

Using Personalised Authentication Flows to Address Issues with Traditional Authentication Methods

Jack Holden and Deniz Cetinkaya ^a

*Department of Computing and Informatics, Bournemouth University, Poole, U.K.
{s5204619, dcetinkaya}@bournemouth.ac.uk*

Keywords: Personalised Authentication Flow, Customised Access Methods, Model-View-Controller Approach.

Abstract: Nowadays, a huge proportion of people's data and files are stored online behind a password. While better and more secure methods exist, traditional password-based authentication remains the most predominant. With the current computing processing power trends and the advances in emerging technologies, the need for migration to improved authentication frameworks is becoming more essential. This paper explores the limitations of password-based authentication and how we could begin a gradual migration by using model-driven approaches, reducing password's significance in authentication and encouraging the adoption of newer and more secure methods whilst still ensuring a low access barrier. This paper proposes a new model-based authentication approach returning choice back to the user. The users would be given the ability to choose their own authentication flow, helping bridge the digital divide ensuring people from all technical proficiencies, demographics, and socio-economic classes utilise more secure authentication flows without impacting usability or accessibility. This would be achieved through a modular technological solution allowing developers to add more secure methods of authentication as they come about. The modularity in combination with user choice will ultimately play a huge role in improving uptake and migration to newer authentication methods helping mitigate future risks.

1 INTRODUCTION


When the Internet technologies were simpler compared to the advances today, simple authentication using a username and password was an acceptable way to authenticate. However, with the recent developments and emerging technologies such as artificial intelligence and machine learning as well as the advances in quantum computing, the limitations and risks of using traditional password-based authentication have become increasingly apparent thus highlighting the need for migration to improved authentication frameworks. While the rest of the web is constantly modernising, password-based authentication in its core premise has remained the same since its inception and password-based authentication still dominates the web despite its known weaknesses (Dutson et al., 2019).

Nowadays, a huge proportion of people's lives are stored online behind a password; but humans are inherently predictable when it comes to passwords (Zhang-Kennedy et al., 2016). In addition, with

human password predictability and proliferation across sites, once a password is compromised, other accounts are then also at high risk (Pilar et al., 2017).

The requirement for everyone to transition from traditional authentication methods to more secure multi-factor alternatives is evident. These new methods will shape the future of authentication and are already implemented in various shapes and forms. However, it is essential that users can keep up with this innovation to not risk leaving people from certain generations, demographics and technical proficiencies struggling to adapt, thus isolating them further and increasing the already apparent digital divide (Ahmed et al., 2017). This can be mitigated through a gradual migration strategy and a user-centred personalised approach. By promoting a unified interactive experience and offering user choice when it comes to their authentication flow, both will play a huge role in improving uptake and migration to newer authentication methods.

The aim of this paper is to propose a model-based framework which will serve as a significant step

^a <https://orcid.org/0000-0002-1047-0685>

towards promoting more secure and modern authentication methods across the web, reducing apprehension amongst the less technically inclined whilst simultaneously opening their minds to alternative authentication methods. The solution will offer custom personalised authentication flows designed in a way that offers familiarity and a low barrier entry providing a pathway to gradual migration away from the sole use of passwords. The potential impact of this research is significant, helping begin the conversation of how to address upcoming threats posed to most sites on the web still using traditional authentication. The proposed solution is a model-view-controller (MVC) based web framework that acts as a foundation for applications to easily be constructed upon with the core developmental focus being the authentication layer. This serves as the control centre for the modular multi-factor authentication, personalised authentication flows and reduced-identity privacy-observing protections.

2 LITERATURE SURVEY

2.1 Authentication Methods

Authentication is the process of proving the claimed identity of something or someone, commonly associated with the digital world and access to a system (Ahmed et al., 2017). For decades, traditional knowledge-based passwords have been a steadfast, constant presence on websites, and remain the predominant method to this day (Quermann et al., 2018). This is despite the sheer amount of research highlighting human predictability when it comes to passwords and their susceptibility to emerging threats (Habib et al., 2017). According to Zhang et al., the average user manages 25 password protected accounts and having a complex unique password for each simply exceeds human memory capabilities (Zhang-Kennedy et al., 2016), thus making it no surprise the prevalence of password reuse.

