher than magic links, highlighting the gap between theoretical benefits suggested in literature and actual user experiences in enterprise environments.

The thesis is written in English and is 82 pages long, including 7 chapters, 22 figures and 8 tables.

Annotatsioon
Lingipõhine sisselogimine SaaS tarkvara kasutajatele ettevõtetes

Traditsioonilisel paroolipõhisel autentimisel on mitmeid murekohti SaaS-tarkvara kasutajatele ettevõtetes. Nende hulka kuuluvad samade paroolide kasutamine erinevatel platvormidel, erinevate paroolide meelespidamine ja haavatavus parooli äraarvamise rünnakute vastu. Lingipõhine autentimine on potentsiaalne alternatiiv paroolidele, mis suurendab turvalisust ja parandab kasutajakogemust, kuna puudub vajadus paroolide haldamiseks.

Käesolev magistritöö kombineerib kvalitatiivse ja kvantitatiivse meetodi, et uurida kasutajate kogemusi lingipõhise autentimise kasutamisel tööalastes veebirakendustes. Kvantitatiivne info koguti veebipõhise küsitluse kaudu ning kvalitatiivse info kogumiseks kasutati põhjalikku autentimismeetodi kasutatavuse testimist.

Tulemused näitavad, et kuigi lingipõhine autentimine pakub eeliseid paroolide haldamise kaotamise ja suurema turvalisuse näol, on sellel ka mitmeid miinuseid. Näiteks puutuvad kasutajad kokku e-maili kohalejõudmise muredega ning puuduvad teadmised selle turvalisusest. Samuti on lingipõhine autentimine aeglasem kui paroolipõhine autentimine. Kasutatavuse testimine näitab, et mõlemat süsteemi on hea kasutada, kuid paroolipõhine autentimine sai veidi kõrgema tulemuse kui lingipõhine autentimine. See tulemus erineb kirjanduses välja toodud levinud arusaamast, et lingipõhine autentimine on kasutajate jaoks lihtsam ja kiirem.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 82 leheküljel, 7 peatükki, 22 joonist, 8 tabelit.

List of Abbreviations and Terms

UI	User interface
UX	User experience
SaaS	Software as a Service
SLR	Systematic Literature Review
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SUS	System Usability Scale
MFA	Multi-factor authentication
2FA	Two-factor authentication
OTP	One-time password
SSO	Single sign-on
ANOVA	Analysis of Variance

Table of Contents

List of Figures

List of Tables

1. Introduction

Software as a Service (SaaS) applications have become a game changer in today's fast-changing business technology environment. These cloud-based solutions significantly influence how companies consume and manage software. Unlike traditional software models that require extensive on-site infrastructure and complicated installation procedures, SaaS applications provide software solutions over the Internet, making them accessible through web browsers and mobile devices. This cloud-based model has opened the door for companies of all sizes to utilize advanced technological tools without the need for large initial capital expenditures.

In the rapidly evolving landscape of SaaS software, secure and user-friendly authentication mechanisms are crucial for web applications. Today's enterprise users often juggle numerous digital accounts on different platforms, ranging from communication tools and project management platforms to financial systems, customer relationship management software, and collaborative workspaces. While password-based systems are still common, they are increasingly being replaced by more advanced techniques like multi-factor authentication and passwordless alternatives.

1.1 Motivation

Traditional password-based authentication systems present numerous security challenges. Users often create weak and easy-to-guess passwords. [1, 2] These are good targets for brute-force attacks where attackers systematically attempt different combinations of passwords. When the same credentials are used across multiple systems, then compromise of one account can lead to compromise of all other accounts. Social engineering is used to trick users into entering their password through deceptive emails or fake websites. [1] There are also challenges regarding user experience. With the growing popularity of cloud-based software, users have more accounts and more passwords to remember, creating a cognitive burden and decrease in the ease of use. [1]

The prevalence of password-related security incidents continues to escalate in severity and scope. In 2024, two major data breaches highlighted the devastating impact of stolen credentials. Cloud data hosting provider Snowflake experienced a significant breach when attackers gained access through compromised username and password combinations, affecting 165 organizations that stored their data on the platform. [3] Among those impacted was Ticketmaster, where sensitive information of approximately 560 million customers was exposed. [4] Similarly, UnitedHealth suffered a breach when stolen credentials gave attackers access to systems containing personal information of nearly 190 million customers. [3, 5] In the UnitedHealth case, the attackers gained initial access by using compromised login credentials on a company remote desktop portal. [6] Despite industry best practices, two-factor authentication had not been enabled on these critical systems, allowing attackers to gain full entry with just the stolen passwords. These incidents demonstrate how password vulnerabilities can create enterprise-wide security disasters, affecting millions of individuals and causing substantial financial and reputational damage to the organizations involved.

In response to the challenges of traditional password-based systems, SaaS software providers have increasingly embraced passwordless authentication technologies. [7] Hardware tokens offer a physical form of multi-factor authentication, generating time-based one-time passwords or cryptographic challenges that significantly reduce the risk of remote attacks. [8] While highly secure, they require users to carry additional devices and may present accessibility challenges. Biometric solutions offer authentication based on unique physical or behavioral characteristics, such as fingerprint scanners, voice recognition, or facial recognition. [9] These methods provide good user experiences but may raise privacy concerns and require specialized hardware. [9] One-time password (OTP) codes sent via SMS are widely used and practical but vulnerable to rerouting attacks. [10]

Among these passwordless alternatives, magic link authentication has gained popularity due to its balance of security and implementation simplicity. Magic links function by sending a secure, unique, time-limited URL to a user's verified email address when they attempt to authenticate. [11] When the user clicks this link, they are automatically authenticated without needing to enter a password. This method leverages existing email infrastructure to create a secure authentication channel, with each link typically valid for only a short period. The security model relies on the assumption that only the legitimate user has access to the registered email account, essentially transforming email account security into application security. [11] For enterprise environments, this approach aligns well with existing access management systems, as email accounts are typically deactivated when employees leave the organization, automatically preventing access to applications using magic link authentication. [12] Implementation requires minimal changes to existing systems compared to biometric solutions, making it an attractive option for SaaS providers seeking to enhance security without substantial infrastructure changes. However, as with any authentication method, magic links present their own set of challenges, including reliance on email deliverability and dependency on email accessibility. [11, 13, 14]

Organizations using different SaaS software tools face another challenge called shadow IT, where employees independently adopt and use cloud-based applications and services without formal approval or oversight from the IT department [15, 16]. This creates multiple security problems, such as the potential exposure of sensitive corporate data to unauthorized access, compliance violations, and increased vulnerability to cyber threats through an expanded organizational attack surface. [15, 16] Magic link authentication can serve as a strategic mitigation tool by providing centralized identity management. Access to different SaaS software tools depends on the access to corporate email account this way. Magic links approach transforms shadow IT from a potential security liability into a more manageable challenge for organizations.

1.2 Scope

This thesis studies magic link authentication as a passwordless authentication solution, specifically selected for its relatively straightforward implementation within SaaS software platforms [2]. The research focuses on end-user perceptions of usability and security rather than technical aspects of implementation, examining how employees at various organizations experience and evaluate magic link authentication during their daily work activities. By comparing these experiences with traditional password-based systems, the study aims to develop a comprehensive understanding of magic link authentication within the broader context of authentication methods. This approach helps to identify both the benefits and challenges that affect adoption in workplace environments. The scope is limited to SaaS applications used for work purposes within organizational settings, excluding software designed for personal use, as enterprise environments present unique authentication challenges related to organizational security policies, account management, and employee access control.

1.3 Research Questions

The primary goal of this research is to establish a comprehensive understanding of how end-users perceive magic link authentication and its usability in enterprises. To help achieve this goal, following research questions are aimed to be answered:

1. What are the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software?
2. How does magic link authentication compare to password-based authentication in web applications from an end-users perspective?

1.4 Novelty

The thesis will provide novelty to the field of authentication systems by specifically studying magic link authentication in the enterprise-level SaaS context. Usability studies on magic link authentication so far have not differentiated user groups and the purpose of software being used. [17, 18] This study is among the first to systematically evaluate how organizational context and enterprise requirements influence user perceptions of magic link authentication, moving beyond the traditional focus on personal use cases. The findings will provide valuable insights for SaaS software providers and enterprise security architects, offering evidence-based recommendations for authentication system design. Additionally, the research methodology developed for this study could serve as a template for evaluating other emerging authentication methods in enterprise contexts.

The findings will contribute to the broader field of usability research in web application authentication solutions by providing empirical evidence on the effectiveness and user acceptance for one of the passwordless solutions. By focusing on the needs and expectations of enterprise users, this study will provide the understanding of how passwordless authentication can be successfully implemented in cloud-based solutions designed for organizations.

2. Systematic Literature Review

Systematic Literature Review (SLR) was conducted to assess the current state of art on the topic. For a transparent review process, Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines were followed. [19] PRISMA provides a structured framework that helps to minimize bias, increase reproducibility, and ensure critical evaluation of the review findings. This approach was chosen because it allows for a more reliable identification of existing evidence on magic link authentication and helps in clearly documenting the search, screening, and selection processes. [20] The review aims to address the following research questions:

- **[RQ1]**: What are the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software?
- **[RQ2]**: How does magic link authentication compare to password-based authentication in web applications from end-users perspective?

2.1 Information Sources

The systematic review utilized multiple digital libraries to ensure thorough coverage of relevant literature. The databases used for searching were ACM Digital Library, Web of Science, Sciencedirect and Scopus. These databases were chosen for their extensive coverage of computer science, information technology, and cybersecurity research. IEEE Xplore digital library was excluded because it was not accessible for the researcher at the time. The search keywords were developed through an iterative process. Initially, core terms directly related to the research topic ("magic link" and "authentication") were identified. These were then expanded to include synonyms and related concepts (such as "passwordless" and "email" for authentication methods, and "login" or "sign in" for the authentication process). Context-specific terms ("web" and "cloud") were added to focus the results on enterprise SaaS environments. The final search query used across all databases was:

("magic link" OR "passwordless" OR “email”) AND (authentication OR login OR “sign in”) AND ("web" OR “cloud”)

2.2 Eligibility Criteria

The inclusion and exclusion criteria are described in Table 1. Research is limited to papers written in English. Papers from before 2015 are excluded to ensure relevance to current technologies. Systematic literature review is focusing only on magic link authentication and papers on unrelated authentication systems are excluded.

Table 1. *SLR inclusion and exclusion criteria*

Inclusion	Exclusion
I1. Papers related to magic link authentication or email-based one-time password systems	E1. Non-peer-reviewed papers
I2. Papers related to authentication of cloud-based softwares	E2. Papers older than 2015
I3. Papers taking into account end-user perspective of authentication	E3. Papers not written in the English language

2.3 Selection Process

Total of 583 studies from database searches were exported to Zotero reference management software [21]. 71 duplicates were automatically found by the software and filtered out. Exported documents were first screened by reading the title and abstract to assess their compliance with eligibility criteria. During this phase, 486 studies were excluded, primarily because they did not meet the first inclusion criterion (I1). Many papers discussed other authentication mechanisms such as biometric authentication, multi-factor authentication, or traditional password systems without addressing magic links. Some papers were excluded based on criterion E2 (published before 2015) as they did not reflect current technology standards and user expectations. A total of 25 papers were downloaded for full-text review, of which 4 were included in the final selection. 21 excluded studies were not related to magic link authentication and therefore not eligible for this study.

Due to small number of studies found via database search, citation searching was used to get more complete overview of existing literature. An additional 10 studies were identified for full-text review through forward and backward citation searching. 5 papers were eligible to be included in the final selection. Selection process is visualized in Figure 1 according to PRISMA guidelines.

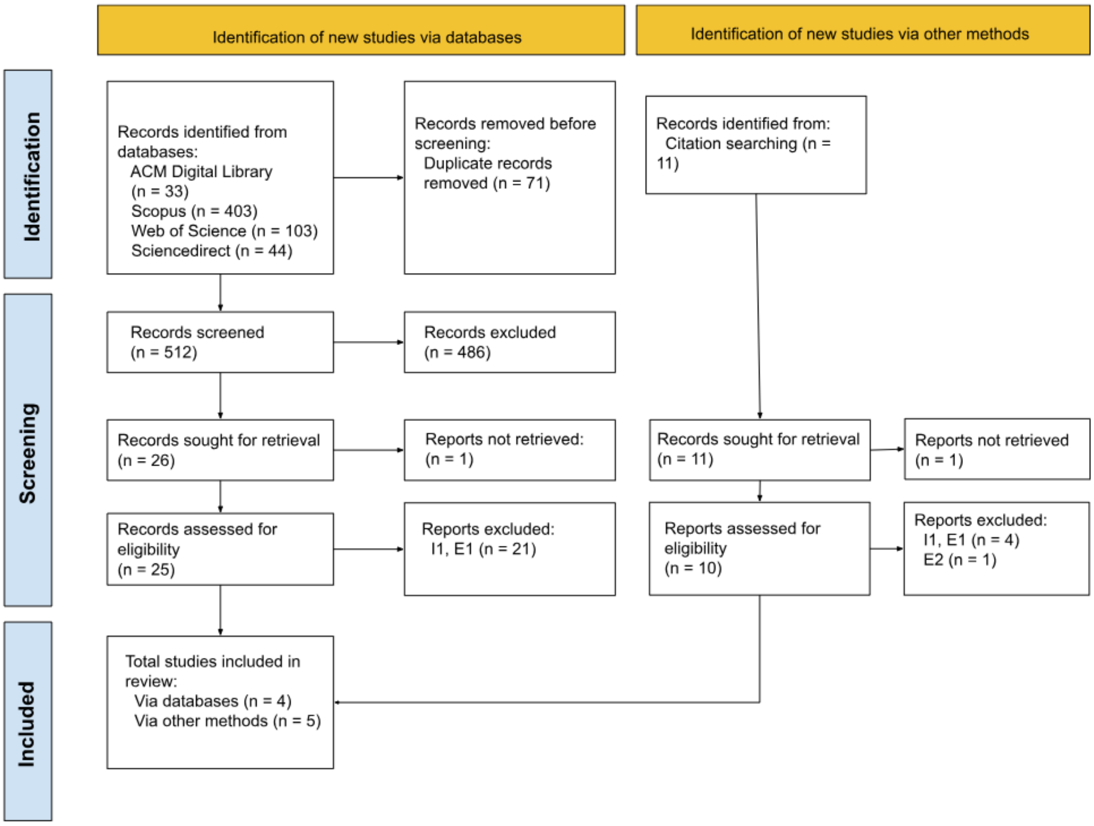

Identification of new studies via databases
Identification of new studies via other methods
Identification
Screening
Included
Records identified from databases: ACM Digital Library (n = 33) Scopus (n = 403) Web of Science (n = 103) Sciencedirect (n = 44)
Records removed before screening: Duplicate records removed (n = 71)
Records identified from: Citation searching (n = 11)
Records screened (n = 512)
Records excluded (n = 486)
Records sought for retrieval (n = 26)
Reports not retrieved: (n = 1)
Records sought for retrieval (n = 11)
Reports not retrieved (n = 1)
Records assessed for eligibility (n = 25)
Reports excluded: I1, E1 (n = 21)
Reports assessed for eligibility (n = 10)
Reports excluded: I1, E1 (n = 4) E2 (n = 1)
Total studies included in review: Via databases (n = 4) Via other methods (n = 5)

Figure 1. *PRISMA flow diagram*

2.4 Information Extraction

Information extraction from the selected studies focused on multiple key data points. The primary objective was to gather insights into the potential benefits and drawbacks of magic link authentication for end-users. Additionally, the extraction process aimed to understand end-users' perceptions of magic link authentication, particularly regarding its usability and security aspects. To provide context, comparisons with traditional password-based authentication systems were also extracted.

2.5 Results

In this section, the results of the literature review are summarized. Total of 9 studies were collected. Studies are grouped based on their methodology. Two empirical studies are seen in Table 2. Seven theoretical studies are visible in Table 3.

Table 2. *Empirical studies*

Author	Findings
Ruoti et al.	Participants preferred SSO authentication (average SUS score 75) over email-based (average SUS score 53.2) and QR-based authentication (average SUS score 68.4) options. Transparency was found to be important factor in usability. [17]
Taylor	For account sharing, participants preferred email-based links to passkey-based options because of better usability. [18]

Ruoti et al., "Authentication Melee: A Usability Analysis of Seven Web Authentication Systems" [17] Study compares three different authentication systems - SSO, email-based passwordless authentication and QR-code passwordless authentication. A total of 106 participants were recruited at Brigham Young University to conduct usability studies. Participants were asked to complete multiple tasks in two different websites by using different authentication options. To gather results, System Usability Scale (SUS) was used as a standardized questionnaire for usability. SUS is a well-established 10-item questionnaire that measures perceived usability on a scale from 0 to 100, providing a reliable and validated tool for comparing different user interfaces and systems. As a result, authors found that SSO was the most convenient to use by having the average system usability score of 75. Email-based solutions had average score of 53.2 and QR-based solutions 68.4. Also, qualitative feedback from end-users showed that transparency of authentication systems is highly valued. Around 95% of participants were undergraduate students, which affects generalizibility of results. Results do not provide insights into authentication in work-related applications as undergraduates have minimal work experience.

Taylor, "What's the Password? Account Sharing in the Context of Passwordless Authentication" [18] Taylor studied how account sharing can work with passwordless authentication methods. A total of 20 participants were recruited on a university campus for usability testing. The task was to sign up with a passkey or hardware token. Afterwards, participants were asked to evaluate authentication options and provide insights for sharing access to these accounts with other people. Most participants responded that setup via email link was the easier option compared to sharing passkeys. The author pointed out that email links are also frequently used as an authentication mechanism when resetting passwords. Several limitations must be acknowledged for the study. Only 20 participants were recruited from the university campus, which means that demographically participants were similar and generalizations cannot be made for all end-users. In addition, results were validated using qualitative feedback from participants and observations from the researcher, which could lead to biased conclusions based on the researcher's personal preferences.

