# Visions of the Future: What Could Happen to User Authentication?

**Hanna Paananen and Naomi Woods**
University of Jyväskylä, Finland

hanna.k.paananen@jyu.fi
naomi.woods@jyu.fi

**Abstract:** The most prevalent information system security feature for the user is the authentication process. Passwords have been the primary authentication method for decades due to their simplicity for both the user and the system provider. However, over recent years, the digitalization of services has increased the number of credentials each user must manage, making traditional password authentication problematic for the user. Strong candidates for easier and more secure authentication methods are emerging (e.g., FIDO alliance, Single-sign-on, biometrics). Still, a single method has yet to dominate the market due to the rapid changes in technology, costs of implementation, trust in these methods, and the vast number of users and digital services. Due to the varied reasons that affect the adoption of these methods, it is unclear what kinds of authentication methods will be the forerunners in the future. This study aims to envision the future of user authentication and security features emerging from the interaction of different factors. We present a qualitative interview study, which examines six experts from the fields of authentication, cybersecurity, and emerging technologies. A hermeneutic mode of analysis is used to form scenarios of the future based on the observations of different experts. The results reflect an understanding of how users and their interactions with security features, such as authentication, may change over the following decade and beyond and how security professionals intend to incorporate this knowledge into future security systems. The results shed light on the influence of society, developing technology, and the need for user- and future-proof security in the coming years. This study will have several implications, as it will contribute to forming a coherent picture of the different elements that shape the future and give an idea of how to prepare for what is coming. Furthermore, it will provide an understanding of how choices with technology today lead to different futures.

**Keywords:** User Authentication, Future, Qualitative Study, Interview

## 1. Introduction

Today, digitalization creates a constant change in the world around us. We have several digital identities and user accounts in the systems to determine which services we can use. At the cusp of the digital and physical world is the act of user authentication, which the physical human does to prove their digital identity and gain access to their user accounts, systems, and devices. Today, 90% of users have over 90 online accounts (FIDO Alliance, 2024). As people use digital services more and more, so has the time spent on authentication increased, which may be one of the reasons they take shortcuts such as reusing passwords. At work, people spend, on average, over two days every two months on authentication-related activities (Bhana and Flowerday, 2020). This shows that while authentication is a critical security control, it comes with threats and inconveniences yet to be solved.

Within the bigger picture of digitalizing societies and transforming work-life, the security of systems and users' privacy are significant issues. Today, there are forces such as the changing threat environment, government regulation, business competition, emerging technologies, and user needs and values that shape the authentication landscape. As attackers create more professional operations and increasing political motivations alter the conception of what security-critical systems are, the legitimate users of the systems are required to use more robust authentication methods to ensure security. (Lella et al., 2023 p. 4, 140.)

This study is motivated by the idea that academia, as an impartial and independent institution, must produce knowledge supporting decision-making that shapes the future of secure digitalized societies. To understand this change better, we have set a research question: *how do experts view the future of user authentication and security in light of the major trends of digitalizing societies?*

This paper is structured as follows. First, we introduce authentication concepts and current issues. Then, we present the method and results of a qualitative interview study. Lastly, we discuss the implications of the study and propose further research.

## 2. Overview of User Authentication

Passwords and encryption tools have been used throughout the centuries within different contexts, from the Greeks to the Enigma machine in the Second World War, but mainly as a military tool to protect national secrets and strategies (Rathidevi et al., 2017; Yaschenko, 2002). When the first business mainframe computer systems

in the 1960s required limiting the access of users, passwords were a convenient choice since the input could be done easily through the keyboard (Bonneau et al., 2015; Ciampa, 2013).

Authentication methods are commonly categorized into three groups based on what characteristic they are assessing as proof of the user's identity (Grassi et al., 2017).