With research showing data breaches and cybercrime on the increase (Dutson et al., 2019; Monteith et al., 2021), and computational power being far less scarce than it used to (Kelley et al., 2018), the underlying weakness of using passwords as a primary authentication method is clear. If one password is compromised through guessing or cracking, password reuse on other accounts has a potential domino effect where malicious actors use the same compromised credentials to try and access the users' other accounts (Nguyen Ba et al., 2021).

Multi-factor authentication (MFA) has helped to improve online account security and has been recommended by leading security agencies including the UK's National Cyber Security Centre (NCSC) (NCSC, 2018). To increase the security of authentication systems, three core factors were recommended in the literature (Lal et al., 2016; Stobert and Biddle, 2018) which are:

- Knowledge: Something you know – e.g., passwords, PINs
- Possession: Something you have – e.g., phone, smart card
- Inherence: Something you are – e.g., biometrics such as face id or fingerprint

To achieve this, it is only possible through advanced methods and with most websites still only providing traditional password-based authentication, they are only able to satisfy the 'Something you know' factor. Big tech companies started to use conditional access controls that allow administrators to specify which authentication methods can be used to access a resource (Microsoft, 2023a). Admins can set any valid combination of strong authentication methods like an old-school password and SMS or modern and stronger methods such as the Authenticator app, OAuth 2.0 or a FIDO2 security key (NCSC, 2022).

These results highlight MFA adoption improvements over the years, but these are only indicative of the websites that offer it with the findings also showing a lack of consistency amongst the users, who do not always enable it when the opportunity presents (e.g., will enable it for email but not social media). There remains a disproportionate number of businesses that have been slow to adopt it and provide it for their users. In addition, research shows it is commonly taken up on a voluntary basis meaning the user must locate it themselves rather than it being a default practice. There is a fine line between choice and security and our proposed authentication approach aims to change the perception so that choice can be moved from the "whether I turn MFA on or off" to "what MFA methods should I use".

2.2 Digital Divide and Inclusive Design

The digital divide refers to the gap between people in society who do not have the opportunity or knowledge to use digital technologies that others do. The main factors contributing to the digital divide include age, socioeconomic status, and other disadvantaged groups (Baker et al., 2020). Research shows these groups are more likely to own older, outdated technology that do not support some of the

modern technical software and hardware advancements used in digital solutions nowadays thus, further isolating them (Martins, 2020). Additional research also highlights how as humans age, we become less open to change partly due to declining cognitive abilities which can result in anxiety, thus stifling exploration meaning stagnation whilst the rest of society progresses, thereby widening the divide (Choi, 2013; Pappas, 2019).

The digital divide issue has had a renewed focus since Covid-19 due to lockdowns resulting in limited face-to-face contact and a rapid shift to online services and working. This stressed the importance of internet access and digital devices to allow communication amongst friends and family as well as access to virtual doctor's appointments, etc. For people used to in-person interactions this shift was especially hard as research shows older people are more likely to own outdated technology and be lesser technically inclined making it harder to navigate a new digital environment (Kumar, 2013). This was recognised by the UK Parliament highlighting their concerns of the digital divide and the effect the pandemic would have on vulnerable groups particularly the elderly and disabled people due to digital exclusion (Baker et al., 2020). Although Covid-19 has now subsided digital exclusion is still relevant and needs to be addressed as the world becomes more digital, ensuring these demographics are not left behind.

These findings reinforce the need for a solution that is easily extensible thus not stifling innovation while still providing an interface that offers familiarity, ensuring a low usability barrier but crucially, through personalised choice promote adoption amongst people from isolated demographics and different technical proficiencies to choose what is best suited for them. This encourages exploration of new methods allowing natural human curiosity to take over whilst still improving authentication and safety of their accounts to protect from the ever-growing threats. Through these steps, it improves the accessibility of using more secure authentication, stemming the divide.

2.3 User Experience and Accessibility

Usability is defined by the ease in enabling users to achieve goals effectively, efficiently and with satisfaction using a product (ISO, 2018). With authentication, usability has a huge role in the uptake and success of new methods, including accessibility, ease of setup and convenience. Reese et al. (2019) analysed the usability of five common MFA methods

through usage and setup over a two-week period. These methods included: SMS, Time-based One-Time Password (TOTP), pre-generated codes, push notifications and YubiKey. All five authentication methods were seen as usable, with overall positive feedback and willingness to use MFA. However, one-third of participants reported not having their MFA devices accessible. Participants also did not want to be required to use MFA from a known computer (Reese et al., 2019).

