Accessible Authentication and Authorization in FinTech

Ensuring financial applications are inclusive to users with disabilities

David Cropley
Computing and Informatics
Bournemouth University
Poole, United Kingdom
dcropley@bournemouth.ac.uk
ORCID: 0009-0000-1026-9239

Paul Whittington
Computing and Informatics
Bournemouth University
Poole, United Kingdom
whittingtonp@bournemouth.ac.uk
ORCID: 0000-0002-4401-3503

Huseyin Dogan
Computing and Informatics
Bournemouth University
Poole, United Kingdom
hdogan@bournemouth.ac.uk
ORCID: 0000-0002-9138-9319

ABSTRACT

There exists a growing body of evidence to suggest that authentication (and related authorization) used by online applications is not as accessible as we would ideally like to think. In fact, current research suggests that there is an increased likelihood of usability and security issues for disabled users, leading to frustration, abandonment, and inequality for this sector.

Detrimental to this, the body of existing research lacks empirical data in any substantial quantity and is often devoid of any real solutions to the problem. Therefore, we propose a Framework which will outline how an organization can construct an authentication system (this Framework will feature a prototype application known as 'Authentibility' as a proof-of-concept) to provide accessible features and communicate needs to an organization on a disabled users behalf.

Indeed, parties that have already expressed an interest in this Framework include those from the financial sector. Other sectors may include governmental department, charities, educational establishment and other public or private sector Small and Medium-sized Enterprises (SMEs). Notably, financial technology (FinTech) use cases could prove quite lucrative to this large market sector, given the correct circumstances and environment to thrive in.

Naturally, financial companies will expect an elevated level of security and features, such as an Application Programming Interface (API) connection for banking systems to be able to communicate autonomously with the said application or bespoke framework system. Through a system of empirical research, analysis and contemplation over a multitude of interrelated factors such as human computer interaction, assistive technology, software design and established cybersecurity practices, the study aims to provide an advanced solution for the disabled sector which can account for up to 25% of the population in some regions.

A further advantage of this Framework is that it goes beyond just authentication into the realm of authorization. The user has the option of allowing the application to pass information about their disability to the connected organization. Crucially, this data could be invaluable to a FinTech business, when deciding what type of product is best suited to their client when assessing an application; for example: when considering stipulations or allowances that could be either vital, mandatory, or desirable, under the current disability equality act.

This is important because while the traditional finance industry deliberates over affordability issues based on discount values covering protracted periods, it should not exclude a unique and often gifted sector of the market due to technical challenges. In fact, as an obligation, FinTech should inherently be spearheading sound and professional technical practices in the marketplace, simply due to its very namesake.

CCS CONCEPTS

- Human-centered computing
- Accessibility • Human computer interaction (HCI)

KEYWORDS

Accessibility, Assistive Technology, Authentication, Authorization. Cyberpsychology, Cybersecurity, Disability, E-business, Financial Sector, FinTech, Framework, System Architecture

1 IMPORTANCE OF ACCESSIBLE AUTHENTICATION TO FINTECH

Currently there is a gap in research for Accessible Authentication for online applications and current studies have indicated that there is an indication that there are severe "usability issues" for disabled people trying to use authentication procedures [1], however, regrettably they lack empirical evidence to back up this claim. Furthermore, a recent literature review about authentication for the disabled [2] reveals a lack of dispersed analysis across a large enough variety of impairments, a disparity of involvement from disabled users in the design of these systems along with issues with the methodological approaches and other factors indicating that the research has yet some way to progress.

This paradigm highlights issues for people with disabilities when trying to login that is over and above those experienced by able- bodied people and highlights a fundamental technological problem that developers have neglected to properly address when creating systems. Although this may not be deliberate, it can indicate a lack of understanding of requirements, and hence the need to develop a Framework to help define a sensible guideline when implanting an authentication tool. Naturally, a FinTech e-business relies on technology to expedite financial transactions and having a usable yet secure interface to operate with, will be key to its principal brand recognition for promoting usability, reliability, and inclusivity for all its customers.