- *Something the user knows*: These include knowledge-based methods, e.g., passwords (text-based and graphical) (De Angeli et al., 2005; Stobert and Biddle, 2013), Personal Identification Numbers (PINs), and challenge-response methods (Haga and Zviran, 1991).
- *Something the user possesses*: This category refers to the authentication process using objects, such as a device or token, to prove the user's identity. The token may be a dedicated item that is used for authenticating (e.g., a USB key), or it may be a digital certificate on a mobile device (Al-Ameen et al., 2016; Butler and Butler, 2015).
- *Something the user is*: Biometrics are physical or behavioral characteristics of the user that are used to prove their identity. The most popular biometrics include fingerprint scanning and face recognition (Cho et al., 2020). Behavioral biometrics are also used, including keystroke dynamics, mouse movement, and gait. (Dasgupta et al., 2016).

Nowadays, authentication processes that just require a password are deemed insufficient and insecure (Aloul et al., 2009). Due to several factors, such as the increased number of digital services and their passwords, which are needed daily, users are managing their passwords insecurely (Woods and Siponen, 2024). Furthermore, in an attempt to improve security, password creation requirements imposed in online systems require users to meet a minimal level of security in the composition of their passwords; however, these rules do not consider the psychology of users nor the multitude of other passwords the user is required to have (Furnell et al., 2022; Grawemeyer and Johnson, 2011; Woods and Silvennoinen, 2023).

## 2.1 User Authentication Today

Lately, technological development has introduced new authentication solutions, which provide security yet still have drawbacks (Zhang et al., 2019). Therefore, multifactor authentication (MFA) methods, which require users to authenticate using multiple techniques, are becoming the preferred and most secure type of authentication (Ometov et al., 2019). One long-lived example is the chip and PIN combination used in credit cards (Weir et al., 2010).

Modern smartphones carry several means of authentication, such as fingerprint scanners, cameras for face recognition, and input for memory-based methods (Cho et al., 2020), as well as mobile connectivity for out-of-band authentication (Butler and Butler, 2015). As MFA requires extra effort from the user and could cause discontent, methods have been developed to reduce the effort in low-risk interactions. The system assesses and classifies the user's behavior, device information, and sensitivity of the assets they are accessing. More robust authentication is then only required in high-risk situations. (Bonneau et al., 2015; Butler and Butler, 2015.)

One way of reducing the constant authentication requests when using multiple services is the single-sign-on (SSO). Companies often have centralized identity management, which allows using SSO to open various systems and devices. For example, Facebook and Google have provided similar services in the consumer market. However, their adoption has been hindered by privacy concerns as these corporations could access login session information and use it for profiling. (Bonneau et al., 2015; Järpehult et al., 2022.)

## 2.2 The big Picture of Authentication

Because our economy is already largely dependent on digital services, the security of these services has become a societal issue. The European Union (EU) has enacted legislation that affects authentication. For example, the Second Payment Services Directive (PSD2) requires strong authentication in bank transactions, which has consolidated the MFA as a part of online services. Further, the General Data Protection Regulation (GDPR) requires that user account data must be stored safely, which can be seen as a requirement for secure authentication. (McDowell, 2019).

Online service providers are also moving towards providing SSO options for their users. Due to privacy-compromising security incidents (e.g., the Cambridge Analytica case), governments have started to pay attention to the amount of information shared between services, reducing the sharing of sensitive information. (Järpehult

et al., 2022.) There are standardization initiatives for authentication to balance the amount of credentials and privacy, such as FIDO authentication (FIDO Alliance, 2024) and OpenID Connect (OpenID Foundation, 2024).

## 3. Research Method

This research was conducted as a qualitative interview study. The interviews were semi-structured and followed the dramaturgical model put forth by Myers and Newman (2007). The interview started by asking about the work status of the informant, their current projects, and their influence in society. The main body of the interview was steered by a 10-year timeline and six themes: society, organizations, individuals, values, services, and technology. The themes were not forced into the conversation, and not all of them needed to be covered. The interviews were conducted face-to-face or through online video conferencing in English or Finnish. Within the results section, these experts will be identified as participants A-F. The researchers interpreted the data using the hermeneutic circle by moving from the details of the data to forming an understanding of a larger vision of the anticipated changes in the future (Klein and Myers, 1999).