Risk-based authentication (RBA) is an adaptive security measure that strengthens authentication systems providing a score determining if that person is who they say they are, and requiring additional checks if the system is not confident (Wiefling 2020). RBA works by recording and monitoring additional information such as IP addresses, time zones, and device details including fingerprint and user agent. A risk score is then estimated, typically classified into low, medium, high. Based on this score, validation requirements can be adjusted (Wiefling 2020). It maintains usability for users assessed as low risk, returning a familiar sign in experience with minimal barriers. Whereas a stranger who is identified as high risk, is faced with a multitude of barriers in the form of additional authentication methods providing an inconvenient, long sign in experience. By including this as part of the solution we are ensuring maximum usability and potential uptake from those more cautious or feel this system could be an inconvenience to them.

2.4 Emerging Technologies

Recently, 'Web3', powered by Blockchain, has been gaining increased attention within the industry. Blockchain is an incorruptible decentralised and secure digital ledger technology used for recording and verifying transactions, without the need for middlemen (Golosova, 2018). Web3 has bought about a new method of authentication which takes a new approach in verifying identities. By adopting a decentralised approach, it offers several advantages over traditional methods, resulting in reduced risk of being hacked and data breaches as well as addressing the prevalent issue of password reuse. However, it still pales in comparison to the existing web solutions, especially when it comes to usability, accessibility, practicality, and scalability (Murray, 2023).

Another emerging technology is Quantum Computing which uses the laws of quantum mechanics to solve advanced problems that standard computers cannot (IBM, 2023). This is possible due to its use of quantum bits (qubits) which represent 0s

and is simultaneously meaning multiple calculations can be performed at once, allowing advanced problems to be solved much quicker. Although not readily available enough yet, one day it will be therefore posing a significant threat to existing security infrastructure such as digital authentication and encryption used to keep data and people safe (Chen et al., 2016).

These findings reinforce the fact that traditional password-based authentication will not be sufficient in maintaining account security. This highlights the need for an easily extensible, multi-factor authentication framework that can adapt as the threat landscape changes, thus futureproofing itself. It also emphasises the need for modules to support isolated-logic providing maximum flexibility so that when quantum-safe cryptography is developed or a new threat presents itself, new methods can be easily created and integrated.

2.5 The Power of Choice

There is extensive research surrounding the psychology behind the power of choice and the corresponding human behaviour when that choice is inhibited. A concept called “psychological reactance theory” (PRT) posits that when a human feels their freedom of choice is restricted or removed, a negative emotional reaction is triggered such as stubbornness or anger (Brehm 1966; Steindl 2015). Research on the psychology of control further reinforces PRT, discussing control and behavioural traits. It examines perception and how those who feel they have control over their choices are more likely to be open minded and explore new options, this can be applied to the authentication framework (Langer 1983).

As technology continues to advance, so does the threat landscape. Incorporating these psychological findings into the solution will change the way users perceive authentication, making it feel more personal, increasing engagement, and promoting adoption of more secure methods in place of traditional authentication.

2.6 Privacy Implications and Concerns

Authentication frameworks aim to find the right balance to reduce the privacy concerns whilst still providing a seamless secure experience. When a user signs up to a website and hands over personal data, it becomes the websites responsibility and legal obligation to protect so no unauthorised access can occur. However, with the increase in cybercrime and cyberattacks, there is a constant threat to users’ data.

With the introduction of the General Data Protection Regulation (GDPR), it is mandated that users must give explicit consent before sites could store and process personal data only for as long as necessary for its specified purpose and that valid reasons must be given for its collection (GDPR.eu, 2018). In the occurrence of a data breach, the businesses are legally obligated to inform all users due to depending on the severity of the breach including personal identifiable information or passwords, this exposes their users’ other accounts to risks such as identity theft and fraud (Bisogni and Asghari 2020).

Personal data is collected in authentication systems and used for additional verification purposes such as recognising fraudulent attempts based on patterns and habits. RBA is recommended by the NCSC actively promoting zero-trust architecture in systems (NCSC 2021), and it is used by big tech companies. However, RBA involves using personally identifiable information to help assess risk levels and genuine attempts, such as IP address, browser information, and device fingerprint. This raises legitimate concerns regarding privacy, ethics, and data protection law compliance like GDPR. If a database storing this information was breached, it could be possible for malicious actors to identify and target individuals, exposing locations and other personal data not traditionally collected with username and password leaks.