Table 3. *Theoretical studies*

Author	**Findings**
Chaudhari et al.	Magic links have easy user experience, are fast and simple. [22]
Maqbali et al.	Password recovery emails, which are similar to magic link emails, were found to have multiple usability and security concerns among 50 websites studied. Usability for magic links largely depends on readability and trustworthiness of the emails. [23]
Matiushin et al.	Magic links are considered more secure than passwords because they eliminate vulnerabilities associated with many common cyber attacks that focus on obtaining or cracking passwords. Additionally, magic links offer improved convenience for users by removing the need to remember multiple complex passwords across different services. [24]
Ukwandu et al.	One-Time Passcode (OTP) via email, which is similar to magic links, was considered easy to use and secure by respondents of a survey on passwordless authentication methods with 204 respondents. [25]
Chowhan et al.	Passwordless authentication methods are considered to offer better user experience by simplifying the signup process in applications and eliminating the cognitive burden associated with remembering multiple passwords. On the downside, there is a risk of mailbox being compromised. [26]
Parmar et al.	Magic links are recognized as a user-friendly alternative to traditional passwords. However, email deliverability is identified as a significant disadvantage. [8]
Agrawal et al.	One-Time Passcode (OTP) via email are considered more secure than passwords. Elimination of password management reduces the administrative workload for IT departments. [27]

Chaudhari et al., "A Comprehensive Study on Authentication Systems" [22] Authors conducted a literature review on passwordless solutions and identified several weaknesses in password-based authentication systems. They highlighted research showing that a significant number of security breaches occur due to weak password practices. The authors argue that users now manage too many digital accounts to reasonably remember unique passwords for each one. Among the passwordless alternatives examined, they present magic link authentication as a promising option. The authors suggest this method offers improved security by eliminating password breaches while providing better user experience through simplified login procedures. However, it should be noted that these assessments of magic links are be based on theoretical analysis rather than empirical validation through user testing.

Maqbali et al., "Email-based password recovery — risking or rescuing users?" [23] Authors examined design issues in password recovery emails. The researchers analyzed emails from 50 popular websites by registering accounts, triggering recovery processes, and evaluating the received emails. They found several security problems: 44% of emails had unclear instructions, 70% lacked contact details, 40% didn't explain what to do if recovery wasn't requested, and 4% exposed recovery codes in headers or preheaders where they could be seen on locked devices. 88% of the websites used link for password recovery instead of code, which is very similar to magic link authentication process. Based on this study, the authors created practical recommendations for designing better recovery emails. These recommendations can also be followed when sending out magic link emails.

Matiushin et al., "Passwordless authentication using magic link technology" [24] Authors examined security vulnerabilities in traditional password-based systems and presented magic link authentication as an alternative. The authors highlight that up to 80% of successful cyber attacks exploit weaknesses in password protection systems, while users struggle with password management (33% need multiple login attempts and 60% reset passwords frequently). They describe how magic link authentication works through a unique, time-limited email link that eliminates the need for passwords. The researchers note that major companies like Google and Medium have already adopted this technology. Their findings are based on theoretical analysis and may present a biased perspective favoring this technology over traditional methods, since the study specifically focuses on promoting magic links. The authors highlight security benefits of magic links while not critically evaluating potential drawbacks or vulnerabilities of this approach.

Ukwandu et al., "Exploring The Views of End-Users On Passwordless Authentication Methods" [25] Researchers conducted an online survey to study user perceptions on different authentication methods with 204 respondents. One-Time Passcode (OTP) via email, which is similar to magic links, was considered secure and convenient authentication option. Most respondents were also using it daily. OTP was preferred for actions needing high security, such as payments. This study does not directly provide insights on user perceptions on magic links, but provides insights into how users perceived logging in via email (OTP).

Chowhan et al., "Password-Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites" [26] Authors introduce multiple passwordless authentication options to solve security challenges that come with password usage. All passwordless solutions are considered more secure and having better user experience. Authors say that the risk of mailbox being compromised is a downside for magic links as it would allow access to all the accounts using magic link authentication. This security risk occurs because magic links transfer the authentication responsibility to email account security - if an attacker gains access to a user's email, they can intercept all incoming magic links and potentially access multiple services. Multiple solutions are recommended to mitigate this risk. Study is a theoretical analysis of different passwordless solutions and does not validate the results. Focus is on the technical implementation.

Parmar et al., "A Comprehensive Study on Passwordless Authentication" [8] The authors conducted a comprehensive analysis of passwordless solutions through a review of existing literature, identifying specific advantages and disadvantages for each method. Their findings indicate that magic links represent a user-friendly and more secure alternative to traditional passwords. However, they highlight email deliverability as a significant limitation, noting that authentication emails may be bounced by servers, filtered as spam, or delivered with delays. It should be noted that the study does not provide empirical validation for these findings.

Agrawal et al., "Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behaviour Authentication" [27] In this paper, the authors examine web security across various authentication methods through an analysis of existing literature in the field. They primarily focus on multi-factor authentication and CAPTCHAs. The authors identify several benefits of One-Time Passwords (OTP) delivered via email, which function similarly to magic links. These benefits include reduced administrative workload for IT departments through elimination of password policy management. Additionally, OTPs help address security challenges related to account and password sharing. The authors also argue that OTP authentication provides greater security than traditional password systems. However, the study does not provide empirical validation to support these findings.

2.6 Discussion

This systematic literature review analyzed nine studies examining magic link authentication, aiming to understand its benefits and drawbacks for enterprise SaaS users and how it compares to password-based authentication. Of the nine studies reviewed, only two were empirical research papers [17, 18] providing user testing data, while seven were theoretical analyses [22, 23, 24, 25, 26, 8, 27].

The empirical studies by Ruoti et al. [17] and Taylor [18] provide valuable user-centered insights, though with notable limitations. Ruoti et al. conducted usability testing with 106 participants comparing different authentication systems and found that Single Sign-On (SSO) was preferred over email-based authentication methods. Their findings emphasized that users value transparency in authentication systems—they want to understand how the system works and protects their information. This suggests that magic link authentication, despite its potential usability benefits, may face adoption challenges if users don't understand its security model.

Taylor's study [18], though smaller in scale with only 20 participants, revealed that users find email-based authentication easier to set up than alternatives like passkeys. However, both studies were conducted with university participants rather than enterprise users, limiting their generalizability to workplace environments. The combined empirical evidence suggests a mixed reception for magic link authentication, with convenience being recognized but not always translating to overall preference.

The theoretical studies consistently identified several advantages of magic link authentication. Multiple authors, including Chaudhari et al. [22], Matiushin et al. [24], and Parmar et al. [8], argue that magic links enhance security by eliminating vulnerabilities associated with password-based systems such as password reuse, brute force attacks, and phishing attempts. This aligns with broader cybersecurity literature highlighting that password-related vulnerabilities are responsible for a significant portion of security breaches. [1, 2] From a usability perspective, Chowhan et al. [26] and Chaudhari et al. [22] emphasize that magic links reduce the cognitive burden of remembering multiple complex passwords — a particularly relevant benefit in enterprise environments where users may manage numerous accounts. However, as Parmar et al. [8] note, email deliverability represents a significant practical limitation that could undermine the usability benefits in real-world implementations.

The work by Maqbali et al. [23] on email design for password recovery provides valuable insights for magic link implementation, as the processes are technically similar. Their findings that 44% of emails had unclear instructions and 70% lacked contact details highlight the importance of thoughtful design in authentication emails — a factor not adequately addressed in most theoretical discussions of magic link authentication.

A critical gap emerges when comparing the theoretical studies with available empirical evidence. While theoretical papers consistently portray magic links as offering superior usability and security, the empirical studies suggest a more nuanced reality. Ruoti et al.'s [17] finding that users preferred SSO over email-based authentication contradicts the theoretical assumption that magic links provide a better user experience. The gap is further illustrated by the considerable difference in System Usability Scale scores reported by Ruoti et al. [17], where email-based authentication scored only 53.2 compared to 75 for SSO. This difference highlights the importance of user testing in authentication design and suggests that theoretical benefits may not always translate to actual user preference.

Addressing the research questions about benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software, the literature provides several clear insights. The primary benefits identified across multiple studies include enhanced security through elimination of password-related vulnerabilities. Chowhan et al. [26] and Matiushin et al. [24] note that magic links remove risks associated with password reuse, weak password selection, and vulnerability to brute force attacks. This is particularly valuable in enterprise environments where security breaches can have significant financial and reputational consequences. Additionally, the literature consistently highlights reduced cognitive burden for users as a major advantage. As Chaudhari et al. [22] emphasize, the growing number of SaaS applications used in workplace settings makes remembering unique, complex passwords increasingly challenging. Magic link authentication addresses this by removing the need for password creation and recall entirely. Improved user experience is also recognized as a key benefit, with Chaudhari et al. [22] and Parmar et al. [8] describing magic link authentication as more user-friendly and simpler to use.

However, the literature also identifies significant drawbacks. Email delivery issues emerge as the most critical limitation, with Parmar et al. [8] noting that authentication emails may be bounced by servers, filtered as spam, or delivered with delays. This creates a single point of failure that could prevent access to critical business applications. Additionally, Maqbali et al. [23] identify considerable inconsistency in the design and security of authentication emails, which could create usability challenges and security vulnerabilities if not properly addressed.

This systematic review reveals several important research gaps and limitations. Most notably, there is a significant absence of empirical studies examining magic link authentication in enterprise environments. The two empirical studies identified were conducted with university participants, who differ from business professionals in terms of security requirements, usage patterns, and organizational constraints. This limits the applicability of their findings to workplace contexts and highlights the need for enterprise-specific research.

Another notable gap in the collected studies was the absence of discussion on user and account management. While this may not be relevant for personal-use SaaS applications, it presents a significant challenge for enterprise-level users. [15, 16] Organizations need efficient methods to manage employee access to various SaaS tools used for daily work tasks. Magic link authentication offers a potential solution by validating email addresses for each login attempt. [11, 13, 14] Typically, when an employee leaves a company, their email account access is revoked. Consequently, for applications using magic link authentication, access to these software tools is automatically restricted as well. This feature of magic link authentication helps mitigate risks associated with shadow IT. Further research into this topic could potentially benefit enterprise security and access management.

Primary limitation of this systematic literature review is the small number of studies, which does not cover user experiences and opinions across different industries and organizational contexts. Additionally, the research only focused on user perceptions, leaving out factors like security implications and technical challenges. These are also important factors to consider when developing an authentication system for a cloud-based application.

2.7 Conclusion

Systematic literature review using the PRISMA guidelines was conducted to study the benefits and drawbacks of magic link authentication. In total 9 papers were collected from various digital databases. The findings answer RQ1 and RQ2 by showing that magic links are considered a more secure alternative for password-based systems. In addition, magic link authentication is considered more user friendly because there is no need to remember passwords. While this review provides valuable insights into the potential advantages of magic link authentication, several limitations must be acknowledged. Sample of 9 papers is relatively small and shows novelty of magic link authentication in the enterprise context. Moreover, only two papers conducted empirical studies to gather end-user perceptions. As enterprises continue to prioritize both security and user experience, further research on this topic would be beneficial.

3. Research Design

This research employs a mixed methods approach to research end-user perceptions of magic link authentication in enterprise-level SaaS applications. The systematic literature review revealed a significant gap in empirical research on magic link authentication, with only two identified studies examining user experiences, neither of which specifically focused on enterprise environments. To address this gap and provide more comprehensive insights, a two-phase mixed methods research design was used. This approach combines quantitative data collection through an online survey followed by qualitative usability testing, allowing for both extensive statistical evidence and detailed insights into how users actually experience these authentication methods. Both studies aim to answer the following research questions: "What are the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software?" (RQ1) and "How does magic link authentication compare to password-based authentication in web applications from an end-users perspective?" (RQ2).

The online survey (Study 1) provides quantitative data on user perceptions, authentication habits, and experiences with magic links across a broader sample of enterprise SaaS users. This approach allows for identifying patterns and correlations that can be statistically analyzed. The usability testing (Study 2) employs a controlled experimental design where participants interact with both authentication methods, providing qualitative insights into actual user behaviors and preferences. This complementary design enables methodological triangulation, where findings from both methods can be compared and integrated to validate outcomes and develop a deeper understanding of the research questions. The combined approach is particularly suitable for studying authentication methods, as it captures both large-scale user perceptions and detailed individual experiences with the technology in context.

4. Study 1 - Survey

The first study was conducted to gather quantitative data about end-users' perceptions of magic link authentication in enterprise-level SaaS software applications. To address the research questions, this survey aimed to collect insights from a bigger sample of business professionals who regularly use SaaS applications in their work environment.

The primary research question (RQ1) focuses on identifying the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software. Through this survey, data on participants' experiences with magic link authentication was collected, specifically measuring perceived benefits such as password management reduction and security improvement, as well as challenges like email delivery issues and time efficiency concerns. This systematic quantitative approach provided data about which aspects of magic link authentication are most valued by end-users and which present barriers to adoption in enterprise settings.

The second research question (RQ2) seeks to compare magic link authentication with password-based authentication in web applications from an end-user's perspective. The survey addressed this by examining participants' authentication habits and preferences between different authentication methods. Respondents reported which authentication methods they regularly use for work-related applications and whether they prefer magic links over password-based authentication. By gathering data on actual usage patterns and preferences, the survey provides insights into how magic link authentication compares to traditional password systems.

4.1 Methodology

To address the research questions about magic link authentication in enterprise-level SaaS applications, an online survey was created using Google Forms. The survey consisted of two sections covering different aspects of authentication experiences and perceptions. The complete questionnaire is available in Appendix 2. The first section gathered information about respondents' SaaS software usage habits. Questions included current job title, which types of web applications participants use (e.g., CRM, project management, communication tools), how often participants use them and how often they have to authenticate. In addition, participants were asked which authentication methods they use and how frequently they use magic links. This section provided baseline data about participants' existing authentication practices.

The second section formed the core of the survey, measuring participants' views of magic link authentication using six statements rated on a 5-point scale (from "strongly disagree" to "strongly agree"). These statements assessed features like usability ("Magic links simplify my login process"), time efficiency ("Magic links save me time compared to passwords"), security ("Magic links are secure"), reliability ("Magic links are reliable for business applications"), understanding ("I understand how magic links protect my account"), and overall preference ("I prefer magic links to password-based authentication"). These questions provided data about how participants evaluated different aspects of magic link authentication. Reliability score for the six statements was acceptable ($\alpha = 0.784$). This demonstrates that all questionnaire items are reliably measuring the same core aspect of users' perceptions toward magic link authentication.

The last two questions in the survey were about the benefits and challenges of magic link authentication through multiple-choice items where participants selected all options that applied to them. The benefits section included options such as "No password management," "Faster login process," "Improved security," "Better user experience," and "Fewer login issues." The challenges section included options like "Email delivery issues," "Link expiration issues," "Device switching problems," "Email access issues," and "Difficult to use." These questions directly addressed the first research question about the benefits and drawbacks of magic link authentication.

The survey was shared on LinkedIn, as it gave direct access to business professionals who use SaaS applications at work. The survey was active for three weeks during March 2025. To ensure participants had relevant experience, a screening question was included at the beginning. Only people who reported using at least one SaaS application for work purposes were included in the survey. This helped maintain the quality of responses by ensuring all participants had direct experience with SaaS software applications in work environment. For data analysis, data was first organized using Google Sheets. Statistical analysis was conducted using JASP [28], an open-source statistical software, with ANOVA and linear regression analysis performed to examine relationships between variables and differences across participant groups. For better overview, charts were created in Google Sheets for results of multiple questions.

4.1.1 Ethics

In conducting this survey, ethical considerations were prioritized to ensure participant privacy. All responses were collected anonymously, with no personally identifiable information required. Participants were informed about the research purpose and the voluntary nature of their participation, with a clear indication that the data would be used solely for academic research purposes as seen in Appendix 2 - Questionnaire. While demographic information such as job title was gathered to provide context to the findings, this information was collected and stored in a way that prevented the identification of individual participants.

4.2 Results

The survey received a total of 102 responses by people who regularly use at least one SaaS web application for work purposes. The following sections analyze these responses in detail, examining respondent demographics, authentication habits, perceptions of magic link authentication, and the benefits and challenges experienced when using this authentication method.

4.2.1 Respondent Demographics

For more concise analysis, job titles are categorized into 9 professional categories (Figure 2). The Business/Management sector was the most represented among the sample with 20.6%. This category includes roles such as project managers, business analysts, and executives. Administrative/Support roles (customer support specialists, assistants, etc.) comprised 17.6% of respondents. These were followed by Sales/Marketing (14.7%), Technology/IT (14.7%), Education (8.8%), and Creative/Design (6.9%). Financial, Logistics, and Other categories each represented less than 6% of respondents.

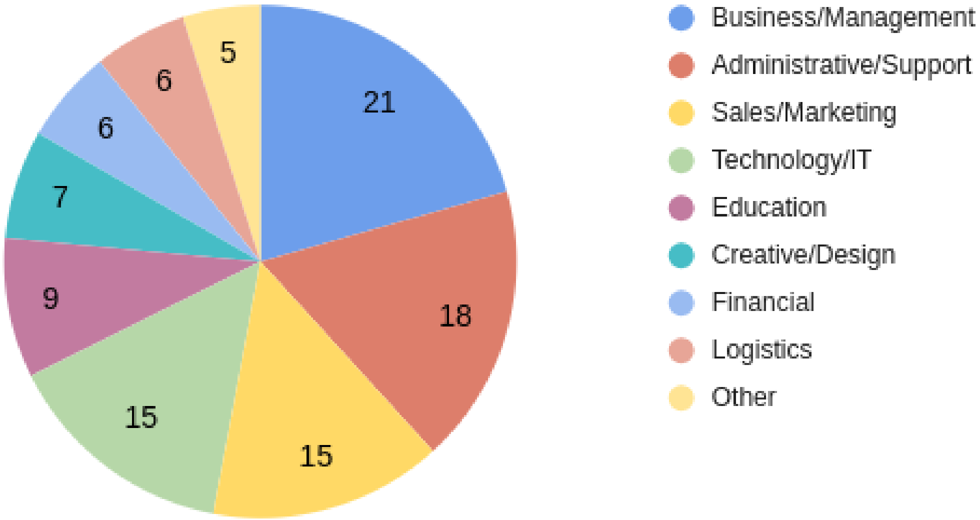


Figure 2. *Professional categories*

The survey sample was relatively evenly distributed across different professional categories, with no category exceeding 21% of respondents. This distribution helps gather more comprehensive data to draw broader conclusions. Important thing to note is the proportion of technical IT people in the sample. IT/technology sector represented 14.7% of participants, which is important considering that end-users working in IT might have a different perspective on the magic link authentication since they most likely understand the technical mechanisms behind it.

The criterion for survey participation was that respondents must regularly use at least one SaaS web application for work purposes. Figure 3 illustrates the number of different applications used by respondents in a typical work week. The largest group (49%) consisted of 50 respondents who regularly use 1-2 different work-related web applications. 26 respondents (25.5%) reported using 3-5 different applications, while 20 participants (19.6%) indicated using 6-10 applications. A smaller group of 6 respondents (5.9%) reported using more than 10 different SaaS applications regularly. These findings show that SaaS applications are widely used in workplaces, with more than half of the respondents regularly using 3 or more different SaaS applications. The high number of different applications used by employees highlights the need for convenient and secure authentication methods to help users manage their multiple work accounts.