The research data consists of six interviews with experts from cybersecurity and emerging technologies. All informants currently work in European research institutions in a senior researcher position, each with over a decade of experience in their respective fields. The participants influence society by teaching, conducting research, publishing in both academic journals and mainstream media, participating in international professional associations and standardizing work, and giving talks and recommendations to industry and political decision-makers.

## 4. Results

The views of the experts are presented here under the interview themes, although the conversations did not follow this template. The ideas from the discussions are here merged into more general ideas of the current state and future of user authentication and cybersecurity.

### 4.1 Individuals

Authentication is a required step for a user to enter digital services, but authenticating is rarely the ultimate goal of people's actions. This is why the security-usability trade-off is often discussed as the balance of securing information while avoiding inconveniencing the user. Unfortunately, we see services coming to market emphasizing user convenience, and security is not added until breaches occur. However, these two are not the opposite ends of one line but two axes in a matrix. A preferable future scenario would be to find solutions where both usability and security are high.

> *"I realized that the whole practice of authentication was old fashioned [...] it was stuck in the past. [...] You have to use all these strong passwords, and there was never any acknowledgment that these are humans, not robots." Expert E*

Currently, there are many emerging authentication methods, but passwords are still widely used in many online services. People may use several services and devices daily, each with different authentication requirements. We see that online consumer services provide alternative authentication methods, but this may not be the case with enterprise systems, which often have higher security requirements. When looking forward to a decade from now, these same issues may still exist if the development mirrors the previous decade. The password mechanism may still be widely used and allow short, easily guessable passwords. As smartphones have become ubiquitous, the alternatives that most likely could replace passwords require a personal device. This may introduce new types of threats since, e.g., if malicious actors become interested in breaching the device, the user's biometric data may become useless as an authentication method for the rest of their lives.

> *"The password [could] literally become the poor man's version of security because [...] they don't have the devices with them that support other things." Expert E*

A smart mobile device that holds the key to digital identity can also be a way of moving away from personal computers. As services and data are increasingly moving to the cloud, it reduces the need to design workstations as personal devices. This may give way to new ways of working when the authentication or user-related sensors and control interfaces are on the mobile device. On the other hand, device-dependent authentication can pose threats not only to security but also to the users' ability to function in a digitalized society. When devices are

used as tokens or biometric sensors, replacing them may be troublesome as there does not seem to be viable fallback methods beyond passwords.

### 4.2 Organizations

Before, organizations were the ones that adopted new technologies first, and the consumer versions would come along later. Now, the tide is turning, especially after the COVID-19 pandemic, which brought forward the trend of people mixing work and personal tasks using their online services and devices. They may share files on personal cloud drives with friends and colleagues and read their work emails on personal phones. This has brought forward the need to adapt the user security features to be flexible enough to handle bring-your-own-device (BYOD) situations and the use of various services. This motivates a move away from passwords and towards more secure authentication methods. However, emerging is a new issue of whose device is used in device-dependent authentication. As users may not want multiple devices, organizations may have to choose between allowing personal use of company phones or applying strong authentication methods that do not require a smartphone. The third option would require using personal smartphones, but governments and labor unions may oppose this for invading privacy and liability in security concerns.

> *"Wow, because they thought they could put their big feet into my people's personal phones, and people said no. So this is the other thing that you see is organizations thinking they can get security for free." Expert F*

### 4.3 Values, Norms, and Control

Earlier, the internet might have been a playground for free information and equal opportunities for participation. As technology has advanced and become more complex, the resources required to enter the market may not be available for small players. This development seems to be continuing with corporations trying to gain more power over users. This serves the values of the technology providers and raises the question of the rights over people's digital identities and their right to security. The user experience and security with different devices can improve if standardizing supports the building of ecosystems where technologies from various manufacturers work together and reduce the number of user authentication requests. In the future, users are either tied to a single platform or can jump from one platform to another seamlessly. The future seems to depend on the government's ability to control the market and create an environment where technology companies are willing to participate in standardization. Furthermore, in these alternative futures, the power over people's digital identities is either held by the heads of the corporations or by the political decision-makers.