Overall, it is clear that there is a need for a privacy-by-design solution incorporated into the authentication methods that mitigates the risk of personal data exposure protecting both users and businesses ensuring compliance and safety. Proposed solutions include data deletion feature, database encryption, reduced login history or consent mechanism allowing the user to set what level of data to share, etc. Implementing some of the above will provide further choice and awareness to the user and provide a better authentication solution that balances privacy and security.

3 DATA COLLECTION

In this study a quantitative research method was used to collect data about the participants’ views and preferences on authentication as well as secondary research was performed from the literature. The primary data was collected via an anonymous survey by using JISC online surveys. 80 participants took part in this research of varying proficiencies and demographics. Participants have been recruited randomly from a variety of places including students,

professional and personal connections via email and social media. The target demographic was those aged 18-70 from all genders and professions. The only stipulation for this study was to aim a 60/40 rule was maintained with 60% of participants not having affiliations with the IT industry and are therefore less technically inclined with the remaining 40% having considerable IT knowledge.

3.1 Results and Findings

Overall, the data produced positive insights from a wide demographic of varying technical proficiencies. Most participants (63.7%) were between the ages of 18-25 with the majority being higher education students (36.3%). 19 participants (23.8%) were from the technology and IT sector while others were from various sectors such as sales, finance, education, healthcare, etc. Most participants were male (61.3%). The question “Thinking about your passwords right now, are you reusing the same password across multiple sites?” was answered as “Yes” by 65 people, so most participants (81.3%) still reuse their passwords in some capacity reinforcing apparent password weaknesses.

To further get an insight into the data, two independent t-tests were run in Jamovi. Analysis showed that on average participants who were technically proficient viewed password authentication as less safe and secure (M=3.06, SD=1.50) than participants without (M=3.75, SD=1.86). An independent t-test was conducted to investigate the difference between means further. The t-test revealed that there was not a significant difference between technically proficient and non-technical participants’ perception of password safety, $t(78) = -1.74, p = .085$. As there was not a significant difference between both proficiencies’ perception of password safety and security, it can be interpreted that both groups do understand the risks associated but still choose to use it anyway.

The second analysis depicted those who reported being hacked before view passwords as less safe (M=3.88, SD=1.58) than those who have not (M=3.20, SD=1.73). The independent t-test illustrated that there was no significant difference between those who had been hacked and those who had not’s perception of password security. Despite the difference between means not being significant, the data shows that being previously hacked does affect their perception of password security.

Findings show most participants across all demographics (90%) have been exposed to MFA suggesting its wide acceptance by users.

Consequently, the use of this technology in the solution will be familiar to most users meaning no shock factor nor steep learning curve.

When measuring the authentication methods that participants would be happy to use as part of their sign in process, the data was split by technical proficiency providing a more targeted insight. The findings shown in Figure 1 illustrate that overall, all participants would include biometrics as part of their authentication flow. From here it deviates with technically proficient participants more likely to choose ‘Additional-device authentication’ (84.4%), compared to non-technically proficient (41.7%) who would prefer to use one-time passwords (79.2%).