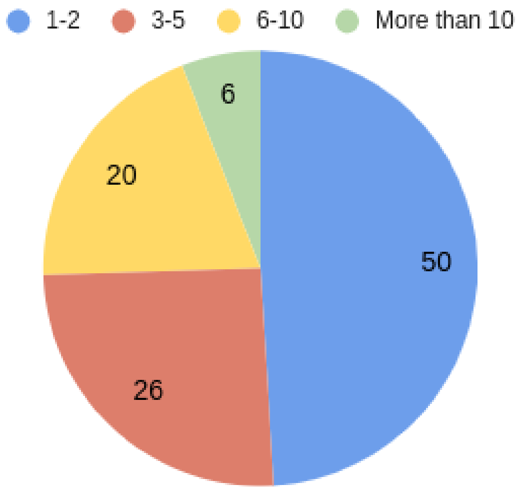


Figure 3. *Number of different web applications used*

When analyzing the types of SaaS software being used, two categories stand out (Figure 4). Communication/collaboration tools are used by 83 respondents and AI assistants are used by 81 respondents. High adoption rate for communication tools shows the important role they play in modern workplace environments, especially with the growing popularity of remote and hybrid work models where digital collaboration has become a necessity rather than an option. The similarly high usage of AI assistants is also notable as it represents a relatively newer category of SaaS tools that has gained traction.

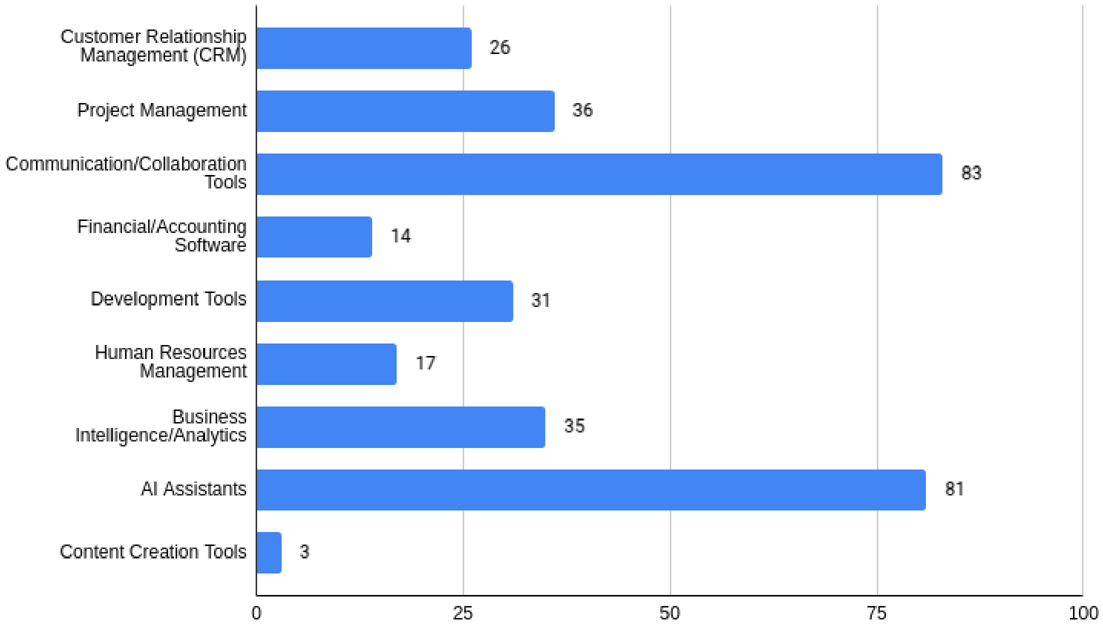


Figure 4. *Software types*

Other commonly used SaaS categories included project management tools (used by 36 respondents), business intelligence/analytics platforms (35 respondents), development tools (31 respondents) and CRM applications (26 respondents). While communication tools and AI assistants serve general purposes across all business operations, these other categories typically address specific business needs or departments. This explains the difference in adoption rates between the universal and specialized tools. The wide range of SaaS applications used shows how cloud-based software has become essential for most business operations.

4.2.2 Authentication Experience

Figure 5 illustrates how frequently respondents need to authenticate in different SaaS applications. The largest group (40.2%) consists of 41 respondents who authenticate multiple times per day across various applications. 27 respondents (26.5%) reported authenticating once a day, while 11 respondents (10.8%) authenticate several times per week, and another 11 (10.8%) authenticate weekly. The remaining 12 respondents (11.8%) authenticate less frequently than once a week.

These findings reveal that a majority of users (66.7%) authenticate at least once daily in their work-related SaaS applications, with 40.2% doing so multiple times throughout the workday. This high frequency of authentication displays the potential impact that authentication experiences can have on daily productivity and user satisfaction. For

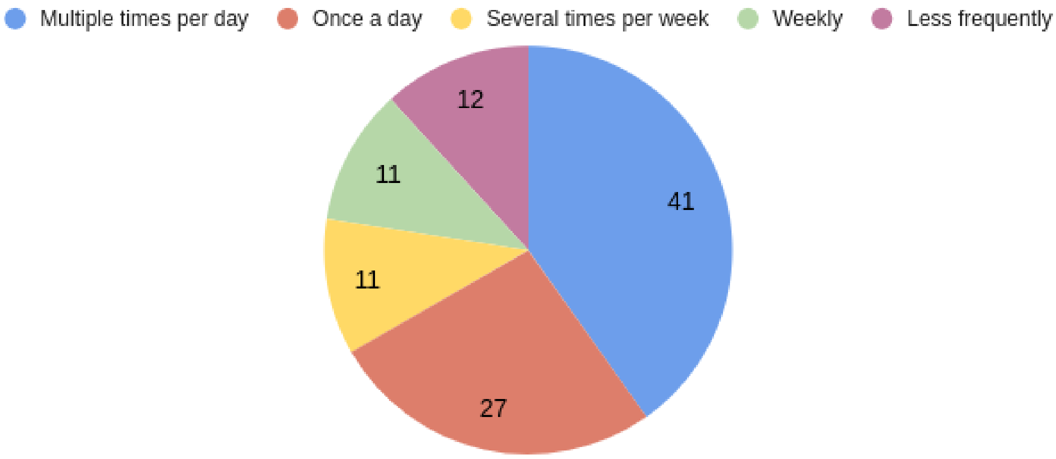


Figure 5. *Authentication frequency*

users authenticating multiple times per day, even small frictions or usability issues in the authentication process can pile up to create noticeable disruptions to workflow.

Figure 6 presents the authentication methods used by respondents for their work-related SaaS applications. Traditional passwords remain as the most popular option, with 97 respondents reporting their use. This shows how passwords remain standard in workplace applications despite their security challenges, such as brute-force attacks, phishing vulnerabilities and password reuse across multiple accounts. Two-factor authentication (2FA) is the second most common method, used by 76 respondents, showing that many organizations are adding extra security layers.

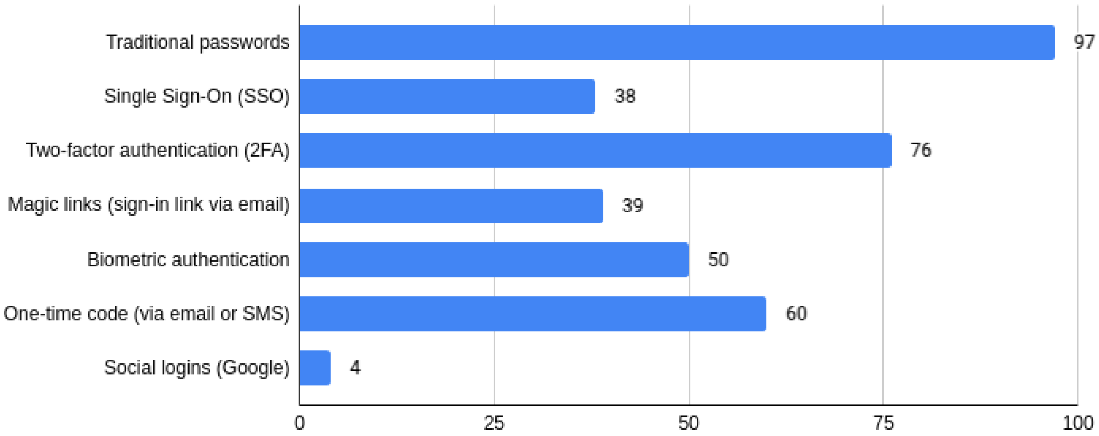


Figure 6. *Authentication methods*

One-time codes via email or SMS are used by 60 respondents, and biometric authentication by 50 respondents. Magic links, which are the focus of this research, are used by 39 respondents, similar to Single Sign-On (SSO) at 38 respondents. A total of 4 people added social login as an additional option that they are using for authentication.

The results show that most users use multiple authentication methods for their work applications, with each respondent using about 3.6 different methods on average. While passwords are still used by almost everyone, many SaaS software applications are adding other authentication options rather than replacing passwords completely. Magic links are currently used by over one-third of respondents, which means this method has gained some popularity in web applications but still has room to grow if users find it more secure and easier to use than passwords.

Figure 7 illustrates the frequency of magic link authentication usage among respondents. Nearly half of the participants (48 respondents, 47.1%) use magic links less frequently than once a week. Weekly usage was reported by 18 respondents (17.6%), while 12 respondents (11.8%) use magic links several times per week. Only a small minority use magic links on a daily basis, with 6 respondents (5.9%) using them once daily and just 1 respondent (1%) using them multiple times per day. It is also worth noting that 17 respondents (16.7%) reported never using magic links for authentication purposes.

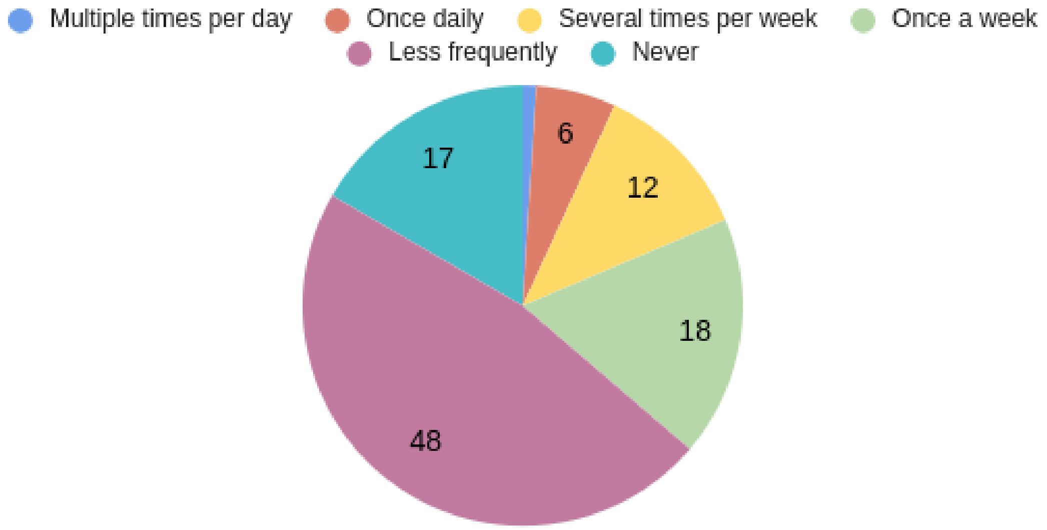


Figure 7. *Magic link usage*

The data reveals a significant difference between general authentication frequency and magic link usage. While 66.7% of respondents authenticate to various applications at least once daily, only 6.9% use magic links with the same frequency. This gap indicates that magic links currently serve as a secondary or occasional authentication method for most users rather than their primary means of accessing work applications. This limited regular usage may affect users' familiarity with the magic link process and therefore influence their perceptions of its usability and security benefits.

4.2.3 Perceptions

The survey included six statements regarding magic link authentication to assess participants' perceptions of this authentication method. Respondents were asked to rate their agreement with each statement on a five-point Likert scale ranging from "strongly disagree" to "strongly agree." These statements covered various aspects of magic link authentication, including usability, perceived security, reliability for business applications, and overall preference compared to password-based authentication. The following section presents and analyzes the responses to each statement.

The data regarding whether magic links simplify the login process reveals mixed opinions among respondents (Figure 8). Out of 102 participants, almost half (47.1%) expressed agreement with the statement, with 41.2% agreeing and 5.9% strongly agreeing that magic links simplify their login process. This suggests that approximately half of the users recognize the potential of magic links to reduce login complexity. A substantial portion (30.4%) remained neutral on this statement, indicating that these users may not have experienced significant differences in login simplicity between magic links and other authentication methods.

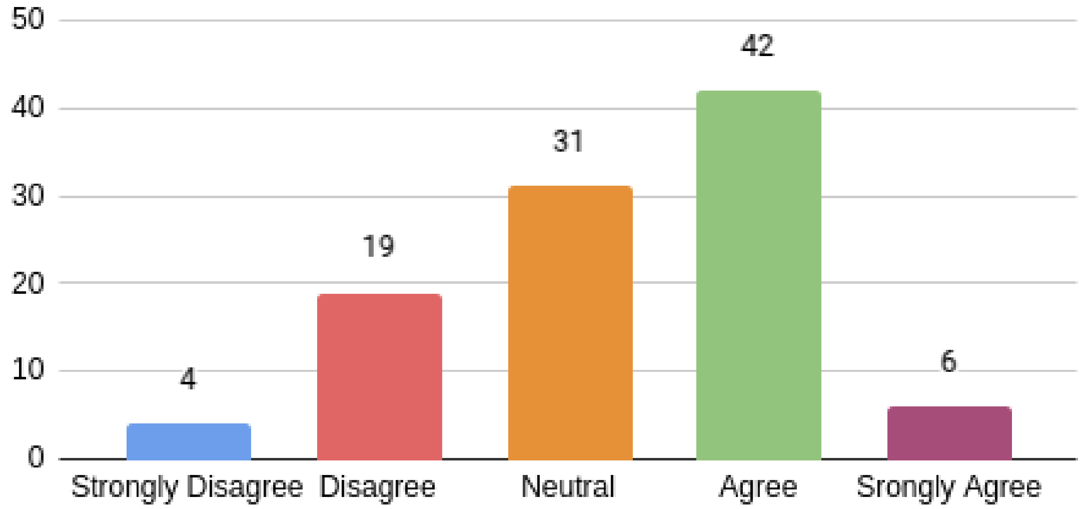


Figure 8. *Statement: Magic links simplify my login process*

A notable portion of respondents (22.5%) expressed disagreement with the statement, with 18.6% disagreeing and 3.9% strongly disagreeing that magic links simplify their login process. This relatively high percentage of negative responses suggests that usability challenges with magic links exist for a number of end-users. The moderate positive-to-negative ratio (47.1% agreement versus 22.5% disagreement) indicates that while magic links succeed in simplifying authentication for many users, there remains a considerable group who do not find this authentication method simpler than alternatives. These findings align with the SLR, which highlighted that magic links offer improved usability by eliminating the cognitive burden of remembering passwords. [26, 22]

Regarding time savings during authentication, respondents showed a more negative opinion (Figure 9). Out of 102 participants, half (50%) expressed disagreement with the statement, with 39.2% disagreeing and 10.8% strongly disagreeing that magic links save them time compared to passwords. This indicates that half of the surveyed users perceive magic links as a more time-consuming authentication method than traditional passwords. Only 17.6% of respondents agreed with the statement (14.7% agreed and 2.9% strongly agreed), suggesting that time efficiency is perceived as a weakness of magic link authentication. A substantial portion (32.4%) of respondents remained neutral on this statement.

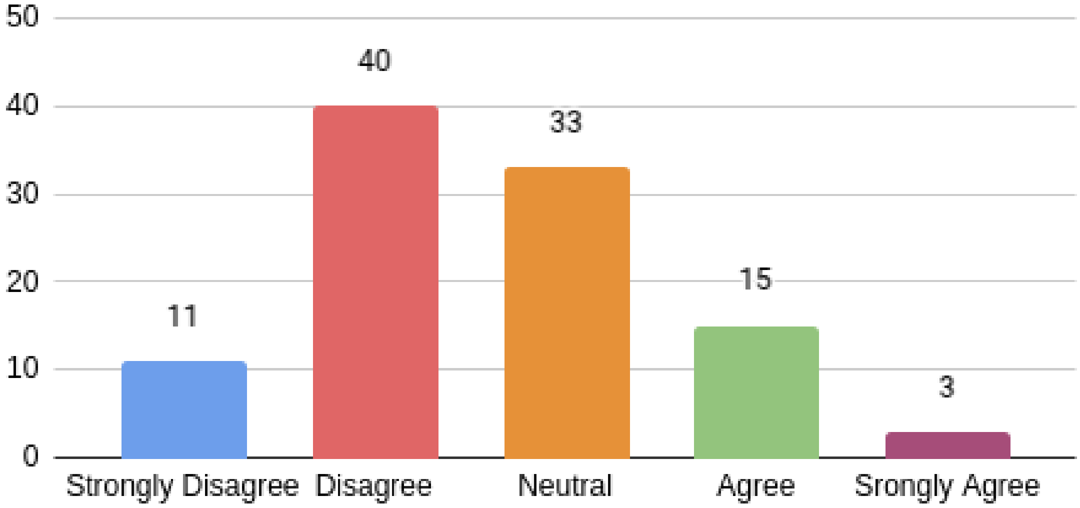


Figure 9. *Statement: Magic links save me time compared to passwords*

This data could be explained by multiple factors that contribute to how long it takes to authenticate with magic links. Most important factor is email deliverability which could take time depending on circumstances. Another factor is the need to switch between application and email client. In addition, authentication with passwords is substantially quicker when end-users use password managers or browser auto-fill features, which make signing in possible with just one click. It is important to note that speed is a critical component of overall usability; when an authentication method is perceived as slow, it can negatively impact the user experience regardless of other usability benefits. The time efficiency perception demonstrated here may therefore be an important barrier to magic link adoption in enterprise environments where employees need to authenticate frequently and switch between different applications.

Figure 10 illustrates opinions regarding security of magic links. The most notable finding is the large portion of neutral responses. Nearly half of the respondents (45.1%) neither agreed nor disagreed with the statement that magic links are secure, suggesting that end-users are uncertain about security of magic links. This high percentage of neutral responses shows that many end-users may not fully understand how magic link security works or how it compares to traditional password-based authentication.