> *"We are seeing that single technological players and through that, certain individuals have a tremendous amount of power over what the digital environment is like. [...] Furthermore, there are different countries that follow various justice systems and fundamental ideologies about human values and that type of social system. […] I can't see that the original utopia of the open network would be coming true in the near future." -Expert B*

Using biometrics is seen as a viable way to create secure and convenient authentication methods. However, the value of the biometric and digital identity may become higher as society digitalizes. We are already seeing value conflicts in this situation. If facial recognition is connected to security cameras, it may lead to people being misidentified and blamed for crimes they did not commit. Furthermore, people may lose control over their own digital identity if their features change due to, e.g., an illness. These examples show that the development of authentication methods may hold significant value conflicts. In the future, we may see crimes and lawsuits that radically change how we accept using our physical features in the digital world.

### 4.4 Services

One thing that may significantly reduce the number of authentication requests and user accounts is the forming of even bigger platforms. We are already seeing large corporations (e.g., Google, Amazon, Alibaba) adding new services that can be accessed through the platform credentials, and this development may continue to expand to new service types in different areas of life.

Organizations that provide digital services do so with varying capabilities and values. For example, small and medium-sized enterprises (SMEs) may not have adequate resources available for evaluating the usability and security of their selected authentication methods. Especially services where the commercial value of each credential is low may continue to use insecure password mechanisms since replacing them would be expensive.

New authentication innovations may overtake the market when large online service corporations adopt them. When these methods are targeted for the masses, they are designed to be convenient and fun to use.

### 4.5 Technology

Quantum computing (QC) is currently getting much attention since many countries and large organizations are investing significantly in it. The field is still quite scattered, with many different technologies being developed, and some practical issues, such as noisiness or cooling requirements, are still unsolved. However, the technology is already in a state where information processing and transmission have been successful. This has evoked threat scenarios where QC is used to breach current encryption methods. The standardization and preparation for quantum-resistant encryption have already started. Within a decade, this type of encryption should be easy to implement and in place in the most critical systems. However, the same timeline applies to developing quantum computers that could break the current cryptography, meaning that information that is encrypted and stolen today may be exploited in the future.

Blockchain is another emerging technology that has had many hopes for improved security attached to it. However, while there are many domains where an uncentralized source of trust and security might be useful, the application of blockchain technology may not be the answer. It might be a good technology for digital identities, but its immutability might go against privacy and the inevitable occurrence of human errors.

> *"To me, [blockchain] seems like a dud. [...] There have been cryptocurrencies that cybercriminals can use to blackmail people easily. To me, it was a disappointment." -Expert B*

Artificial intelligence (AI) is also a hot topic due to ChatGPT gaining popularity. There is much speculation about AI changing digital processes and services, but security concerns exist. Not only can it be used to help create more sophisticated attacks, but if the AI breaks, it may turn into a new kind of insider threat. This spurs the need for a novel control: not only humans authenticating to use systems but AI authenticating to humans. There is an increasing need to make sure that we are not dealing with AI that is designed to push misinformation or hallucinations.

The Internet of Things (IoT) is becoming a part of our daily lives as more devices are connected to networks. As new IoT devices and sensors are added to smart homes, cities, and factories, the security landscape becomes more complex. This also requires that the interaction with authentication methods becomes more natural. For example, in a smart home, the verbal commands to operate devices should be seamlessly limited only to authorized users to counter meddling from mischievous neighbors. The security of these devices must be improved simultaneously with convenience since, without secure connectivity and encryption, IoT devices could be used increasingly to cause real-life harm.