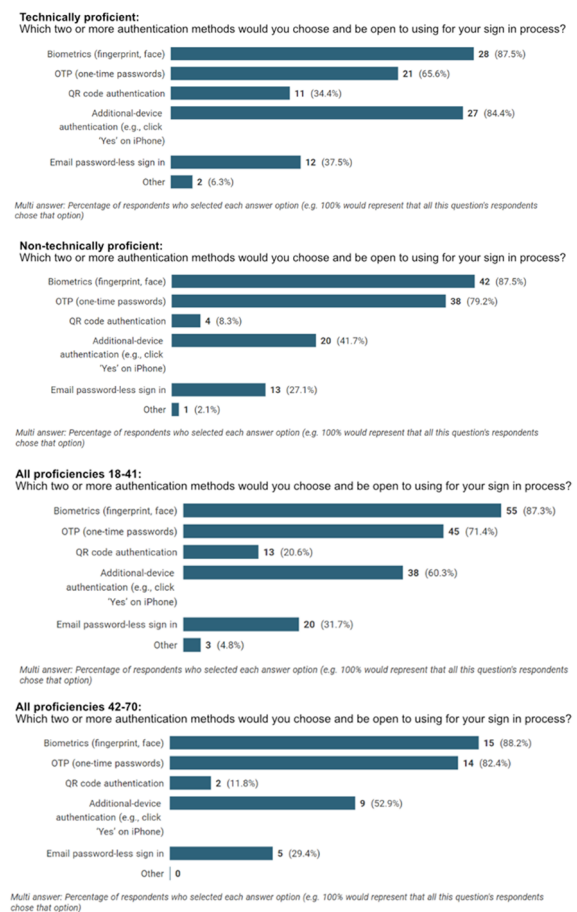


Figure 1: Survey participants’ methods of choice.

These findings were further analysed by age group suggesting those aged 18-41 are more likely (20.8%) to include QR code authentication as part of their flow compared to 42-70 (11.8%). Thus, reiterating the important of offering choice, allowing the solution to cater to all demographics and proficiencies. Participants were asked which

authentication methods they currently use on their accounts. For this question, there was one surprising result, 72.9% reported actively using biometrics as a medium for account authentication. This result may be the consequence of participants potentially mistaking password autofill, which utilises FaceID/TouchID, as a form of biometric account authentication. Therefore, we interpret with caution.

4 A PERSONALISED MODULAR AUTHENTICATION FRAMEWORK

Findings from the literature and survey data helped to prioritise the requirements for our proposed authentication framework which utilises a user-centric and personalised approach. A modular authentication system is designed allowing users to choose methods best suited to them and their circumstances. Figure 2 gives a high-level overview of the framework. MVC architectural pattern was chosen due to being widely used and simple to implement. The MVC pattern ensures a clean separation of concerns with the application split into three main components: the Models, Views, and Controllers. This helps ensure the components are loosely coupled from each other and provides extensibility and maintainability (Microsoft 2023b).

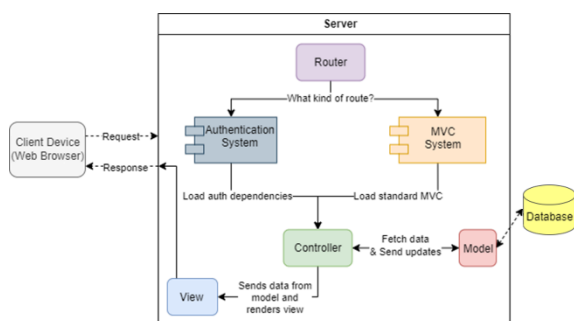


Figure 2: System overview diagram.

With model-driven development, the framework is designed so it abstracts the complexity of a large authentication system into manageable authentication method modules. Each module can then be developed independently (following the plugin “house-style”), tested through setting test data values, and integrated easily. The proposed framework distinguishes between authentication system and business-specific system.

The authentication system implementation follows a flexible approach where it provides

modularity with the authentication methods, so each authentication method is effectively its own self-contained isolated MVC. Each method has its own controller logic, view template and ability to interact with the database through functions exposed. This creates a robust, isolated environment for the authentication method developer to work in and create their unique method without having to worry about breaking other elements of the system.

This modular approach to the traditional MVC ensures layers are separated: method database interaction (Models), method UI design (Views), and method control/validation logic (Controllers), thereby ensuring maintainability, scalability and simplifies the ability to introduce new authentication methods into the system.

The router supports attribute routes, normal array routes, and method routes. When developing the authentication part, attribute routes allow for separation of concerns in regard to the rest of the business specific application. Figure 3 shows a workflow for the proposed authentication system and provides a high-level outline of its functionality.

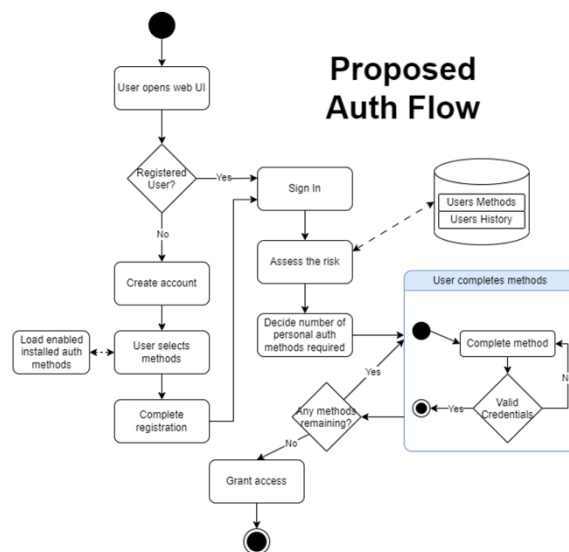


Figure 3: Proposed authentication flow diagram.