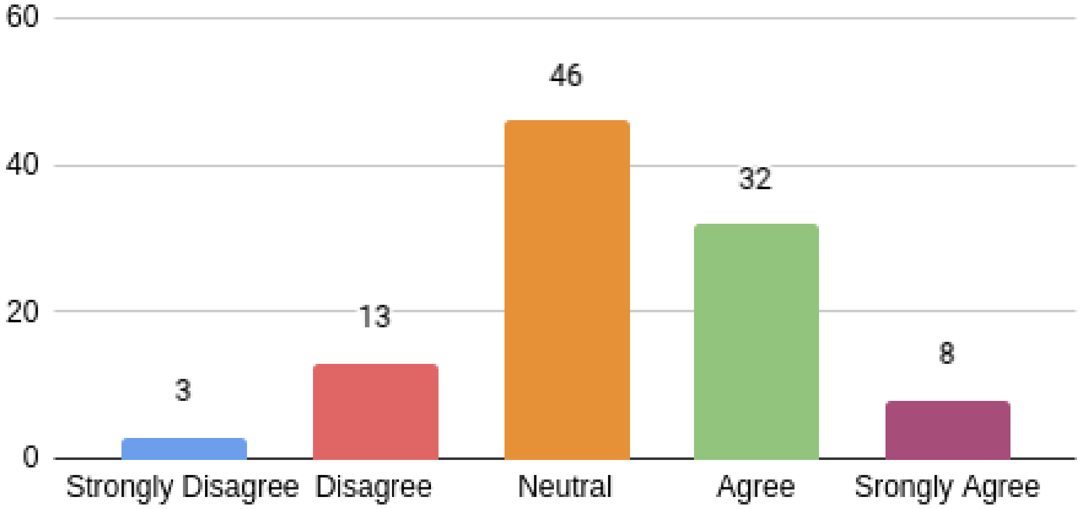


Figure 10. *Statement: Magic links are secure*

Among respondents who did express an opinion, more users trusted magic links than distrusted them. 39.2% of participants expressed agreement with the statement (31.4% agreed and 7.8% strongly agreed), while only 15.7% expressed disagreement (12.7% disagreed and 2.9% strongly disagreed). This shows that users who have formed an opinion about magic link security tend to view it positively. However, the high percentage of neutral responses points to a challenge - if users are unsure about security, they may hesitate to use magic link authentication in enterprise environments where data security is often a high priority.

Figure 11 displays perceptions regarding magic links reliability as authentication mechanism for business applications. 47.1% of respondents agreed with the statement that magic links are reliable for business applications (42.2% agreed and 4.9% strongly agreed). This indicates that nearly half of the surveyed users perceive magic links as a dependable authentication method for enterprise-level SaaS software. However, a considerable portion (36.3%) of respondents remained neutral, suggesting that many users may have limited experience with magic links or have had mixed experiences with their reliability.

A smaller group of respondents (16.7%) disagreed with the statement (15.7% disagreed and 1% strongly disagreed) that magic links are reliable for business applications. This disagreement likely comes from practical challenges such as email delivery issues, where authentication emails may be delayed, filtered by corporate email systems, or categorized

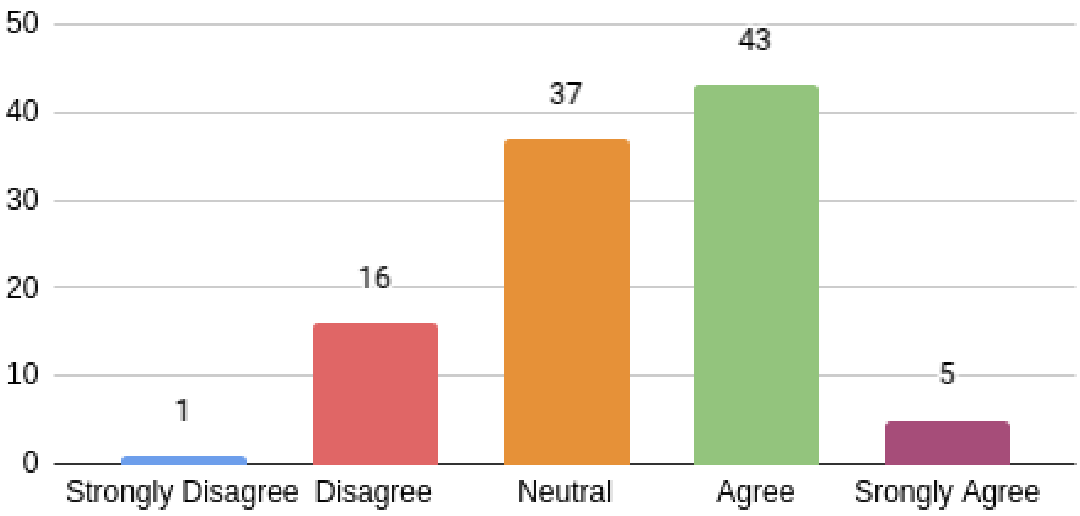


Figure 11. *Statement: Magic links are reliable for business applications*

as spam. Another potential factor behind this could be uncertainty about the security implications of using magic links for business-critical applications, where data breaches could have serious consequences.

Figure 12 shows results for the statement "I understand how magic links protect my account." Only 23.5% of respondents agreed with the statement (16.6% agreed and 6.9% strongly agreed). This is much less than for previous statement that magic links are secure, showing that users believe in security of magic links while not exactly knowing how it protects their account.

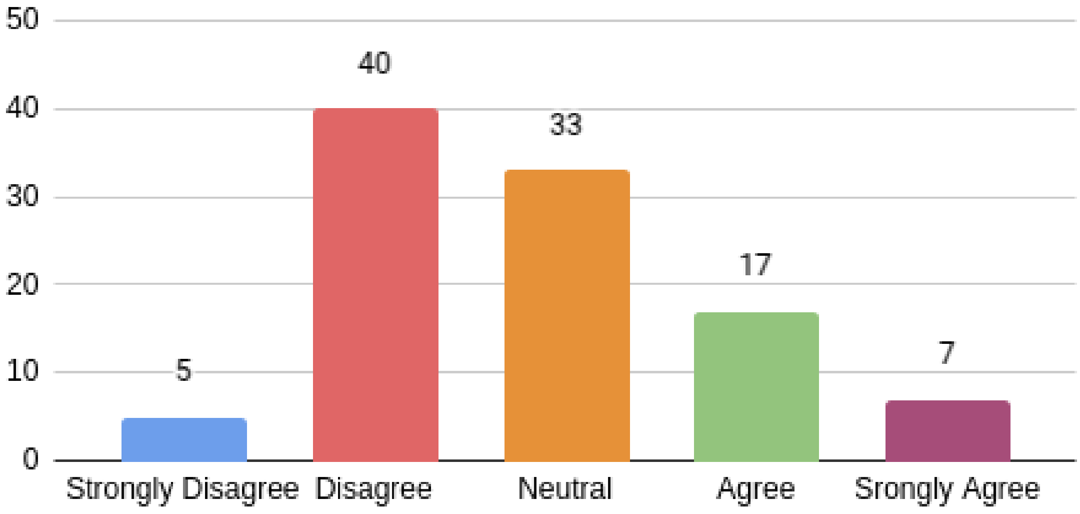


Figure 12. *Statement: I understand how magic links protect my account*

Large number of respondents (32.4%) were neutral and 44.1% of respondents disagreed with the statement (39.2% disagreed and 4.9% strongly disagreed). This knowledge gap points to a need for increased awareness about how magic links work. SaaS companies implementing magic link authentication should consider providing clear explanations about their security mechanisms, as users are unlikely to embrace authentication methods they don't understand, regardless of how secure those methods might actually be.

Figure 13 illustrates respondents' preferences between magic link and password-based authentication. The results show balanced distribution across opinions, with a slight preference toward passwords. 36 respondents (35.3%) remained neutral on this statement, suggesting that many users do not have a strong preference between these authentication methods. This may indicate that users see value in both methods depending on the specific context or application.

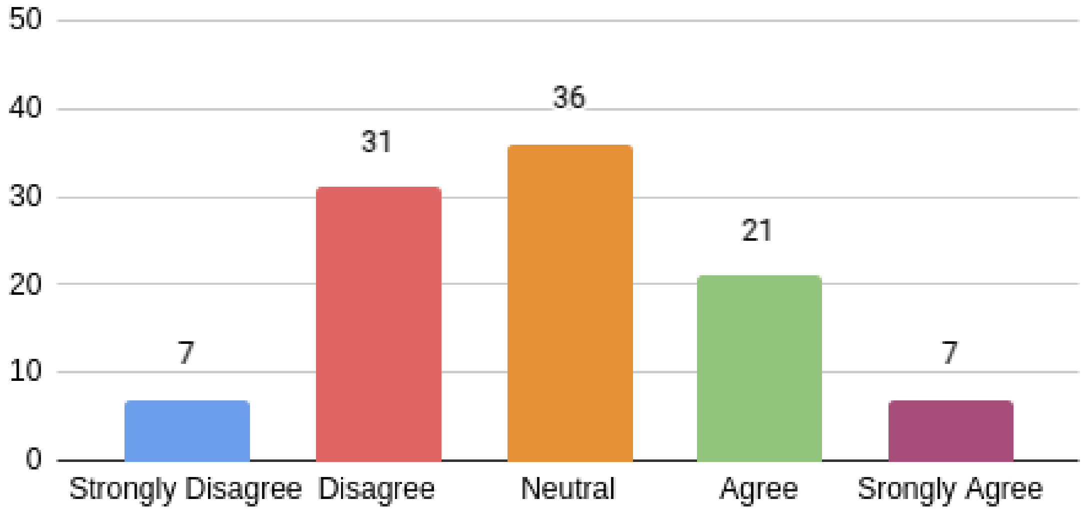


Figure 13. *Statement: I prefer magic links to password-based authentication*

Among respondents who expressed a preference, the distribution was also relatively balanced. 28 respondents (27.5%) indicated they prefer magic links (21 agreed and 7 strongly agreed), while 38 respondents (37.3%) preferred password-based authentication (31 disagreed and 7 strongly disagreed with preferring magic links). This slight preference toward password-based authentication aligns with the previous findings about time efficiency, where respondents indicated that magic links were perceived as more time-consuming. It also reflects the current dominance of password-based authentication systems in SaaS applications, which likely influences user familiarity and comfort. This preference for password-based authentication also aligns with the earlier findings about understanding security mechanisms, as users naturally tend to favor authentication methods they comprehend better. When users don't fully understand how magic links protect their accounts, they're more likely to stick with the familiar password approach.

Linear regression analysis (Table 4) was conducted to analyze which perception factors significantly predict users' preference for magic links over password-based authentication. Statement "I prefer magic links to password-based authentication" was chosen as the dependent variable and all other statements as the independent variables. Three factors emerged as significant predictors: perceived simplicity of the login process ($\beta = 0.499, p < 0.001$), security ($\beta = 0.296, p < 0.001$), and time efficiency compared to passwords ($\beta = 0.228, p = 0.004$). The standardized coefficients indicate that simplicity has the strongest influence on preference, with an impact nearly twice as strong as security perceptions. This suggests that users' preference for magic links is primarily driven by how much they simplify the authentication process rather than by security considerations.

Table 4. Linear regression analysis of perceptions

Variable	Unstandardized	Std. Error	Standardized (β)	t	p
Magic links simplify my login process	0.533	0.095	0.499	5.618	<0.001
Magic links save me time compared to passwords	0.242	0.082	0.228	2.967	0.004
Magic links are secure	0.340	0.099	0.296	3.451	<0.001
Magic links are reliable for business applications	-0.053	0.109	-0.043	-0.482	0.631
I understand how magic links protect my account	-0.011	0.078	-0.011	-0.144	0.886

Interestingly, while participants rated reliability for business applications relatively high, it did not significantly predict preference for magic links ($\beta = -0.043, p = 0.631$). Similarly, understanding how magic links protect accounts had virtually no impact on preference ($\beta = -0.011, p = 0.886$). This indicates that users' comprehension of the security mechanisms behind magic links is less important than their overall perception of simplicity and security. The regression model explained 58% of the variance in preference for magic links over passwords ($R = 0.769$, $R^2 = 0.583$, $F = 22.632, p < 0.001$), suggesting that these perception factors strongly influence authentication method preference.

To examine whether professional background influences authentication preferences, ANOVA analysis was conducted with job category as the independent variable and perception statements as dependent variables (Table 5). For five of the six perception statements, including simplicity ($F = 0.245, p = 0.972, \eta^2 = 0.022$), time efficiency ($F = 0.340, p = 0.933, \eta^2 = 0.030$), security ($F = 1.744, p = 0.111, \eta^2 = 0.138$), reliability ($F = 0.334, p = 0.936, \eta^2 = 0.030$), and overall preference ($F = 0.607, p = 0.749, \eta^2 = 0.053$), no statistically significant differences were found between job categories. This suggests that professional background does not significantly influence these aspects of how users perceive magic link authentication. These consistent perceptions across different professional roles indicate that factors beyond occupational context may be more influential in shaping attitudes toward these authentication aspects.

Table 5. ANOVA analysis of perceptions by job category

Variable	F	p	η^2
Magic links simplify my login process	0.245	0.972	0.022
Magic links save me time compared to passwords	0.340	0.933	0.030
Magic links are secure	1.744	0.111	0.138
Magic links are reliable for business applications	0.334	0.936	0.030
I understand how magic links protect my account	2.393	0.029	0.181
I prefer magic links to password-based authentication	0.607	0.749	0.053

However, a statistically significant difference emerged for understanding how magic links protect accounts ($F = 2.393, p = 0.029, \eta^2 = 0.181$). This finding suggests that professional background may influence users' comprehension of the security mechanisms behind magic link authentication. Post hoc comparisons using Tukey's test revealed that participants in Technology/IT roles reported higher understanding compared to Business/-Management roles (mean difference = 1.162, d = 1.196, p = 0.015) and Sales/Marketing roles (mean difference = 1.133, d = 1.166, p = 0.041). Although Technology/IT professionals also reported higher understanding compared to other job categories, these differences did not reach statistical significance. This finding highlights that professional background influences comprehension of security mechanisms, with technical professionals demonstrating a clearer understanding of how magic link authentication works compared to those in business management and sales roles.

4.2.4 Benefits

Figure 14 shows the benefits of magic link authentication as reported by survey respondents. "No password management" was the most valued advantage, selected by 86 respondents (84.3%). This high response rate indicates that users appreciate not having to create, remember, and manage passwords across multiple work applications. For employees who use many different SaaS tools daily, the elimination of password management appears to be the primary advantage of magic link authentication.

"Faster login process" and "Improved security" were equally popular among respondents, with each option selected by 42 participants (41.2%). It's noteworthy that many users see magic links as faster, even though earlier responses indicated that most didn't think magic links saved them time compared to passwords. This difference may be attributed to varying email delivery efficiency, different comparison points (manual password entry versus

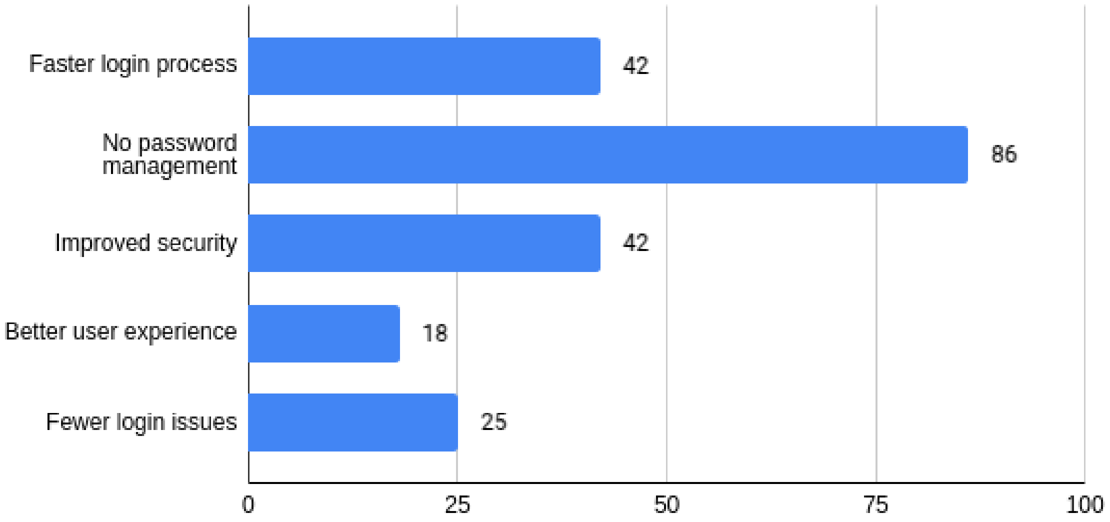


Figure 14. *Magic link benefits*

password managers with auto-fill functionality), or individual workflow preferences. The percentage of respondents identifying improved security as a benefit aligns with previous data where 39.2% of participants agreed that magic links are secure, showing consistency in security perceptions across different survey questions.

"Fewer login issues" was chosen by 25 respondents (24.5%), indicating that approximately a quarter of users experience fewer problems with magic links than with other authentication mechanisms. Common password-related issues such as forgotten credentials, account lockouts after failed attempts, and password reset procedures may be the main reason for this. Magic links seem to help some users avoid these difficulties.

Only 18 respondents (17.6%) selected "Better user experience" as a benefit. This relatively low number is interesting when compared to how many valued no password management, which is itself an aspect of user experience. This suggests that while users appreciate specific elements of magic links (the absence of password management), the overall experience — including email switching and potential delivery delays — is not perceived as improvement to traditional password authentication for most respondents. This finding contrasts with results from the systematic literature review, where multiple studies reported magic links as having good usability and being easy to use, suggesting a gap between theoretical assessments and real-world user experiences.

4.2.5 Challenges

Figure 15 presents the challenges users face when using magic link authentication. "Email delivery issues" was identified as the most significant challenge by a large margin, selected by 87 respondents (85.3%). This highlights that email deliverability remains the primary concern for magic link authentication in SaaS software applications. Factors such as corporate email filtering, spam categorization, and network connectivity can all affect the reliable delivery of authentication emails, potentially blocking access to the application.

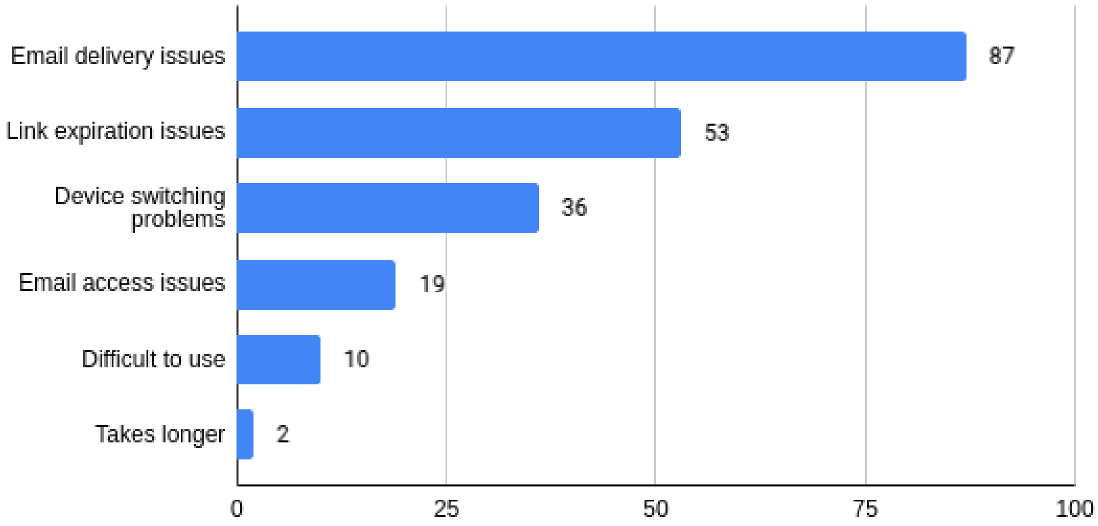


Figure 15. *Magic link drawbacks*

"Link expiration issues" ranked as the second most common challenge, selected by 53 respondents (52%). This indicates that over half of the users have encountered situations where magic links expired before they could use them. This problem likely occurs when users don't immediately notice authentication emails or when they get distracted by other tasks before completing the authentication process. Since security best practices recommend short expiration times for magic links, this creates a usability trade-off that affects many users.