### 4.6 Society

With the rise of new technologies and the importance of cybersecurity to personal and national security, governments have started to implement more regulations in the market. In the EU, there are many new directives in preparation for controlling both the management of cybersecurity and the design of secure products. However, it is difficult to foresee how they may affect society and if they ultimately cause more good than harm. Overreactions are possible, especially if the decision-makers do not understand technology well enough.

As advanced technologies are becoming available to organizations and consumers, there are those who are not able to enjoy their benefits. The digital divide may deepen and leave some people behind. Issues such as personal finances, language processing, and education impact what devices and services, and as an extension, authentication methods, are accessible. As the population in European countries is aging, democratic processes may push for more inclusivity. However, this requires innovations that lower the burden of configuring the personal user experience and incentives to the technology providers to offer adaptable options. Governments may, however, be unable to support the creation of these innovations as one of the driving forces behind digitalization is saving money on services.

## 5. Discussion

User authentication has evolved from a single password needed at work to something that ensures the security of our digital identities in different walks of life. While exciting things await the future, the current situation is complex and scattered, making predicting difficult. The experts identified several issues in the current state of authentication and cybersecurity that would need to be addressed going forward. The main themes repeated in the interviews were the fragmentation of the authentication method landscape, people having multiple roles, and emerging technologies.

Currently, we are seeing a move away from the traditional password mechanism. The smartphone is a central part of the emerging methods as it has biometric sensors and can be used as a token, but this has introduced more complexity to authentication. There are many initiatives, such as laws and standards, that promote SSO and MFA to add security to the authentication process (FIDO Alliance, 2024; Järpehult et al., 2022). However, several solutions are emerging and creating another problem. Before, the user had to remember passwords for potentially dozens of accounts, but now they must install several apps on their phones to gain access to services. Different actors must take the initiative to fight further fragmentation. Consumers must choose authentication methods that reduce the number of credentials. Service providers must adhere to standards to diminish the authentication overload. Lastly, governments must acknowledge that cybersecurity threats may also emerge from an overly heterogeneous system landscape and steer service providers away from burdening users with security and from creating excessive unmanageable complexity.

Authentication plays a different role depending on whether we are employees, citizens, or consumers. While previously we separated the roles for privacy, the COVID-19 pandemic set in motion a change in attitudes. The use of devices and systems for both work and home tasks became necessary during the pandemic and has been common ever since. This creates a dilemma of whose rules are adhered to with cybersecurity. The use of the smartphone for authentication seems logical from the security perspective but does not fix the problem of multiple roles. More seamless authentication experiences would require changing the conventions of organizational authentication policies, flexibility from governmental bodies, and willingness from the consumer service providers to invest in methods that can be used across the board. Furthermore, device-reliant authentication would need to be designed in a way that does not cause stress or conflicts.

Emerging new technologies promise profound changes in the digital world. Generative AI is transforming digital content creation. IoT is bridging the gap between concrete and digital. Quantum computing makes it possible to solve formerly “unsolvable” problems. As things from sci-fi movies become a reality, we are reminded of these stories' dystopias. The more reliant we become on technology, the more catastrophic the consequences of cyber breaches can become. The positive futures with new technologies involve the empowerment and agency of users to control the technology securely. Yet, it requires us to rethink how we interact with the digital world and what authentication is like.

Overall, the power to make changes is distributed across players with different goals and values, making it difficult to influence the unfolding of more secure and inclusive futures. One obvious solution is to support informed decision-making by producing independent research about authentication and cybersecurity. Challenging but important topics include *what incentives drive service providers to select authentication methods that reduce user load, how can the transitions between roles be made smoother with digital identities and authentication solutions, and how governments can support human agency and inclusivity in cybersecurity legislation*.

This study has some limitations. The use of only academics in senior positions may be a source of elite bias (Myers & Newman 2007). Firstly, academics may not put much weight on business aspects and tend to focus on phenomena from a research point of view. This setting also omits the views of junior researchers whose thinking might be less constrained by experience. Thus, the value of the results lies in the independence of academia and the tacit knowledge gained from a long research career. Further, the sample of six informants may not be representative of the field, but it was enough to gain several viewpoints on phenomena around user authentication and cybersecurity. The interpretive research approach reflects the researchers’ worldview, and thus, the selection of themes for the interviews and analysis emphasizes human-centric and less technology-oriented findings.