4.1 Interface Design

High-fidelity interface wireframes were created on Figma, a popular powerful online tool for UI designers. Some key designs can be seen in Figure 4.

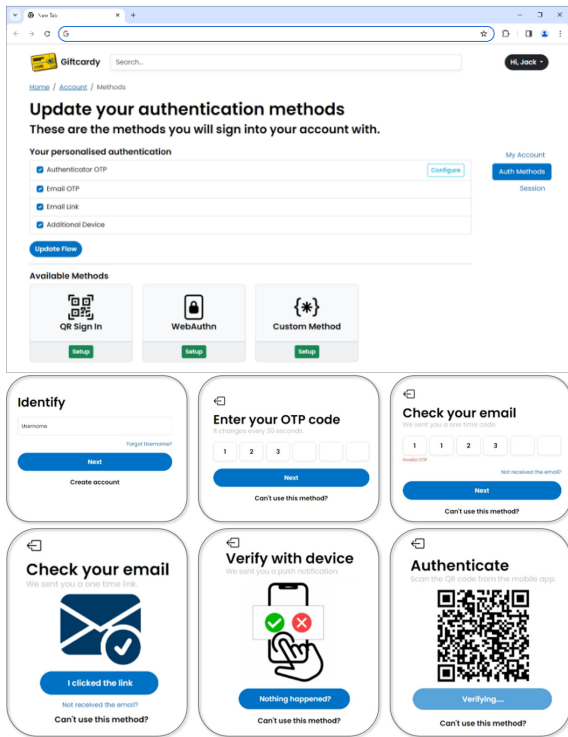


Figure 4: Selected designs for setup and various methods.

4.2 Prototype Implementation

For the implementation of the authentication solution, the Bootstrap framework was used for the frontend of the web application and React Native was used for the mobile application. The traditional LAMP stack (Linux, Apache, MariaDB, and PHP) was used for the backend server setup. GitHub was used for version control, PhpStorm was selected as the IDE.

With the authentication system, in its current prototype form, it consists of two routes: /identify and /authenticate. /identify is responsible for fetching user info and assessing initial risk. Cookie-based sessions are used to keep track of the method for /authenticate and load the correct method automatically and thereby loading its logic and view. An automated process flow was designed so that each auth method step is triggered sequentially in a random order defined by the server. One then iterates through each method's individual validation logic, view and check with the database ensuring all met before moving onto the next until all are completed and authentication is successful.

Dynamic loading of authentication modules is employed where namespaces were used and a "house-style" where methods must include a template.php for their view file and then the controller file must be the same name as the class which then allows autoloading

to be successful. The database design for the prototype implementation is given in Figure 5. We utilised Expo Web Browser package allowing the sign in experience to be consistent throughout all platforms, reducing technical debt. We enabled Progressive Web App (PWA) support meaning devices such as iPads could receive push notifications to complete actions.

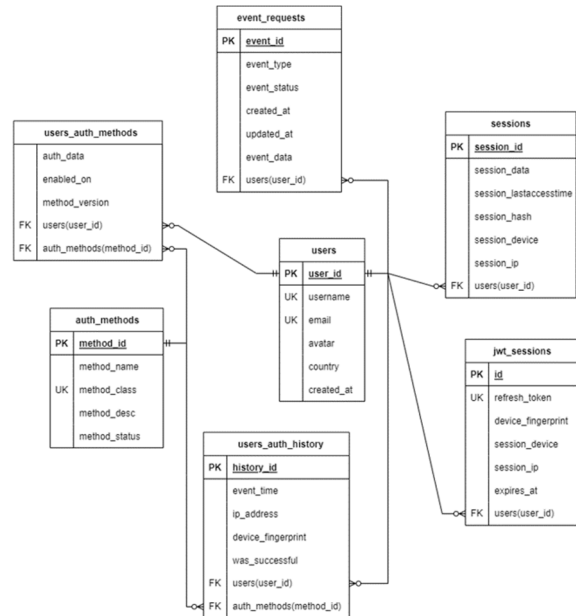


Figure 5: Database design.