"Device switching problems" was identified by 36 respondents (35.3%) as a challenge. This refers to difficulties that arise when users need to authenticate on one device but receive magic links on another. For instance, a user trying to log in on a work computer might receive the authentication email on their mobile phone, creating friction in the authentication process. This challenge particularly affects enterprise users who often work across multiple devices or in shared device environments.

"Email access issues" was selected by 19 respondents (18.6%), pointing to situations where users cannot access their email accounts when authentication is needed. This might occur due to separate email account lockouts, connectivity issues, or attempting to log in through shared accounts where email access isn't available. Only 10 respondents (9.8%) considered magic links "Difficult to use," suggesting that once email delivery and timing issues are addressed, the actual interaction with magic links is relatively straightforward for most users.

Additionally, 2 respondents (2%) specifically added that magic links "Take longer" than alternative authentication methods. While this represents a small percentage of respondents, it reinforces the earlier finding that time efficiency is a concern for magic link authentication. The overall response pattern suggests that most challenges with magic links are related to infrastructure and timing factors rather than fundamental usability problems with the authentication concept itself.

4.3 Discussion

This survey examined how enterprise users perceive and experience magic link authentication in their workplace environments, focusing on the benefits, challenges, and comparisons with traditional password-based systems. The results reveal several key findings that help address the research questions.

The first research question (RQ1) asked: "What are the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software?" The survey findings clearly identified password management elimination as the primary advantage, with 84.3% of respondents selecting this benefit. This matches what was found in the literature review, where studies from Chowhan et al. [26] and Chaudhari et al. [22] highlighted reduced cognitive burden as a main advantage of passwordless solutions. The regression analysis ($R^2 = 0.583$) strongly supports this finding, revealing that simplicity ($\beta = 0.499, p < 0.001$) was the most influential predictor of user preference for magic links, with almost twice the impact of security considerations ($\beta = 0.296, p < 0.001$). This statistical evidence confirms that users primarily value magic links for reducing cognitive load rather than for security enhancements.

However, the survey uncovered a contradiction between theory and practice in terms of user experience. While the SLR suggested that magic links would provide better overall usability [26, 22], only 17.6% of survey respondents selected "better user experience" as a benefit. This gap between theoretical assumptions and actual user perceptions is notable, suggesting that the benefits that appear clear in academic literature may not translate to real-world enterprise environments. The ANOVA analysis further supports this observation, showing no significant differences in perceptions across job categories for most variables (all $p > 0.05$), indicating that this contradiction between theory and practice exists regardless of professional background. The only exception was understanding of how magic links protect accounts, which showed a statistically significant difference among job categories ($F = 2.393, p = 0.029, \eta^2 = 0.181$).

The findings also revealed that email delivery issues represent a much more significant barrier than suggested in the literature. With 85.3% of respondents identifying this as a challenge, it becomes evident that the practical implementation of magic links faces difficulties that theoretical studies may underestimate. This practical challenge helps explain why time efficiency ($\beta = 0.228, p = 0.004$) emerged as a significant predictor of preference in the regression analysis. Parmar et al. [8] did mention email deliverability as a potential issue, but the survey suggests this problem is far more widespread than previously documented. Similarly, link expiration issues (52%) and device switching problems (35.3%) emerged as significant challenges that affect daily use.

Based on these findings, the survey provided substantial evidence regarding RQ1, identifying both clear benefits and significant challenges of magic link authentication. While password management elimination emerges as the primary advantage, the practical implementation challenges - particularly email delivery issues - represent more substantial barriers than theoretical literature had suggested.

The second research question explored: "How does magic link authentication compare to password-based authentication in web applications from an end-users perspective?" Despite the acknowledged burden of password management [26, 22], password-based authentication appears to maintain an advantage in perceived time efficiency. Half of the survey respondents disagreed that magic links save time compared to passwords, a finding that contradicts the theoretical benefits suggested in the literature [22, 26, 8]. This perception likely comes from the widespread use of password managers and browser auto-fill features, which allow users to authenticate with a single click, eliminating the need to manually type passwords.

The security perceptions revealed an interesting pattern. While more users trusted magic link security (39.2%) than distrusted (15.7%), nearly half (45.1%) remained neutral. More concerning is that 44.1% of respondents indicated they don't understand how magic links protect their accounts. This knowledge gap can represent a barrier to adoption. As Ruoti et al. [17] found in their empirical research, users value transparency in authentication systems, and the lack of understanding about how magic links work likely contributes to hesitation in using this technology.

These mixed perceptions were reflected in the overall preference data, with slightly more respondents (37.3%) preferring password-based authentication over magic links (27.5%), while a substantial portion (35.3%) remained neutral. This distribution suggests that while magic links offer certain advantages, they haven't yet demonstrated sufficient improvements over password-based systems to drive widespread preference among enterprise users.

The survey findings provide a comprehensive answer to RQ2, demonstrating that from end-users' perspectives, magic link authentication currently compares less favorably to password-based authentication than theoretical literature suggests. Despite its potential security advantages, magic links face significant challenges in perceived time efficiency and user understanding of security mechanisms.

4.3.1 Limitations

This study acknowledges several methodological limitations that should be considered. First, the sample size and demographic distribution may not fully represent the diverse range of enterprise SaaS users across different industries, technical proficiency levels, and organizational sizes. This limits how the findings of this study could be used for generalization. Second, since the survey relied on self-reporting, participants' responses may have been affected by recall bias, especially when reporting on authentication habits across multiple applications.

4.4 Conclusion

This study employed a quantitative survey methodology to gather data about enterprise users' perceptions of magic link authentication in SaaS applications. The online survey collected 102 responses from business professionals across various industries, with participants answering questions about their authentication habits, preferences, and experiences. The results revealed that while users highly value the elimination of password management (84.3% selected this as a benefit), they face significant challenges with magic link implementation, particularly email delivery issues (85.3%) and concerns about time efficiency (50% disagreed that magic links save time). Statistical analysis showed that perceived simplicity ($\beta = 0.499, p < 0.001$), security ($\beta = 0.296, p < 0.001$), and time efficiency ($\beta = 0.228, p = 0.004$) were significant predictors of preference for magic links, explaining 58.3% of the variance. Additionally, nearly half of respondents (44.1%) indicated not understanding how magic links protect their accounts, suggesting a knowledge gap in that area. These findings demonstrate a clear disconnect between the theoretical benefits of magic link authentication described in literature and the practical experiences of enterprise users.

5. Study 2 - Usability Testing

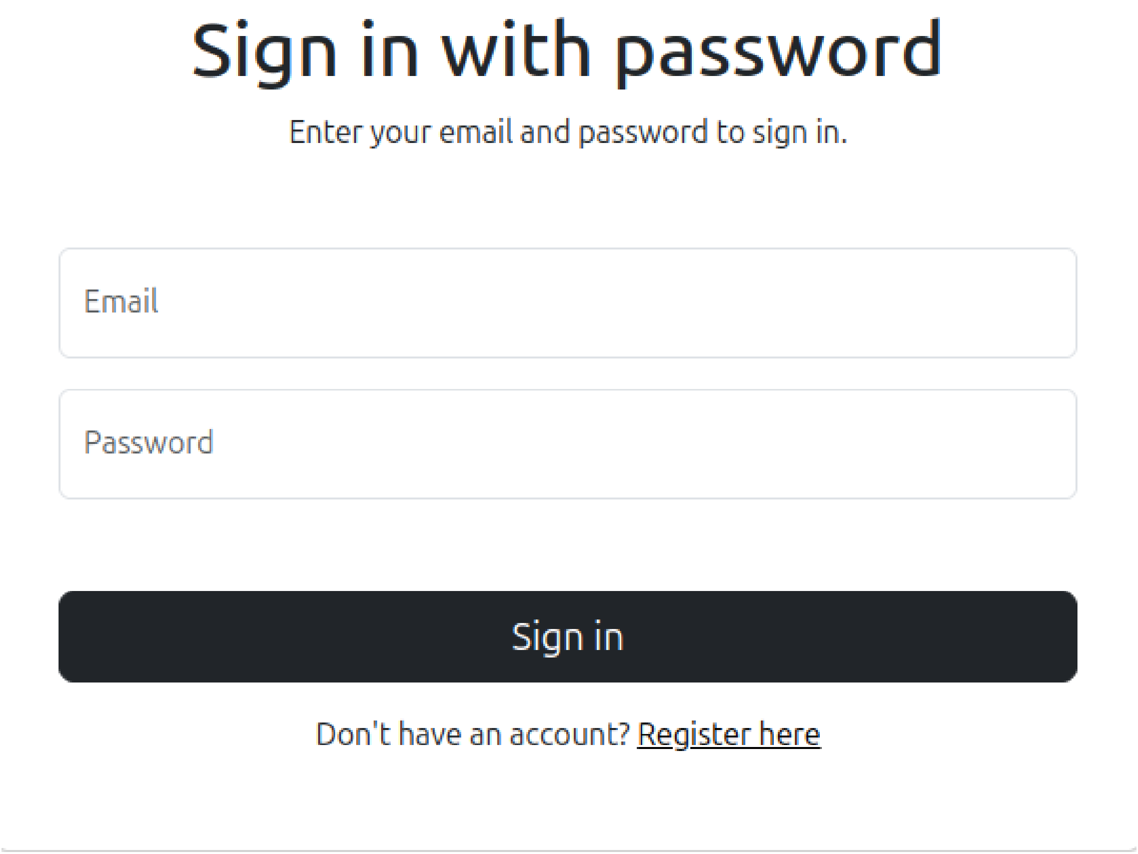
The second study was designed to gather qualitative data about users' experiences with both magic link and password-based authentication methods in a controlled environment. While Study 1 provided valuable statistical insights into users' perceptions and experiences with authentication methods in their workplace settings, Study 2 aimed to observe actual user behaviors and collect detailed feedback through practical testing of both authentication approaches.

This usability testing study directly addresses the research questions by allowing for observation of users' interactions with both authentication methods. For the first research question (RQ1) about the benefits and drawbacks of magic link authentication, the controlled testing environment allowed participants to try magic link authentication and provide specific feedback about its advantages and limitations. For the second research question (RQ2) concerning how magic link authentication compares to password-based authentication, the study allowed participants to compare the two methods using the same application and standardized tasks. By having participants complete identical authentication flows with both methods and then evaluate each experience using the System Usability Scale (SUS), usability metrics could be systematically compared while controlling for variables like interface design and task complexity. This helped identify specific differences in user experience between the two authentication methods.

5.1 Methodology

To gather qualitative data about user experiences with different authentication methods, a controlled usability testing procedure was designed and implemented. Usability testing is a method for evaluating user interfaces and interaction models by observing real users completing specific tasks. [29, 30] This approach allows researchers to identify usability issues and gather direct feedback from participants in a structured environment. For this study, a special demo application was developed with two distinct authentication flows to facilitate direct comparison between password-based and magic link authentication methods.

The first authentication flow implemented in the demo application was a traditional password-based system. In this flow, participants began by registering with their email address and receiving a confirmation email. Upon clicking the confirmation link, users were directed to a password selection screen where they were required to set a password with a minimum of eight characters to simulate real-world security requirements. After successful password creation, participants were logged into the application. Participants could then log out and log back in using their email address and password. This flow represented the conventional authentication experience familiar to most users. Figure 16 shows the login screen with password authentication.



Sign in with password

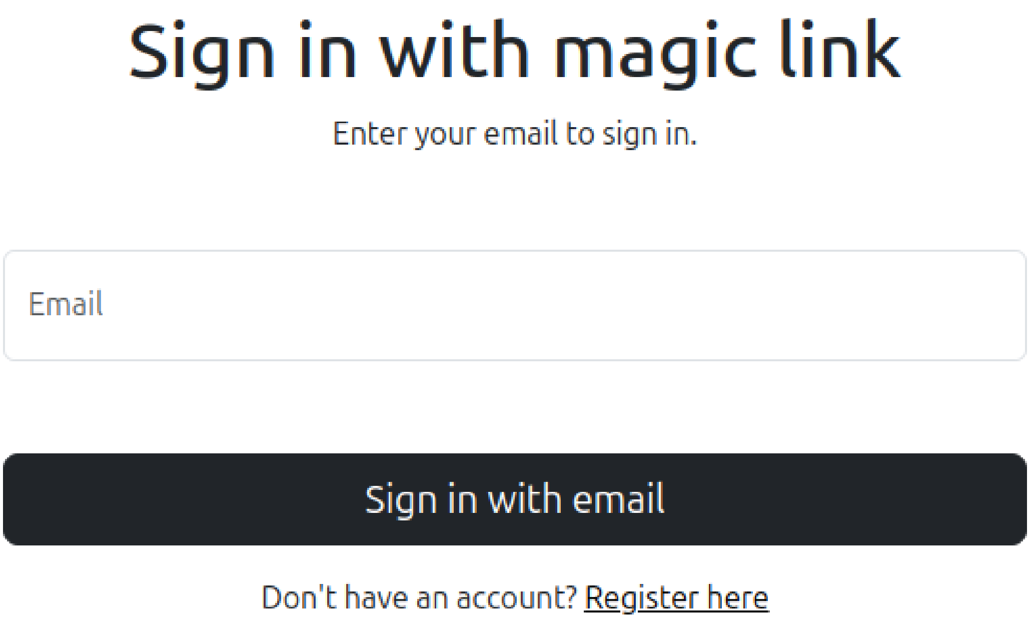
Enter your email and password to sign in.

Don't have an account? Register here

Figure 16. *Password sign-in page*

The second authentication flow implemented a passwordless magic link approach. Similar to the password flow, users began by registering with their email address and received a confirmation email. However, upon clicking the confirmation link, users were automatically logged into the application without the need to create or enter a password. For subsequent logins, users would enter their email address and receive a magic link via email. Clicking this link would authenticate them directly into the application without requiring password entry at any point in the process. Image of magic link authentication login screen can be see in Figure 17. Figure 18 shows the magic link email content.

A total of 10 participants were recruited for the usability tests from family members, friends, colleagues, and acquaintances of the researcher. This sample size aligns with J.



Sign in with magic link

Enter your email to sign in.

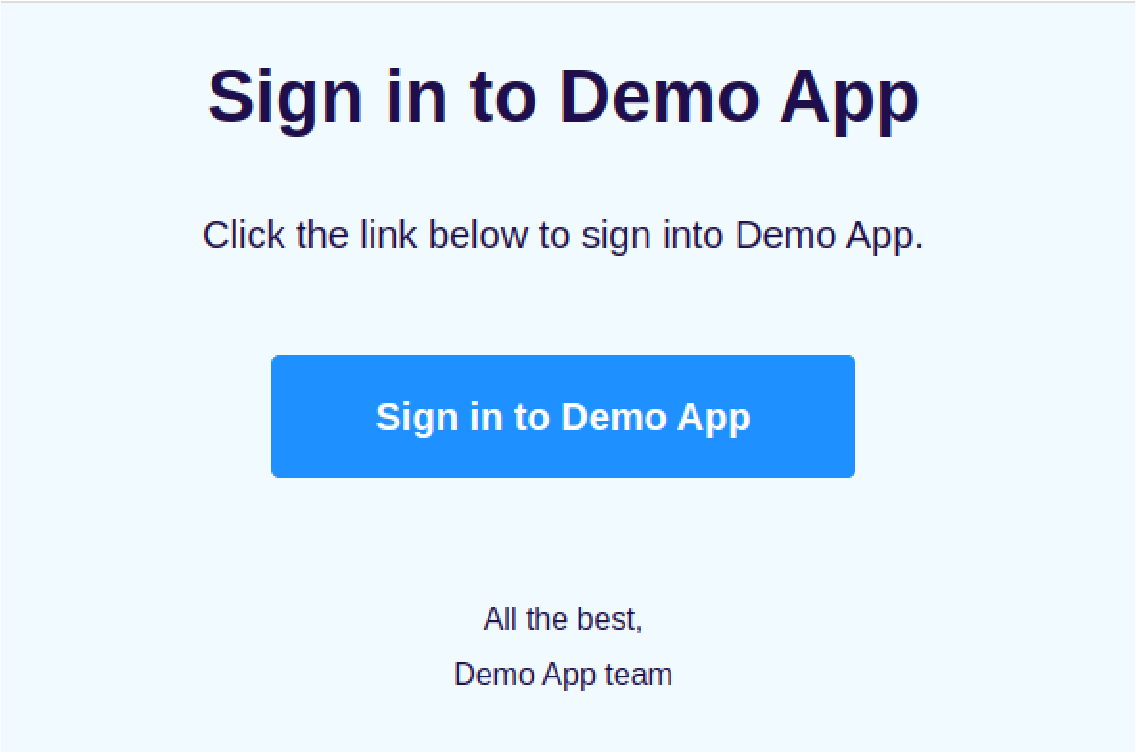
Don't have an account? Register here

Figure 17. *Magic link sign-in page*

Nielsen's research, which suggests that testing with just 5 participants will typically uncover approximately 85% of usability problems [31]. Participants were chosen from different age groups and professional backgrounds, with varying levels of technical expertise and familiarity with authentication systems. For more informative results it is important to have a diverse sample.

All usability tests were conducted in person, with the researcher present to guide participants through the process and observe their interactions. The demo application was hosted locally, and a controlled email environment was provided by the researcher to ensure all confirmation emails and magic links could be accessed without delivery problems. The testing procedure began with asking five questions about the participant's current authentication experiences, preferences and use of work-related SaaS software applications. Participants then completed authentication tasks using both flows in random order. After both authentication flows, participants filled a System Usability Scale (SUS) questionnaire. System Usability Scale is a standardized method for measuring perceived usability. [32, 33] It consists of ten statements that are given a score from 1 to 5, based on how much participant agrees with the given statement. Full list of SUS statements is seen in Appendix 4 - System Usability Scale. Following both authentication experiences, participants answered three additional questions comparing their experiences with both methods.