## 6. Conclusion

This research looked at the future of user authentication in the context of digitalizing societies. We took a very broad interpretation of authentication, including how people are able to control their digital identities in a world where digital services and devices are taking over all walks of life. The aim was to find out how experts view the future of user authentication and security in light of the major trends of digitalizing societies. We conducted semi-structured interviews with six researchers from research areas that touch on the authentication future. We used interpretive hermeneutic analysis to draw themes from these conversations. The major themes were the fragmentation of methods, people's multiple roles, and emerging technologies.

The sample of interviews in this study was rather limited and warrants further study and expanding the pool of experts into other areas of cybersecurity and emerging technologies. Furthermore, after these initial results, the themes could be refined further and used in more structured research, such as a Delphi study. The comprehensive themes used in this study only give indications of how the themes are interrelated, but the data is not extensive or structured enough to draw conclusions within themes. There is a further need for this type of overarching studies that look into the future development of cyber security as a whole to give context to the advances made in technology, society, and individual level.

## References


Al-Ameen, M.N., Haque, S.M.T. and Wright, M. (2016), "Leveraging autobiographical memory for two-factor online authentication", *Information and Computer Security*, Vol. 24 No. 4, pp. 386–399, doi: 10.1108/ICS-01-2016-0005.

Aloul, F., Zahidi, S. and El-Hajj, W. (2009), "Two factor authentication using mobile phones", *2009 IEEE/ACS International Conference on Computer Systems and Applications*, IEEE, pp. 641–644, doi: 10.1109/AICCSA.2009.5069395.

De Angeli, A., Coventry, L., Johnson, G. and Renaud, K. (2005), "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", *International Journal of Human-Computer Studies*, Academic Press, Vol. 63 No. 1–2, pp. 128–152, doi: 10.1016/J.IJHCS.2005.04.020.

Bhana, B. and Flowerday, S. (2020), "Passphrase and keystroke dynamics authentication: Usable security", *Computers and Security*, Vol. 96, doi: 10.1016/j.cose.2020.101925.

Bonneau, J., Herley, C., Van Oorschot, PC and Stajano, F. (2015), "Passwords and the evolution of imperfect authentication", *Communications of the ACM*, Vol. 58 No. 7, pp. 78–87, doi: 10.1145/2699390.

Butler, M. and Butler, R. (2015), "Investigating the possibility to use differentiated authentication based on risk profiling to secure online banking", *Information and Computer Security*, Vol. 23 No. 4, pp. 421–434, doi: 10.1108/ICS-11-2014-0074.

Cho, G., Huh, J.H., Kim, S., Cho, J., Park, H., Lee, Y., Beznosov, K., *et al.* (2020), "On the Security and Usability Implications of Providing Multiple Authentication Choices on Smartphones: The More, the Better?", *ACM Transactions on Privacy and Security*, Vol. 23 No. 4, doi: 10.1145/3410155.

Ciampa, M. (2013), "A comparison of password feedback mechanisms and their impact on password entropy", *Information Management & Computer Security*, Vol. 21 No. 5, pp. 344–359, doi: 10.1108/IMCS-12-2012-0072.

Dasgupta, D., Roy, A. and Nag, A. (2016), "Toward the design of adaptive selection strategies for multifactor authentication", *Computers and Security*, Vol. 63, pp. 85–116, doi: 10.1016/j.cose.2016.09.004.

FIDO Alliance. (2024), "What is FIDO?", available at: https://fidoalliance.org/what-is-fido/ (accessed 25 January 2024).

Furnell, S., Helkala, K. and Woods, N. (2022), "Accessible authentication: Assessing the applicability for users with disabilities", *Computers and Security*, Vol. 113, doi: 10.1016/j.cose.2021.102561.

Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., *et al.* (2017), *Digital Identity Guidelines: Authentication and Lifecycle Management*, Gaithersburg, MD, doi: 10.6028/NIST.SP.800-63b.

Grawemeyer, B. and Johnson, H. (2011), "Using and managing multiple passwords: A week to a view", *Interacting with Computers*, Vol. 23 No. 3, pp. 256–267, doi: 10.1016/j.intcom.2011.03.007.

Haga, W.J. and Zviran, M. (1991), "Question-and-answer passwords: An empirical evaluation", *Information Systems*, Pergamon, Vol. 16 No. 3, pp. 335–343, doi: 10.1016/0306-4379(91)90005-T.

Järpehult, O., Agren, F.J., Backstom, M., Hallonqvist, L. and Carlsson, N. (2022), "A Longitudinal Characterization of the Third-Party Authentication Landscape", *2022 IFIP Networking Conference (IFIP Networking)*, IEEE, pp. 1–9, doi: 10.23919/IFIPNetworking55013.2022.9829804.

Klein, H.K. and Myers, M.D. (1999), "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems", *MIS Quarterly*, Vol. 23 No. 1, pp. 67–94, doi: 10.2307/249410.

Lella, I., Theocharidou, M., Tsekmezoglou, E., Malatras, A., Garcia, S. and Valeros, V. (eds.) (2023) "Enisa Threat Landscape 2023", European Union Agency for Cybersecurity, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

McDowell, B. (2019), "Three ways in which GDPR impacts authentication", *Computer Fraud & Security*, No longer published by Elsevier, Vol. 2019 No. 2, pp. 9–12, doi: 10.1016/S1361-3723(19)30019-3.

Myers, M. and Newman, M. (2007), "The qualitative interview in IS research: Examining the craft", *Information & Organization*, Vol. 17 No. 1, pp. 2–26, doi: 10.1016/j.infoandorg.2006.11.001.

Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y. and Gerla, M. (2019), "Challenges of Multifactor Authentication for Securing Advanced IoT Applications", *IEEE Network*, Vol. 33 No. 2, pp. 82–88, doi: 10.1109/MNET.2019.1800240.

OpenID Foundation. (2024), "What is OpenID Connect", available at: https://openid.net/developers/how-connect-works/ (accessed 25 January 2024).

Rathidevi, M., Yaminipriya, R. and Sudha, S. V. (2017), "Trends of cryptography stepping from ancient to modern", *IEEE International Conference on Innovations in Green Energy and Healthcare Technologies - 2017, IGEHT 2017*, Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/IGEHT.2017.8094107.

Stobert, E. and Biddle, R. (2013), "Memory retrieval and graphical passwords", *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, New York, NY, USA, pp. 1–14, doi: 10.1145/2501604.2501619.

Weir, C.S., Douglas, G., Richardson, T. and Jack, M. (2010), "Usable security: User preferences for authentication methods in eBanking and the effects of experience", *Interacting with Computers*, Vol. 22 No. 3, pp. 153–164, doi: 10.1016/j.intcom.2009.10.001.

Woods, N. and Silvennoinen, J. (2023), "Enhancing the user authentication process with colour memory cues", *Behaviour and Information Technology*, Vol. 42 No. 10, pp. 1548–1567, doi: 10.1080/0144929X.2022.2091474.

Woods, N. and Siponen, M. (2024), "How memory anxiety can influence password security behavior", *Computers & Security*, Elsevier Advanced Technology, Vol. 137, p. 103589, doi: 10.1016/J.COSE.2023.103589.

Yaschenko, V. V. (2002), *Cryptography: An Introduction*, edited by Yaschenko, V. V., Vol. 18, American Mathematical Society.

Zhang, T., Yang, L. and Wu, Y. (2019), "Evaluation of the Multifactor Authentication Technique for Mobile Applications", in Arai, K., Bhatia, R. and Kapoor, S. (Eds.), *Intelligent Computing*, pp. 696–707, doi: 10.1007/978-3-030-22868-2_49.