4.3 Evaluation

To showcase the framework's core functionalities and its usability, a case study and mock-up prototype was designed and implemented to illustrate a real-life scenario. A responsive giftcards website was developed as a proof-of-concept where users can buy giftcards for various supermarkets or shops and send them to others as a gift.

In addition, a user feedback survey incorporating the System Usability Scale (SUS) was conducted to assess the usability of the prototype and gather feedback from six participants representing industry and the general public (Usability.gov, nd). SUS has been shown to be more reliable and detect differences at smaller sample sizes. Participants were given the SUS form to complete along with a text box for additional feedback. Once completed, the feedback was reflected upon, and the SUS scores were calculated to determine the usability. On calculation, the overall score came to 83.75 which indicates the prototype is very usable.

Overall, the results from this survey were very positive with some very valuable feedback, all of which can be applied to a future version. From the survey, everyone agreed the system is usable, although there is a variation in SUS scores suggesting those more technically inclined found it easier to use the prototype and therefore gave a better SUS score. Two participants suggested improving setup instructions such as providing a native modal that is part of the module system and multimedia for better visual understanding.

5 CONCLUSIONS

This paper proposed an alternative approach to the traditional authentication methods with the objective of migrating users towards a choice-based system. This would allow users to choose their own methods that suit their needs and circumstances therefore addressing usability yet also ensuring improved security. The discussed solution is designed with modularity, ensuring easy upgradability and futureproofing against emerging threats through a plugin system and API allowing developers to create custom authentication methods whilst gradually phasing out less secure methods. The proposed solution framework consists of risk-based authentication, multi-factor authentication, and choice. These three components in cooperation with a modular plugin system allow for the best of existing solutions to come together and act as the barebones for future extending with one new component, user choice. Overall, this offers a flexible and user-centric approach that addresses the limitations of password-based authentication, promotes usability, and adapts to evolving security challenges however future work is needed to determine the best method of implementation. For example, a further area for improvement can include setting choice conditions ensuring for example at least one ‘Something you know’ in combination with ‘Something you are’ or ‘Something you have’ have been selected to add variation to authentication flows.

ACKNOWLEDGEMENTS

The authors would like to thank the participants who took part in the survey.

REFERENCES

- Ahmed, E., DeLuca, B., Hirowski, E., Magee, C., Tang, I. and Coppola, J. F. (2017). Biometrics: Password replacement for elderly? *In IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. DOI: 10.1109/LISAT.2017.8001958
- Baker, C., Hutton, G., Christie, L. and Wright, S. (2020). COVID-19 and the digital divide [online]. Available from: <https://post.parliament.uk/covid-19-and-the-digital-divide/> [Accessed 17 Feb 2023].
- Bisogni F. and Asghari H. (2020). More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws. *Journal of Information Policy*, vol 10, pp. 45-82. DOI: 10.5325/jinfopoli.10.2020.0045
- Brehm, J. W. (1966) *A theory of psychological reactance*, New York: Academic Press.
- Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. Available from: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>. DOI: 10.6028/NIST.IR.8105
- Choi, N. G. and DiNitto, D. M. (2013). The Digital Divide among Low-Income Homebound Older Adults: Internet Use Patterns, eHealth Literacy, and Attitudes toward Computer/Internet Use”, *Journal of Medical Internet Research*, vol 15 (5). DOI: 10.2196/jmir.2645
- Dutson, J., Allen, D., Eggett, D. and Seamons, K. (2019). Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. *In IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 17-19 June 2019. DOI: 10.1109/EuroSPW.2019.00020
- GDPR.eu, 2018. What Is GDPR, the EU's New Data Protection law? [online]. Available from: <https://gdpr.eu/what-is-gdpr/>, [Accessed 12 June 2023].
- Golosova, J. and Romanovs, A. (2018). The Advantages and Disadvantages of the Blockchain Technology”, *In IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*.
- Habib, H., Emami-Naeini, P., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Christin, N. and Cranor, L. (2018). User Behaviors and Attitudes Under Password Expiration Policies. *In Proceedings of the 14th USENIX Conference on Usable Privacy and Security (SOUPS)*.
- IBM, “What is Quantum Computing? [online]”, Available from: <https://www.ibm.com/topics/quantum-computing> , [Accessed 29 July 2023].
- International Organization for Standardisation. (2018). ISO 9241-11: 2018 Ergonomics of human-system interaction. Part 11: Usability: Definitions and concepts.
- Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F. and Lopez, J. (2012). Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. *In IEEE Symposium on Security and Privacy*, 20-23 May 2012. DOI: 10.1109/SP.2012.38