After the tests were completed, all data was collected to Google Sheets for analysis.



Sign in to Demo App

Click the link below to sign into Demo App.

All the best,
Demo App team

Figure 18. *Magic link email content*

To analyze the qualitative data gathered from participant interviews and observations, a thematic analysis approach was employed. [34] The process involved first familiarizing with the data by reviewing all interview responses. Next, initial codes were generated by identifying meaningful segments of text related to usability, security perceptions, and user preferences. These codes were then collated into potential themes that represented common patterns across participants' responses. The themes were subsequently reviewed and refined to ensure they accurately represented the data and addressed the research questions.

During usability testing sessions, observation methods were used to document participants' interactions with both authentication methods. The researcher was present throughout each session, taking notes on participants' behaviors, hesitations, comments, and non-verbal cues as they completed the authentication tasks. This direct observation approach helped identify usability patterns that might not emerge through interview responses alone. [31] There are potential limitations of this approach, including the possibility that researcher presence might influence participant behavior, causing them to act more carefully than they would in natural settings. Additionally, the researcher's prior knowledge of authentication systems might introduce interpretation bias when analyzing these observations. While these observations were not subjected to formal validation through specific follow-up questions, they provided contextual information that complemented the qualitative data collected through the usability testing sessions.

5.1.1 Ethics

In conducting this usability testing study, ethical considerations were prioritized to ensure participant privacy and comfort. All testing sessions were conducted with the participants' informed consent, with clear explanation that they could withdraw at any time without consequences. During the observation of authentication behaviors, care was taken to respect participants' privacy, particularly when they were entering passwords. All created accounts and passwords were fictional and used solely for testing purposes, with no connection to participants' actual online accounts. The controlled testing environment ensured that no potentially sensitive information was exposed during the study.

5.2 Results

The usability testing was conducted with 10 participants who completed authentication tasks using both magic link and password-based methods. This chapter presents the testing results in detail, examining participants' backgrounds and software usage habits, System Usability Scale scores for both authentication methods, stated preferences between the methods, security perceptions, qualitative feedback, and observations of user behavior during the testing sessions.

5.2.1 Participants Background

Before the tests, participants were asked about their job title, SaaS software usage habits and preferred authentication method for work-related applications. Full questions and answers can be seen in Appendix 3 - Usability Testing Questions And Answers. Out of the 10 participants, only 2 have a technical IT related job. These were software engineer and IT administrator. Working in the field of IT may change usability and security perceptions because of the technical knowledge about how authentication systems work. For this reason it was important that portion of participants working in the IT field was not too large. Other jobs titles included lawyer, financial auditor, customer support trainee, logistics coordinator, growth hacker, product manager, CEO and fashion designer.

Participants are regularly using multiple SaaS web applications for work purposes as seen in Figure 19. Over half of the respondents regularly use 6-10 software applications during a typical week, 3 respondents use 3-5 applications and only 1 respondent uses 1-2 different applications. The high number of different software applications used for work purpose highlights the growing popularity of SaaS software. Using password authentication for large number of applications comes with cognitive burden of remembering unique, secure passwords for each platform. This can lead to password reuse and therefore decreased security.

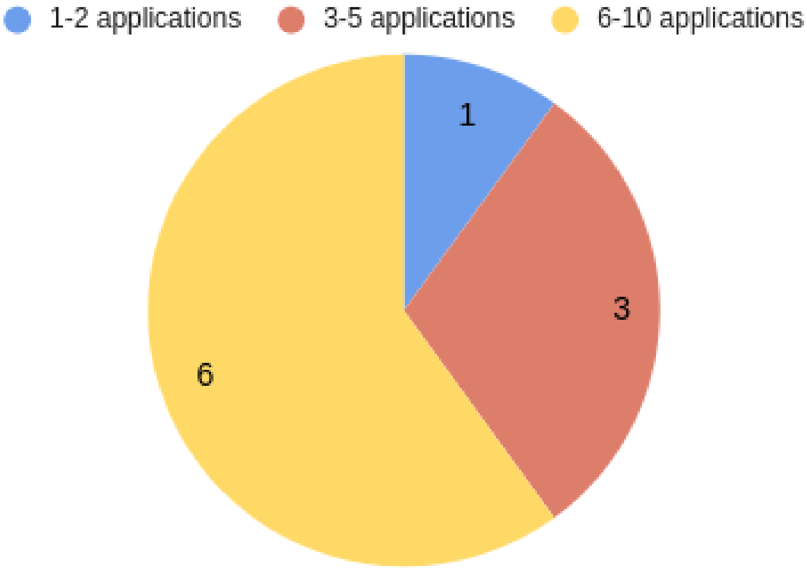


Figure 19. *Number of applications used in a typical week*

Another important indicator for the need of usable authentication methods is the number of times users have to authenticate in software applications during a day (Figure 20). Half of the participants regularly have to authenticate multiple times a day in different applications. 3 participants go through the authentication flow once a day and only 2 participants authenticate approximately once a week. Frequency of authenticating largely depends how often users session is timed out in different web applications and also whether users log out after each use or not. In the context of usability testing, frequent authentication habits can lead to higher standards for usability as any friction will have larger impact on daily productivity.

Although half of the participants authenticate in various software applications multiple times a day, magic link authentication is not a popular option (Figure 21). Out of 10 participants, half of them do not use magic link authentication at all, 1 participant uses magic links multiple times a day, 2 participants use it once a week and 2 participants use it less frequently than once a week. Previous experience can play a role in usability perceptions for an authenticating system. This variation in participant familiarity with magic links — ranging from regular users to those with no prior exposure — provides methodological strength to the study by ensuring a more representative assessment of the authentication method.

Lastly, participants were asked their preferred authentication method prior to the usability testing. As seen in Figure 22, most popular choice is passwords with 4 answers. 3

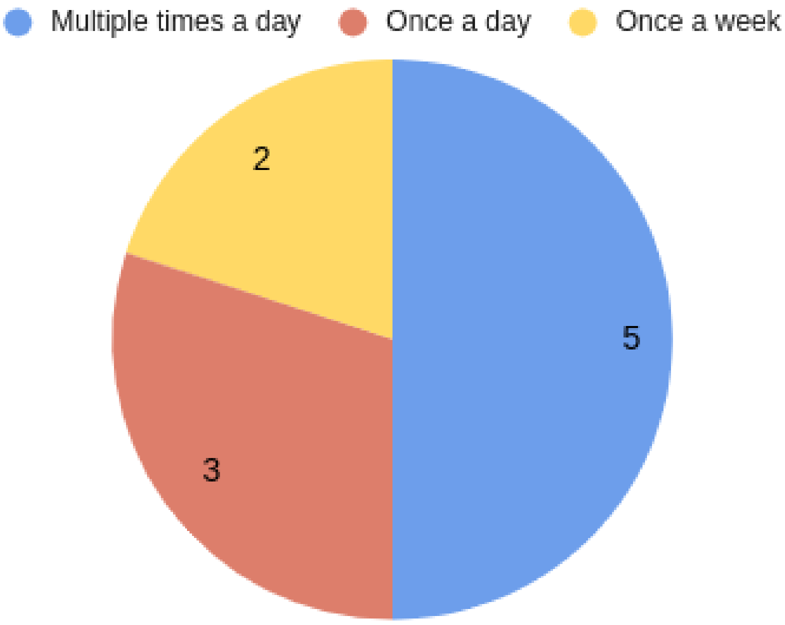


Figure 20. *Frequency of authenticating*

participants prefer two-factor authentication, 1 participant chose sign-in code via email and 1 participant chose social login. Notably, magic link authentication did not receive any votes as a preferred method. The preference for password-based authentication aligns with current trends is SaaS software applications where passwords remain the dominant authentication mechanism. The strong preference for passwords likely reflects users' familiarity and comfort with this method, which could present challenges for the adoption of alternative authentication approaches like magic links. The significant number of participants (3 out of 10) who selected two-factor authentication as their preferred method is particularly noteworthy, especially considering that 2FA typically involves additional steps and potential friction in the login process. This preference suggests that a portion of usability testing participants are willing to trade some convenience for increased security.

The data collected in the pre-testing phase of the usability study demonstrates that the participants have diverse work backgrounds with different authentication and software usage habits. This ensures that usability testing covers broad range of user experiences, preferences and perceptions. Enterprise SaaS software users represent a varied population in terms of technical literacy, comfort with new technologies, and understanding of security principles. For that reason it is important that usability testing also covers different types of end-users.

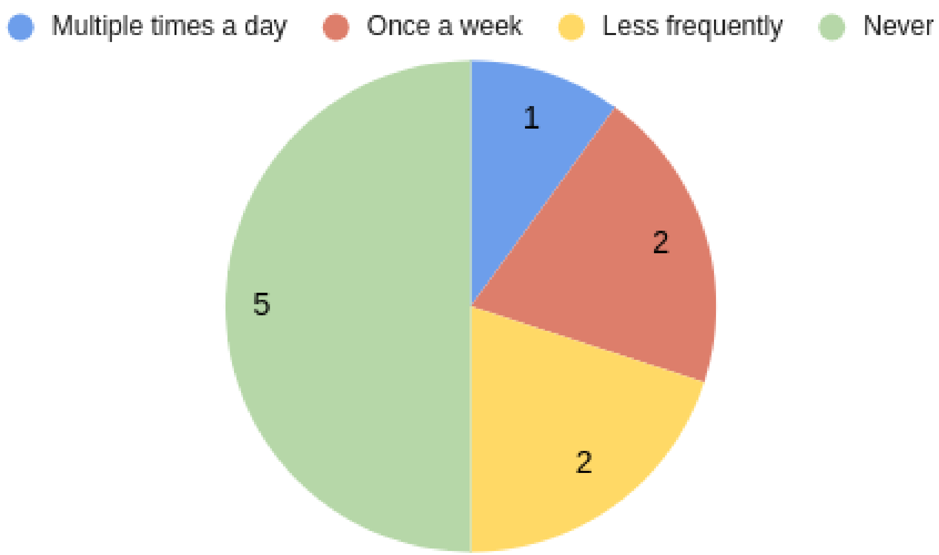


Figure 21. *Frequency of authenticating with magic links*

5.2.2 System Usability Scales

Both authentication methods were evaluated using the System Usability Scale (SUS). The SUS provides a reliable measure of perceived usability, with scores ranging from 0 to 100. This method converts raw scores into a standardized metric that allows for comparison between different systems and interfaces. In the context of this research, SUS provides an objective usability comparison between password-based and magic link authentication. The total score is calculated using the formula below. [35]

- X = Sum of the points for all odd-numbered statements - 5
- Y = 25 - Sum of the points for all even-numbered statements
- SUS Score = (X + Y) * 2,5

The System Usability Scale assessment revealed excellent usability scores for both authentication methods, with password authentication (Table 6) achieving an average score of 88 compared to 85 for magic link authentication (Table 7). Average score for System Usability Scale is considered 68 and everything above 80 is considered excellent. [36] This shows that users found both authentication methods easy to use and neither one have significant usability barriers for adoption by end-users. Scores for password authentication range from 80 to 97.5 and for magic links range from 72.5 to 95.

High SUS scores were expected as both authentication methods are widely used and have refined usability over time. The study deliberately implemented both flows according to industry best practices, with interfaces designed to match users' expectations from their

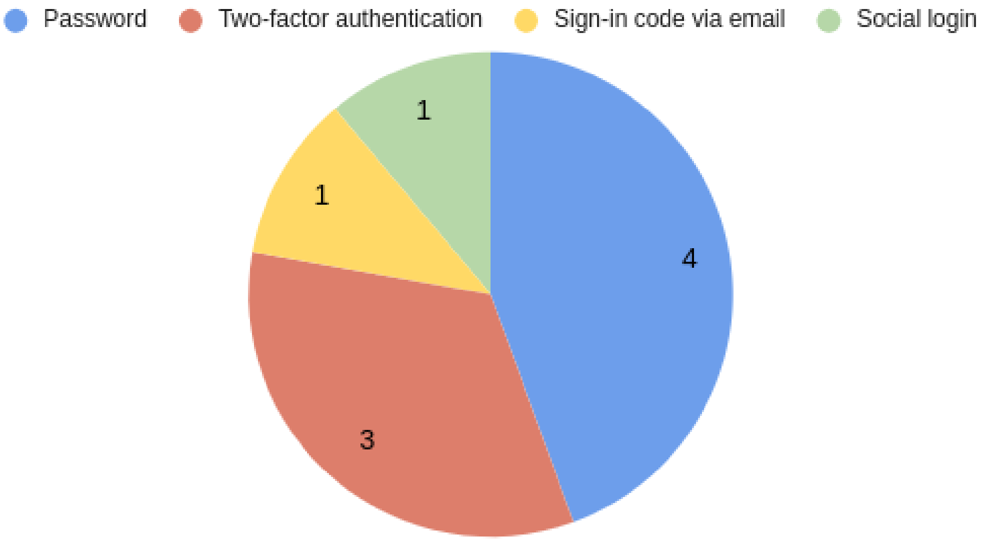


Figure 22. *Preferred authentication method*

daily interactions with enterprise SaaS applications. Participants encountered interfaces that aligned with their mental models of how authentication processes should function, regardless of which method they were evaluating.

The slight difference in System Usability Scale average scores indicates that end-users find passwords to have marginally better usability compared to magic links. One of the most important factors contributing to this preference is participants' greater familiarity with password-based authentication, which makes this flow seem more intuitive to them. As revealed in the pre-test interviews, half of the participants reported not using magic link authentication at all in their work-related applications, further explaining this familiarity gap.

Table 6. *Password usability scale*

Statement	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**
I think that I would like to use this system frequently.	4	5	3	5	4	4	3	5	4	5
I found the system unnecessarily complex.	1	1	1	2	1	2	1	2	1	1
I thought the system was easy to use.	4	5	5	4	5	4	5	4	5	4
I think that I would need the support of a technical person to be able to use this system.	1	1	1	1	1	1	1	2	1	1

Continues...

Table 6 – *Continues...*

I found the various functions in this system were well integrated.	5	4	2	5	5	5	2	5	4	4
I thought there was too much inconsistency in this system.	2	1	1	2	1	1	1	1	1	1
I would imagine that most people would learn to use this system very quickly.	4	4	5	5	5	4	3	5	5	4
I found the system very cumbersome to use.	2	2	1	2	1	2	1	2	2	1
I felt very confident using the system.	4	5	3	4	5	5	4	4	5	4
I needed to learn a lot of things before I could get going with this system.	1	1	1	1	1	1	1	2	1	1
SUS score	**85**	**92.5**	**82.5**	**87.5**	**97.5**	**87.5**	**80**	**85**	**92.5**	**90**

When looking at statements individually, the biggest average point differential (0.4) was for statement "I would imagine that most people would learn to use this system very quickly". Passwords received an average score of 4.4 for this statement while magic links received 4 points on average. Differential indicates that magic links seem to have steeper learning curve for participants, despite their simpler interaction model that eliminates password creation and memorization. This perception gap highlights a potential adoption challenge for magic link authentication in SaaS software applications, where perceived ease of learning can influence organizational acceptance of new technologies.

There were 3 statements that had a 0.3 average point differential - "I think that I would need the support of a technical person to be able to use this system", "I found the system very cumbersome to use" and "I needed to learn a lot of things before I could get going with this system". For all these statements password-based authentication had higher average score. These small but consistent differences across multiple usability dimensions point to a meaningful perception gap between the two methods. Participants perceived magic links as more technically complex, demanding and with a steeper learning curve. The novelty of magic links, despite their simpler interaction model, creates a perception of increased complexity and technical requirements. This highlights the importance of considering not just objective usability metrics but also subjective user perceptions when implementing new authentication technologies in SaaS software solutions, where user acceptance is important for successful adoption.

All other statements had marginal 0.1 average point differential or no differential at all. Notably, the statement "I thought the system was easy to use" received a 0.1 higher average score for magic links compared to passwords. This slight difference suggests that once users become familiar with magic link authentication, they find it marginally easier to use than password-based systems. This finding aligns with the objective interaction model of magic links, which eliminates the cognitive burden of password management.

Table 7. *Magic links usability scale*

Statement	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**
I think that I would like to use this system frequently.	5	5	3	4	5	4	3	4	5	4
I found the system unnecessarily complex.	1	1	1	2	1	2	1	2	1	1
I thought the system was easy to use.	5	5	5	5	5	4	4	4	4	5
I think that I would need the support of a technical person to be able to use this system.	3	1	1	1	1	1	1	2	2	1
I found the various functions in this system were well integrated.	5	4	3	4	5	4	3	4	5	5
I thought there was too much inconsistency in this system.	1	2	1	1	1	1	1	2	1	1
I would imagine that most people would learn to use this system very quickly.	4	3	3	5	5	4	3	5	4	4
I found the system very cumbersome to use.	2	1	3	1	1	3	2	1	3	2
I felt very confident using the system.	4	5	5	4	3	5	3	5	4	4
I needed to learn a lot of things before I could get going with this system.	2	1	1	1	1	1	2	2	2	1
SUS score	**85**	**90**	**80**	**90**	**95**	**82.5**	**72.5**	**82.5**	**82.5**	**90**

An important factor to consider when measuring usability is the end-users' technical background. Two participants with technical IT-related jobs had different average scores in multiple categories for magic link authentication than participants with non-IT jobs. The biggest difference (1.4 points) was for the statement "I found the system very cumbersome to use." IT people viewed magic links as easier to use, which is expected because they are more familiar with the authentication method and also know how it works from the technical side. The statement "I would imagine that most people would learn to use this system very quickly" also had a big score differential (0.6 points). Participants with technical backgrounds were more pessimistic in users' ability to get used to magic link authentication. This may indicate their work experience with the authentication method and reflect problems they have faced in user acceptance.

5.2.3 Authentication Method Preferences

After the usability testing, participants were asked questions regarding their preferences between the two authentication methods. The first question was about which authentication method they preferred. Exactly half of the participants chose passwords while the other half chose magic link authentication as their preferred method. The main reasons for choosing magic links were improved security and the absence of password management. For passwords, participants pointed out that switching between two windows was too troublesome, and because of this inconvenience, password-based authentication was preferred. One participant noted that passwords are the preferred method for logging in, but magic links are preferred for registering an account in a new system. The reason is that with magic links there are fewer fields to fill out, as choosing a password is not needed.

Two participants who chose magic links as their preferred method after the usability testing had previously selected passwords as their preferred authentication method before the test. Both participants also did not use magic links regularly in SaaS software applications. Their reasons included that "magic link was quicker and easier to use since there is no need to type a long password every time" and "magic link felt somehow more secure and easier." This indicates that magic links offer usability benefits that are valuable for end-users. However, it is also important to note that the usability testing was conducted in a controlled environment where email deliveries did not have delays and had a 100% success rate. These conditions may have influenced the usability perception for users who had not used magic links before.

5.2.4 Security Perceptions

When asked about which method felt more secure, 8 out of 10 participants identified magic links as the more secure option, while only 2 participants perceived passwords as more secure. Even though most participants used passwords more regularly in their daily work, they still viewed magic links as the more secure option.

Several participants provided reasoning for their security perceptions. One participant highlighted the vulnerability created by password reuse, noting that magic links eliminated this risk by removing the need to save passwords across multiple websites. Another participant specifically mentioned that magic links would be more secure when combined with two-factor authentication on their email account, demonstrating an understanding of how multiple security layers work together. A third participant recognized that magic links require access to their email account, which serves as an additional security barrier. These responses indicate that participants have a good conceptual understanding of the security model behind magic link authentication.

The two participants who perceived passwords as more secure primarily expressed concern about email account vulnerabilities. One participant specifically stated that "passwords are more secure, because email account can be hacked." This highlights a key consideration in magic link authentication - the security of the authentication method is directly tied to the security of the user's email account. However, it goes the same way with passwords. Most popular way for password reset in SaaS software web applications is that secure link is provided via email. [23] This means passwords also depend on the security of email account. For participants this was something they did not think about.

5.2.5 Qualitative Feedback

As a last interview question, participants were asked to provide qualitative feedback for both authentication methods, describing the main advantages and disadvantages. Answers given by the participants are shown in Table 8.

Main advantages pointed out for passwords were quickness and ease of use. Password managers and browser auto fill features play a big role in that. Users do not have to input anything when input fields are filled automatically and can sign in with only one click. This makes passwords an attractive choice. For magic links, it was considered a disadvantage that logging in takes longer as it usually requires more clicks. Also, participants found window switching between the application and email client to be disruptive. The need for switching between different windows creates additional friction in the authentication process that isn't present in the password method.

Table 8. *Magic links and passwords qualitative feedback*

Passwords	**Magic links**
Passwords are quicker when using password manager and passwords are autofilled.	Magic links take longer to log in but offer better security.
Logging in with a password may be beneficial in situations where you don't have immediate access to your email account.	I think magic link is definitely a faster way to log in, also easier.
Hassle free, but can be forgotten/leaked.	Do not have to remember passwords. Losing access to email account means no login options.
Password method is smoother.	Magic link does not require to handle yet another password but relies on mailbox security.
Con: you have to remember your passwords.	More clicks to do, but feels more secure.
Pros: faster, browser autofill, do not have to open the email with every login. Cons: logging in from other devices without autofill requires me to remember the password, and I often need to use the "Forgot password" feature in those cases.	Pros: faster and simpler sign up, can never forget a password, do not have to share my commonly used password with the provider. Cons: anything related to email deliverability, speed etc. Logging in takes more time due to having to also open the email software.
Easier to use.	Takes longer to log in.
Passwords work well with password managers.	Magic links are better when I have a lot of accounts.
Faster to use, brute force attacks are a con when using weak passwords.	More clicks and need to open separate window but no password management.
Easy to use.	Once I had email delivery issue and could not log in. Otherwise no password management is a plus.

Password management was highlighted as an advantage for magic links, as end-users do not have the cognitive burden to remember their passwords. One participant brought out that magic links are especially beneficial when user has a high number of different accounts. Another participant specifically mentioned that there is no need to worry about forgotten passwords or go through password reset procedures when using magic links. Cognitive burden was the main disadvantage pointed out for password-based authentication systems.

5.2.6 User Behavior Observations

During the usability testing, observations were made regarding how participants interacted with both authentication methods. Overall, both authentication methods demonstrated good usability with minimal points of confusion. Participants were able to complete the authentication tasks without any difficulty, regardless of which method they were using.

One notable observation was the cautious behavior displayed by participants when interacting with magic link emails. Participants took time to carefully read the email content before clicking on the sign-in link. This behavior likely comes from increased awareness of phishing scams that often disguise as some sort of authentication emails. Several participants specifically mentioned checking the link URL before proceeding. Additionally, half of the participants reported not using magic links regularly in their work applications, which contributed to their careful approach. These users specifically looked for clear instructions within the email and proceeded more carefully through the authentication flow compared to those familiar with magic links. This observation highlights the importance of clear, trustworthy design for magic link emails to help users distinguish legitimate authentication requests from potential security threats.

Another thing to note is that many participants had trouble remembering the passwords they had set during the registration phase when attempting to log in again later in the testing session. This observation aligns with the cognitive burden associated with password-based authentication described in the interview answers by multiple participants. Interestingly, these challenges occurred even within the short time frame of the usability testing session, suggesting that in real-world scenarios where users might return to applications after longer periods, the problem could be significantly worse.

5.3 Discussion

This usability testing study examined how users interact with both magic link and password-based authentication in a controlled environment, focusing on the two research questions that guided this thesis.

The first research question (RQ1) asked: "What are the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software?" The usability testing revealed several clear advantages of magic links. Most notably, participants appreciated not having to manage passwords, with one participant explicitly stating that magic links are "better when I have a lot of accounts," highlighting the value in enterprise environments where users manage numerous SaaS applications. This aligns with theoretical benefits suggested by Chowhan et al. [26] and Chaudhari et al. [22], who emphasized reduced cognitive burden as a key advantage.

However, the usability testing also revealed practical drawbacks of magic links. Multiple participants mentioned that authentication was more time-consuming due to the need to switch between application and email client. As one participant noted, it "takes longer to log in" because of "more clicks and need to open separate window." This finding suggests that the theoretical time efficiency benefits of magic links described in literature might not translate to actual user experience, especially when compared with modern password systems supported by auto-fill features.

Security perceptions from the usability testing offered mixed results. While 8 out of 10 participants identified magic links as more secure than passwords, their explanations showed varying levels of understanding. Some correctly identified that magic links eliminate risks associated with password reuse, with one participant noting that magic links "do not require to handle yet another password but rely on mailbox security." However, others expressed misconceptions, with two participants believing passwords were more secure because "email account can be hacked," not recognizing that password reset mechanisms typically depend on email security as well. This knowledge gap suggests that the security advantages of magic links described by Matiushin et al. [24] might not be fully understood by end-users without additional education.

The usability testing study provided substantial evidence to address RQ1, revealing both the benefits and drawbacks of magic link authentication for enterprise SaaS applications. The primary benefit identified was the elimination of password management, with participants explicitly appreciating this feature when managing multiple accounts. However, the study uncovered real-world challenges that weren't highlighted in the literature, especially how users found switching between application and email windows disruptive to their workflow.

The second research question explored: "How does magic link authentication compare to password-based authentication in web applications from an end-users perspective?" The System Usability Scale provided a standardized comparison, with both methods scoring well above the average (88 for passwords versus 85 for magic links). While both scores fall in the "excellent" usability range, the slight advantage for passwords contradicts the literature's suggestion that magic links offer better overall usability.

The authentication preference results showed an even split, with exactly half of participants preferring each method after testing. This balanced preference contradicts the pre-test situation where none of the participants selected magic links as their preferred authentication method. Two participants who initially preferred passwords changed their preference to magic links after direct experience, suggesting that practical exposure might overcome initial hesitations about unfamiliar authentication methods.

Qualitative feedback revealed distinct patterns in how users evaluate the two methods. For passwords, speed and convenience were the predominant advantages mentioned, particularly when used with modern tools: "Passwords work well with password managers." For magic links, security benefits and the absence of password management were the main advantages, with participants appreciating not having to remember passwords. This trade-off between convenience and security management represents a key consideration for SaaS providers designing authentication systems.

User observations during testing showed that participants had difficulty remembering passwords they had just created, even within the short time frame of the testing session. This observation offers tangible evidence of the cognitive burden associated with password-based systems that was theoretically described in the literature. Conversely, participants showed notably cautious behavior when interacting with magic link emails, carefully reading content and checking URLs before clicking. This observation aligns with Maqbali et al.'s [23] research on email-based password recovery. Their study emphasized that well-designed emails with clear instructions, personalization, matching sender details, and appropriate contact information are essential for building user trust in email-based authentication.

The differences between the findings and previous research likely comes from three main factors. First, the evolution of password management tools has reduced the friction associated with password-based authentication, a development not fully considered in earlier theoretical analyses. Second, the controlled testing environment eliminated email delivery issues that might affect real-world magic link experiences. Third, the varying levels of user familiarity with each authentication method influenced perceptions, with magic links being less familiar to most participants.

Regarding RQ2, the usability testing effectively answered how magic link authentication compares to password-based methods from an end-user perspective. Through direct comparison in controlled conditions, this study revealed that contrary to theoretical predictions, magic links don't necessarily provide superior usability to passwords in practice. The findings highlight how modern password management tools have improved the user experience of traditional authentication, creating a more nuanced reality than what previous research has suggested.

5.3.1 Limitations

This study acknowledges several methodological limitations that should be considered. First, technical considerations were excluded from the scope, including implementation complexity and technical security assessments of magic link authentication. This means that the study focuses only on user perceptions rather than technical feasibility or technical security. Second, usability testing was performed in a controlled environment that could not replicate the various external factors present in normal workplace settings. External factors, such as time constraints, stress, interruptions, or multi-tasking, could change the perception of usability and security for different authentication options. Third, the testing environment ensured perfect email deliverability for magic links, which does not reflect real-world challenges. Magic link emails may be delayed, filtered by corporate security policies, blocked as potential phishing attempts and be inaccessible due to email account restrictions or connectivity issues. Fourth, the sample size and demographic distribution may not fully represent the diverse range of enterprise SaaS users across different industries, technical proficiency levels, and organizational sizes. This limits how the findings of this study could be used for generalization. Additionally, as usability tests were conducted in person with researcher being present, participants may have biased opinions regarding authentication method preferences.

5.4 Conclusion

This study utilized a qualitative usability testing methodology to examine users' experiences with both magic link and password-based authentication in a controlled environment. The testing was conducted with 10 participants from different professional backgrounds who completed authentication tasks with both methods and provided feedback through System Usability Scale assessments. Results showed both authentication methods achieved excellent usability scores, with passwords (88) scoring slightly higher than magic links (85). Participant preferences were evenly split between the two methods, with 50% preferring each option. The findings highlighted a fundamental trade-off in how users evaluate authentication methods: passwords were valued for speed and convenience, particularly when used with modern tools like password managers and auto-fill features, while magic links were appreciated for eliminating password management and perceived security benefits. Observations revealed participants struggled with remembering passwords even during short testing sessions but displayed cautious behavior when interacting with magic link emails. These qualitative insights complement the survey findings by providing in-depth understanding of the usability factors influencing authentication preferences.

6. General Discussion

This thesis addressed two research questions: (RQ1) "What are the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software?" and (RQ2) "How does magic link authentication compare to password-based authentication in web applications from an end-users perspective?". Through a systematic literature review and mixed-methods approach combining both quantitative survey data and qualitative usability testing, this study has developed a comprehensive understanding of how enterprise users perceive and interact with magic link authentication.

The findings reveal a significant gap between the theoretical benefits of magic link authentication suggested in academic literature and the practical experiences of users in enterprise environments. This difference provides important insights for SaaS providers considering the implementation of magic link authentication solutions.

The first research question (RQ1) asked: "What are the potential benefits and drawbacks of magic link authentication for organizations using cloud-based SaaS software?" Both the SLR and empirical research identified the elimination of password management as the primary benefit of magic link authentication. [22, 26, 8] The survey showed that 84.3% of respondents considered this the main advantage, while usability testing participants specifically mentioned relief from the cognitive burden of remembering multiple complex passwords. One participant explicitly stated that magic links are "better when I have a lot of accounts," highlighting the particular value of this benefit in enterprise contexts where users must manage numerous SaaS applications. The regression analysis (Table 4) provided statistical confirmation, showing that perceived simplicity ($\beta = 0.499, p < 0.001$) was the strongest predictor of preference for magic links, with almost twice the impact of security considerations.

However, the empirical research revealed practical implementation challenges that were not emphasized in the theoretical literature. Email delivery issues emerged as the most significant drawback, with 85.3% of survey respondents identifying this as a problem. This finding suggests that the real-world reliability of magic links may be considerably lower than academic literature indicates. While researchers like Parmar et al. [8] did mention email deliverability as a potential issue, the survey suggests this problem is far more widespread and impactful than previously documented.

Time efficiency presents another area where empirical findings contradict theoretical benefits. Half of the survey respondents disagreed that magic links save them time compared to passwords, and usability testing participants frequently mentioned the disruption of switching between application and email client. This perception contrasts with 41.2% of survey respondents who identified "faster login process" as a benefit, suggesting that the experience varies considerably depending on context. The evolution of password management tools (with auto-fill capabilities) has significantly improved the efficiency of password-based authentication in ways not fully considered in earlier theoretical analyses [22, 8]. Interestingly, while many users perceived magic links as slower, 41.2% of survey respondents still identified "faster login process" as a benefit. This apparent contradiction can be explained by several factors: varying email delivery efficiency, inconsistent baseline comparisons (manual password entry versus password managers), and individual workflow preferences. ANOVA analysis (Table 5) showed no significant differences in perceptions across job categories for most variables, suggesting that these contradictions between theory and practice exist regardless of professional background.

Security perceptions revealed a complex picture with important implications for implementation. While 8 out of 10 usability testing participants perceived magic links as more secure than passwords, the survey revealed that 44.1% of respondents did not understand how magic links protect their accounts. Almost half (45.1%) of survey respondents remained neutral when asked about magic link security, indicating widespread uncertainty. This knowledge gap represents a critical barrier to adoption that was not adequately addressed in the literature. As Ruoti et al. [17] found in their empirical study, users value transparency in authentication systems, and the lack of understanding about how magic links work likely contributes to hesitation in using this technology.

Based on the findings from both studies, RQ1 has been largely answered, providing clear identification of both the benefits (primarily password management elimination and perceived security improvements) and drawbacks (email delivery issues, time inefficiency concerns, and lack of understanding about security mechanisms) of magic link authentication in enterprise environments. The research particularly highlights the gap between theoretical benefits and practical challenges faced by actual users.

The second research question explored: "How does magic link authentication compare to password-based authentication in web applications from an end-users perspective?" The System Usability Scale assessment provided a standardized comparison between the two authentication methods, with both scoring well above the average usability threshold (88 for passwords versus 85 for magic links). While this difference is marginal, it contradicts the literature's suggestion that magic links provide better overall usability. This finding aligns with the survey results, where slightly more respondents (37.3%) preferred password-based authentication over magic links (27.5%). The regression analysis ($R^2 = 0.583$) revealed that perceived simplicity of login process ($\beta = 0.499$), security ($\beta = 0.296$), and time efficiency ($\beta = 0.228$) were significant predictors of preference for magic links, while reliability for business applications and understanding security mechanisms were not significant factors. This statistical evidence indicates that users' preference for authentication methods is primarily driven by perceived ease of use and security rather than technical understanding or perceived reliability.

The survey findings revealed that enterprise users typically employ multiple authentication methods simultaneously, with respondents using an average of 3.6 different methods. While passwords remain nearly universal (used by 95% of respondents), magic links have achieved moderate adoption (38%) in workplace environments, indicating that SaaS software providers are supplementing rather than replacing traditional authentication systems with newer methods. This moderate adoption rate of magic links (38%) is consistent with Matiushin et al.'s [24] observation that major companies have begun implementing this technology, though it suggests a more gradual transition than theoretical literature might imply.

An important finding from the usability testing was the even split in authentication preferences after participants experienced both methods, with exactly 50% preferring each approach. This balanced preference contrasts sharply with the pre-test situation where none of the participants selected magic links as their preferred authentication method. The shift in preference for two participants who initially preferred passwords but changed to magic links after testing suggests that direct exposure can overcome initial hesitations about unfamiliar authentication methods. This finding has important implications for SaaS providers, indicating that user education and guided experiences with magic links could potentially improve adoption rates.

The qualitative aspects of the usability testing revealed distinct evaluation patterns for each method. For passwords, speed and convenience were consistently mentioned as advantages, particularly when used with modern tools like password managers and browser auto-fill features. For magic links, security benefits and freedom from password management were the primary advantages. This suggests a fundamental trade-off that users consider when evaluating authentication methods: convenience versus security management. This trade-off aligns with findings from Ukwandu et al. [25], who found that users preferred One-Time Passcodes (OTP) via email, which function similarly to magic links, specifically for actions requiring enhanced security such as payment transactions.

User behavior observations during testing provided evidence of the cognitive burden associated with password-based systems that was theoretically described in the literature [26, 22]. Participants had difficulty remembering passwords they had just created, even within the short time frame of the testing session. On the other hand, the cautious behavior participants displayed when interacting with magic link emails (carefully reading content and checking URLs) highlights the importance of email design in building trust, aligning with Maqbali et al.'s [23] findings on email-based authentication, which showed that well-designed emails with clear instructions, personalization, matching sender details, and appropriate contact information are essential for establishing user confidence in email-based authentication systems.

The findings presented throughout this study comprehensively answer RQ2, revealing that from an end-user's perspective, magic link authentication compares similarly but not superiorly to password-based authentication in terms of overall usability. Both methods present distinct advantages and drawbacks that users weigh differently based on their individual priorities, with the ultimate preference being nearly evenly split in controlled testing conditions. The research particularly highlights how modern password management tools have improved the user experience of password-based authentication, challenging earlier theoretical assumptions about the comparative benefits of magic links.

6.1 Security Considerations

While this thesis focused primarily on usability aspects, it's important to address the security-usability trade-off inherent in authentication methods. Magic link authentication shifts the threat model away from password-related vulnerabilities toward email security concerns, creating different security challenges than traditional authentication. Despite their theoretical security benefits, password-based systems face significant practical limitations in enterprise environments. Studies have shown that users often create weak, easily guessable passwords or reuse credentials across multiple services when faced with password management burdens. [1, 2] While password managers with randomly generated passwords offer strong protection, their adoption in enterprise environments remains inconsistent, with many SaaS users relying on memorized passwords that inherently have lower security entropy. [37]

When comparing magic link authentication with alternative methods, several security considerations emerge. Multi-factor authentication (MFA) provides stronger protection than either passwords or magic links alone by requiring multiple verification components. [38] However, the additional steps required for MFA can create friction in the authentication process, potentially affecting user experience and productivity in enterprise environments where employees authenticate multiple times daily. [38]

Hardware tokens and biometric solutions offer robust security profiles but introduce different challenges. Hardware tokens require physical possession and infrastructure investment, while biometric authentication raises privacy concerns and credential revocation challenges. [8] Magic links sit between these options, offering improved security over basic passwords without the implementation complexity of hardware-based solutions.

The security of magic link authentication ultimately depends on the security of the underlying email system. [26] In enterprise environments, where email accounts typically have organizational security policies including forced password changes and potential 2FA requirements [12], this dependency may offer adequate protection for many SaaS applications. However, for high-security operations, additional authentication factors would likely be necessary regardless of whether passwords or magic links form the primary authentication method.