- Kumar, S., Ureel, L. C., King, H. and Wallace, C. (2013). Lessons from our elders, In *Proceedings of the 6th International Conference on PErvasive Technologies Related to Assistive Environments (PETRA)*.
- Lal, N., Prasad, S., Farik M. (2016). A Review of Authentication Methods. *International Journal of Scientific & Technology Research*, vol 5 (11).
- Langer, E. J. (1983). *The Psychology of Control*, SAGE Publications.
- Martins Van Jaarsveld, G. (2020). The Effects of COVID-19 Among the Elderly Population: A Case for Closing the Digital Divide, *Frontiers in Psychiatry*, vol 11.
- Microsoft, (2023a). Conditional Access authentication strength [online], Available from: <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths>, [Accessed 14 July 2023].
- Microsoft, (2023b). Overview of ASP.NET Core MVC [online], Available from: <https://learn.microsoft.com/en-gb/aspnet/core/mvc/overview> [Accessed 1 Apr 2023].
- Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C. and Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, vol 23 (4). DOI: 10.1007/s11920-021-01228-w
- Murray, A., Kim, D. and Combs, J. (2023). The promise of a decentralized Internet: What is web 3.0 and how can firms prepare? *Business Horizons*, vol 66 (2), pp. 191-202.
- NCSC, (2018). Stepping up to multi-factor authentication [online]. Available from: <https://www.ncsc.gov.uk/blog-post/stepping-multi-factor-authentication>. [Accessed 16 Feb 2023].
- NCSC, (2021). Zero trust architecture design principles - Authenticate and authorise everywhere [online], Available from: <https://www.ncsc.gov.uk/collection/zero-trust-architecture/authenticate-and-authorise> [Accessed 16 Dec 2023].
- NCSC, (2022). Authentication methods: choosing the right type [online]. Available from: <https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type> [Accessed 6 Jan 2024].
- Nguyen Ba, M. H., Bennett, J., Gallagher, M. and Bhunia, S. (2021). A Case Study of Credential Stuffing Attack: Canva Data Breach. *International Conference on Computational Science and Computational Intelligence*.
- Pappas, M. A., Demertzi, E., Papagerasimou, Y., Koukianakis, L., Voukelatos, N. and Drigas, A. (2019). Cognitive-Based E-Learning Design for Older Adults. *Social Sciences*, vol 8 (1). DOI: 10.3390/socsci8010006
- Pilar, D. R., Jaeger, A., Gomes, C. F. A. and Stein, L. M. (2012). Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. *PLoS ONE*, 7 (12). DOI: 10.1371/journal.pone.0051067
- Quermann, N., Harbach, M. and Dürmuth, M. (2018). The State of User Authentication in the Wild. In *4th WAY Workshop: Who Are You?! Adventures in Authentication Workshop*, Baltimore, Maryland.
- Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J. and Seamons, K. (2019). Usability Study of Five Two-Factor Authentication Methods. In *Proceedings of the 15th USENIX Conference on Usable Privacy and Security (SOUPS)*, pp. 357-370.
- Steindl, C., Jonas, E., Sittenthaler, S., Traut-Mattausch, E. and Greenberg, J. (2015). Understanding Psychological Reactance: New developments and findings. *Zeitschrift Für Psychologie*, vol 223 (4), pp. 205-214. DOI: 10.1027/2151-2604/a000222
- Stobert, E. and Biddle, R. (2018). "The Password Life Cycle", *ACM Transactions on Privacy and Security*, vol 21 (3), pp 1-32.
- Usability.gov website. System Usability Scale (SUS) [online], Available from: <https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>, [Accessed 16 Feb 2023].
- Wiefeling, S., Dürmuth, M. and Lo Iacono, L. (2020). More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In *Annual Computer Security Applications Conference*. DOI: 0.1145/3427228.3427243
- Zhang-Kennedy, L., Chiasson, S. and Oorschot, P. van. (2016). Revisiting password rules: facilitating human management of passwords. In *Proceedings of the APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, June 2016. DOI: 10.1109/ECRIME.2016.7487945.