6.2 Limitations

This research has several limitations that should be considered when interpreting the findings. First, the usability testing was conducted in a controlled environment that did not fully represent real-world authentication scenarios. In the testing environment, magic link emails were delivered instantly with 100% reliability, which is not always the case in actual workplace settings. Email delivery in enterprise environments can be affected by network issues, security filters, and corporate email policies that might delay or block authentication emails. Additionally, external factors such as time pressure, distractions, and multitasking that are common in workplace environments were absent from the controlled testing conditions, potentially influencing usability perceptions.

Second, researcher presence during the usability testing sessions may have influenced participants' behaviors and responses, potentially causing them to act more carefully than in natural settings or provide biased feedback to meet perceived expectations. As the sole researcher conducting both observations and thematic analysis, interpretations of user behaviors could have been influenced by existing knowledge of authentication systems, potentially emphasizing patterns that aligned with expectations rather than representing unbiased observations.

Third, technical implementation details were excluded from the scope of this research, with focus being solely on end-user perceptions. However, technical considerations such as implementation complexity and security vulnerabilities are critical factors that SaaS software providers must consider when choosing authentication methods. While magic links might be perceived as secure by end-users, the actual security depends on technical implementation details.

Fourth, the sample size of the study presents limitations for generalization. While the survey collected 102 responses, which provided valuable quantitative insights, the usability testing was limited to 10 participants. Although this sample size aligns with Nielsen's research suggesting that 5 participants can identify approximately 85% of usability issues [31], it may not fully capture different perspectives and experiences of enterprise SaaS users across various industries, technical proficiency levels, and organizational contexts.

Finally, the systematic literature review had two significant limitations that should be acknowledged. Only two out of nine papers provided empirical evidence through user testing, with the majority presenting theoretical analyses without practical validation. In addition, the existing literature lacked differentiation between user groups and usage contexts. It was particularly relevant for this research, which focused specifically on enterprise SaaS end-users.

6.3 Future Work

For SaaS providers implementing magic link authentication, several practical recommendations emerge from this research. First, addressing email deliverability is critical, as this was identified as the most significant drawback for magic links. Email delivery reliability needs to be carefully considered during implementation, with mechanisms to handle potential delivery failures. Second, user education about how magic links work and their security benefits could help overcome the knowledge gap identified in this research. Third, developers should consider the workflow disruption caused by switching between application and email client, as this negatively impacts users' perception of time efficiency compared to password-based authentication with auto-fill capabilities.

Building on this research, future studies could expand the scope to compare magic link authentication with other passwordless alternatives such as biometric authentication, hardware tokens, and single sign-on solutions in enterprise environments. Such comparative studies would provide SaaS software providers with a more comprehensive understanding of the strengths and limitations of various authentication options for web applications. Additionally, examining how these different passwordless methods address the email delivery and time efficiency challenges identified with magic links would be particularly valuable for improving authentication solutions.

Future research would also benefit from conducting usability testing with larger and more diverse samples across different industries, organizational sizes, and technical proficiency levels. A larger-scale study could investigate how perceptions of authentication methods vary among different user groups and identify potential patterns based on demographic or professional factors.

7. Conclusion

This research investigated magic link authentication as an alternative to password-based authentication in enterprise-level SaaS software applications. A mixed methods approach was used, combining a quantitative survey with 102 respondents and qualitative usability testing with 10 participants. This methodology provided both statistical insights into user perceptions and in-depth understanding of the authentication experience. The findings show a clear gap between what academic literature suggests about magic links and how they work in real-world situations. While magic links do offer benefits by removing the need to manage passwords and potentially improving security, several practical problems were found in both the survey and usability testing. Email delivery problems were the biggest issue, with 85.3% of survey respondents mentioning this as a drawback. Users also had concerns about the time it takes to use magic links, as they found switching between the application and email client disrupted their workflow, especially when compared to password managers that can fill in credentials automatically.

The research also revealed that many users don't understand how magic link security works. Even though 8 out of 10 usability testing participants thought magic links were more secure than passwords, 44.1% of survey respondents said they didn't understand how magic links actually protect their accounts. The System Usability Scale results showed that both authentication methods had good usability, with password authentication scoring slightly higher (88) than magic links (85). This is different from what was found in the systematic literature review, which suggested that magic links would provide better overall usability. To make magic links work better in SaaS software applications, developers should focus on making email delivery more reliable, helping users understand the security aspects, and making the authentication process faster to address efficiency concerns.

References

[1] Cormac Herley, P. C. Van Oorschot, and Andrew S. Patrick. “Passwords: If We’re So Smart, Why Are We Still Using Them?” In: *Financial Cryptography and Data Security*. Ed. by Roger Dingledine and Philippe Golle. Vol. 5628. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 230–237. ISBN: 978-3-642-03548-7 978-3-642-03549-4. DOI: 10.1007/978-3-642-03549-4_14. URL: http://link.springer.com/10.1007/978-3-642-03549-4_14 (visited on 09/27/2024).

[2] Kirit Sælensminde and Veera Boonjing. “A Simple Password Less Authentication System for Web Sites”. In: *2010 Seventh International Conference on Information Technology: New Generations*. 2010, pp. 132–137. DOI: 10.1109/ITNG.2010.154.

[3] Joanna Krysińska. *Biggest data breaches of 2024*. Dec. 17, 2024. URL: https://nordlayer.com/blog/data-breaches-in-2024/ (visited on 04/18/2025).

[4] StrongDM Team. *Ticketmaster Data Breach: What Happened and How to Prevent It*. Feb. 28, 2025. URL: https://www.strongdm.com/what-is/ticketmaster-data-breach (visited on 04/18/2025).

[5] Reuters. *UnitedHealth says hack at tech unit impacted 190 million people*. Jan. 25, 2025. URL: https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-confirms-190-million-americans-affected-by-hack-tech-unit-2025-01-24/ (visited on 04/18/2025).

[6] Alanna Titterington. *UnitedHealth ransomware attack*. Feb. 20, 2025. URL: https://www.kaspersky.com/blog/unitedhealth-ransomware-attack/53065/ (visited on 05/16/2025).

[7] Chidiebere Obulose and Peter Chinedu Agu. “The Future of Passwordless Authentication: Trends, Predictions, and Emerging Technologies”. In: *Predictions, and Emerging Technologies* ().

[8] Viral Parmar et al. “A Comprehensive Study on Passwordless Authentication”. In: *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. 2022, pp. 1266–1275. DOI: 10.1109/ICSCDS53736.2022.9760934.

[9] Aratek. *What Is Passwordless Authentication and Why Biometrics Is Key?* Feb. 21, 2024. URL: https://www.aratek.co/news/what-is-passwordless-authentication-and-why-biometrics-is-key (visited on 12/15/2024).

[10] Christian Peeters et al. "SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication". In: *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*. ASIA CCS '22. Nagasaki, Japan: Association for Computing Machinery, 2022, pp. 2–16. ISBN: 9781450391405. DOI: 10.1145/3488932.3497756. URL: https://doi.org/10.1145/3488932.3497756.

[11] Aranza Trevino. *Magic Links: What They Are and How They Work*. Mar. 7, 2024. URL: https://www.keepersecurity.com/blog/2024/03/07/magic-links-what-they-are-and-how-they-work/ (visited on 11/02/2024).

[12] Gilad David Maayan. *User Management in the Enterprise: Technologies and Best Practices*. May 21, 2024. URL: https://www.computer.org/publications/tech-news/trends/enterprise-user-management (visited on 05/13/2025).

[13] Deepak Gupta. *Mastering Magic Link Security: A Deep Dive for Developers*. June 5, 2024. URL: https://guptadeepak.com/mastering-magic-link-security-a-deep-dive-for-developers (visited on 11/02/2024).

[14] Wendy Braethen. *The Security Vulnerabilities in Magic Links Authentication*. Dec. 16, 2022. URL: https://vaultvision.com/blog/the-security-vulnerabilities-in-magic-links-authentication (visited on 11/02/2024).

[15] Steffi Haag and Andreas Eckhardt. "Shadow IT". In: *Business & Information Systems Engineering* 59.6 (Dec. 1, 2017), pp. 469–473. ISSN: 1867-0202. DOI: 10.1007/s12599-017-0497-x. URL: https://doi.org/10.1007/s12599-017-0497-x.

[16] Andreas Kopper. "Perceptions of IT managers on shadow IT". In: (2017).

[17] Scott Ruoti, Brent Roberts, and Kent Seamons. "Authentication Melee: A Usability Analysis of Seven Web Authentication Systems". In: *Proceedings of the 24th International Conference on World Wide Web*. WWW '15. Florence, Italy: International World Wide Web Conferences Steering Committee, 2015, pp. 916–926. ISBN: 9781450334693. DOI: 10.1145/2736277.2741683. URL: https://doi.org/10.1145/2736277.2741683.

[18] Daniel Taylor. “What’s the Password? Account Sharing in the Context of Passwordless Authentication”. MA thesis. Daniel Taylor, 2023.

[19] PRISMA. *Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Guidelines*. `https://www.prisma-statement.org`. Accessed: 01.09.2024.

[20] Rafael Sarkis-Onofre, Ferrán Catalá-López, and Edoardo Aromataris. “How to properly use the PRISMA Statement”. In: *Systematic Reviews* 10 (Dec. 2021). DOI: `10.1186/s13643-021-01671-z`.

[21] Zotero. *Zotero reference management Software*. `https://www.zotero.org`. Accessed: 13.09.2024.

[22] Anagha Chaudhari et al. “A Comprehensive Study on Authentication Systems”. In: *2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*. 2023, pp. 1–5. DOI: `10.1109/ICCUBEA58933.2023.10392029`.

[23] Fatma Al Maqbali and Chris J Mitchell. “Email-based Password Recovery - Risking or Rescuing Users?” In: *2018 International Carnahan Conference on Security Technology (ICCST)*. 2018, pp. 1–5. DOI: `10.1109/CCST.2018.8585576`.

[24] I Matiushin and V Korkhov. “Passwordless Authentication Using Magic Link Technology”. In: *CEUR Workshop Proceedings*. Vol. 3041. 2021, pp. 434–438.

[25] Elochukwu Ukwandu and Alexis Bennett. *Exploring the Views of End-Users on Passwordless Authentication Methods*. 2023. DOI: `10.2139/ssrn.4616393`. URL: `https://www.ssrn.com/abstract=4616393` (visited on 09/27/2024).

[26] Rahul Chowhan and Rohit Tanwar. “Password-Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites”. In: Jan. 2019, pp. 190–212. ISBN: 9781522581017. DOI: `10.4018/978-1-5225-8100-0.ch008`.

[27] Vani Agrawal et al. “Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behaviour Authentication”. In: *SSRN Electronic Journal* (2019). ISSN: 1556-5068. DOI: `10.2139/ssrn.3360306`. URL: `https://www.ssrn.com/abstract=3360306` (visited on 09/27/2024).

[28] The JASP Team. *JASP Statistical Software*. https://jasp-stats.org/. Accessed: 18.04.2025.

[29] Muhammad Junaid Aamir and Arshad Mansoor. “Testing Web Application from usability perspective”. In: *2013 3rd IEEE International Conference on Computer, Control and Communication (IC4)*. 2013, pp. 1–7. DOI: `10.1109/IC4.2013.6653765`.

[30] J.M. Christian Bastien. "Usability testing: a review of some methodological and technical aspects of the method". In: *International Journal of Medical Informatics* 79.4 (2010). Human Factors Engineering for Healthcare Applications Special Issue, e18–e23. ISSN: 1386-5056. DOI: https://doi.org/10.1016/j.ijmedinf.2008.12.004. URL: https://www.sciencedirect.com/science/article/pii/S1386505608002098.

[31] Jakob Nielsen. *Why You Only Need to Test with 5 Users*. Mar. 18, 2000. URL: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/ (visited on 03/17/2025).

[32] James R. Lewis. "The System Usability Scale: Past, Present, and Future". In: *International Journal of Human–Computer Interaction* 34.7 (2018), pp. 577–590. DOI: 10.1080/10447318.2018.1455307. eprint: https://doi.org/10.1080/10447318.2018.1455307. URL: https://doi.org/10.1080/10447318.2018.1455307.

[33] Rebecca A. Grier et al. "The System Usability Scale: Beyond Standard Usability Testing". In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 57.1 (2013), pp. 187–191. DOI: 10.1177/1541931213571042. eprint: https://doi.org/10.1177/1541931213571042. URL: https://doi.org/10.1177/1541931213571042.

[34] Victoria Clarke and Virginia Braun and. "Thematic analysis". In: *The Journal of Positive Psychology* 12.3 (2017), pp. 297–298. DOI: 10.1080/17439760.2016.1262613. URL: https://doi.org/10.1080/17439760.2016.1262613.

[35] Will T. *Measuring and Interpreting System Usability Scale (SUS)*. URL: https://uiuxtrend.com/measuring-system-usability-scale-sus/ (visited on 03/23/2025).

[36] Aaron Bangor, Philip Kortum, and James Miller. "Determining what individual SUS scores mean: adding an adjective rating scale". In: *J. Usability Studies* 4.3 (May 2009), pp. 114–123.

[37] Sarah Pearman et al. "Why people (don't) use password managers effectively". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 319–338. ISBN: 978-1-939133-05-2. URL: https://www.usenix.org/conference/soups2019/presentation/pearman.

[38] Aleksandr Ometov et al. "Multi-Factor Authentication: A Survey". In: *Cryptography* 2.1 (2018). ISSN: 2410-387X. DOI: 10.3390/cryptography2010001. URL: https://www.mdpi.com/2410-387X/2/1/1.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Jaan Erik Lepp

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Magic Link Authentication for Enterprise-Level SaaS Software Users”, supervised by Ricardo G. Lugo
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons’ intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

18.05.2025

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student’s Aapplication for restriction on access to the graduation thesis that has been signed by the school’s dean, except in case of the university’s right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - Questionnaire

Hi! My name is Jaan Erik Lepp and I am researching magic link authentication for my Master's thesis at Tallinn University of Technology. Magic links are passwordless authentication mechanisms where users receive a sign-in link via email instead of entering traditional passwords. This research investigates the usability and security perceptions of magic link authentication in Software-as-a-Service (SaaS) web applications. The focus is on business software used for work purposes, such as Pipedrive, GitHub, Jira, ChatGPT, Slack and other similar tools. All responses are anonymous and will be used for academic research purposes only. The questionnaire takes approximately 5 minutes to complete. Thank you for participating in this research!

1. What is your current job title?

2. Which types of work-related web applications do you regularly use? (Select all that apply)
   a. Customer Relationship Management (CRM)
   b. Project Management
   c. Communication/Collaboration Tools
   d. Financial/Accounting Software
   e. Development Tools
   f. Human Resources Management
   g. Business Intelligence/Analytics
   h. AI Assistants
   i. Other:

3. How many different work-related web applications do you use in a typical week?
   a. 0
   b. 1-2
   c. 3-5
   d. 6-10
   e. More than 10

4. How often do you have to authenticate (sign in) to work-related web applications?
   a. Multiple times per day
   b. Once a day
   c. Several times per week
   d. Weekly

   e. Less frequently

5. Which authentication methods do you currently use for work-related web applications? (Select all that apply)
   a. Traditional passwords
   b. Single Sign-On (SSO)
   c. Two-factor authentication (2FA)
   d. Magic links (sign-in link via email)
   e. Biometric authentication
   f. One-time code (via email or SMS)
   g. Other:

6. How often do you use magic link authentication (sign-in link via email)?
   a. Multiple times per day
   b. Once daily
   c. Several times per week
   d. Once a week
   e. Less frequently
   f. Never

7. Rate your agreement with the following statements about magic link authentication (strongly disagree, disagree, neutral, agree, strongly agree)
   a. Magic links simplify my login process.
   b. Magic links save me time compared to passwords.
   c. Magic links are secure.
   d. Magic links are reliable for business applications.
   e. I understand how magic links protect my account.
   f. I prefer magic links to password-based authentication.

8. What benefits have you experienced with magic link authentication? (Select all that apply)
   a. Faster login process
   b. No password management
   c. Improved security
   d. Better user experience
   e. Fewer login issues
   f. Other:

9. What challenges have you faced with magic link authentication? (Select all that apply)
   a. Email delivery issues

b. Link expiration issues

c. Device switching problems

d. Email access issues

e. Difficult to use

f. Other:

Appendix 3 - Usability Testing Questions And Answers

Before Test

1. What is your current job title?

Financial auditor
Lawyer
Software engineer
Customer support trainee
Logistics coordinator
Growth hacker
Product manager
CEO
IT administrator
Designer

2. How many different work-related web applications do you use in a typical week?

6-10
3
10
5
7
10
3-4
7-10
5-6
2

3. How often do you have to authenticate (sign in) to work-related web applications?

2-3 times per day
Once a day
Some, almost never, others every few days.
Once a day
3-4 times a day
5 times per day
Once a week
Multiple times a day
Couple of times a day
Once a week

4. How often do you use magic link authentication (sign-in link via email)?

Couple of times a month
Never
Never
Once per week
Never
3 times per day
Never
Once a week
Once a month
Never

5. What is your preferred authentication method when using web applications for work?

Two-factor for security reasons
Passwords
Password + Authenticator app
Username, password with 2FA
Password
Social account login (Google)
Passwords
MFA with authenticator app
Sign in code
Passwords

After Test

1. Which authentication method did you prefer? Why?

Magic links, because I do not have to remember passwords and it offers a more secure way to log in.
I like both methods, but magic link was quicker and easier to use since you don't have to type your long password every single time you log in.
Password. Less hassle, didn't have to leave the page.
I prefer user name and password because I don't need to switch windows (go out of context) and password managers together with fingerprint readers have made this login method very convenient.
Magic link, as it felt somehow more secure, also easier.
For logging in, I prefer password authentication because I can save the password to my browser's keychain and don't need to leave the website. Email can arrive instantly, or take minutes in some cases - it's inconsistent and can be slow. For signing up, I prefer the magic link authentication because I have to fill in less fields.
Passwords, because I do not want to open email.
Magic link seemed better and secure.
Magic link because I do not want to remember passwords.
Passwords - easier to use.

2. Which authentication method felt more secure for you?

Magic links are more secure to me.
Magic links
Magic link
Magic link (if my email had 2FA)
Magic link, as it felt somehow more secure, also easier
I think the magic link authentication is more secure because I often reuse passwords and it's one less website I will have to save my password to.
Passwords
Magic link because requires access to my email
Magic links
Passwords, because email account can be hacked

3. What are the pros and cons for both authentication methods?

   Answers to this question can be seen in Table 8 under Study 2 results.

Appendix 4 - System Usability Scale Questionnaire

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.