The proposition for this accessible Framework and related application, known as Authentibility, has had feedback from financial organizations as found in a study by Whittington and Dogan [3]. This indicates a desire from them for an API to interface with for conducting security checks and transferring data. This leads us to the hypothesis that authentication (in this context) is the accessible login system and authorization is the vehicle for passing information about a user's disabilities to the firm.

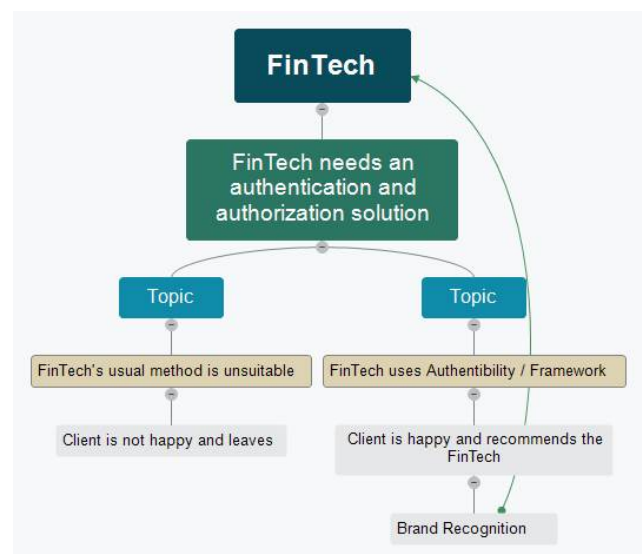The flowchart in Figure 1 below highlights the advantage of this Framework to a FinTech e-business.

Figure 1: **Flowchart highlighting the benefit to a FinTech of using the Authentibility Framework**

2 CURRENT PROTOTYPE

The direction of the research follows multiple paths that are all connected to producing a robust framework either for other firms to work with, or for commercial development of the Authentibility application. Examples of these research domains include types of disability, human computer interaction and related cyberpsychology aspects of system design, good layout practices and human considerations. Other more technically related branches include assistive technology (AT), API

programming, cybersecurity in the form of token generation, number hashing, brute force protection, again alongside more human factors such as susceptibility to social engineering, human error and physical or mental limitations.

2.1.1 Current Progress. Following on from the initial research conducted by Whittington and Dogan [3], a further study has been conducted of current peer-review material, books and related technical information about all the above-mentioned topics. This empirical study will fortify what is known about the topic with fresh data which precludes an in-depth analysis of the results. It will then guide the development of the Framework and lead to a functional prototype as a concept demonstrator.

2.1.2 Prototype Images. To conclude this paper, Figure 2 contains two screenshots of the prototype Authentibility Android application.
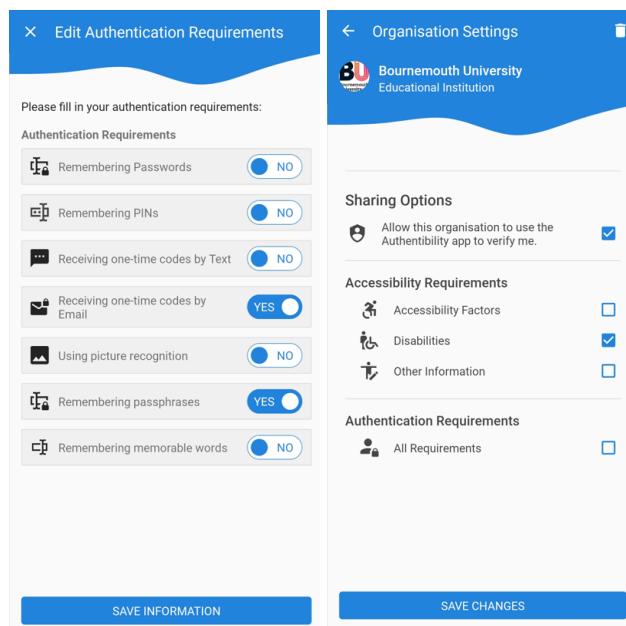

Figure 2: **Entering authentication requirements and informing organizations using the Authentibility application**

REFERENCES

[1] S. Furnell, K. Helkala and N. Woods. 2022. Accessible authentication: assessing the applicability for users with disabilities. In *Computers & Security, Volume 113,102561.* ISSN 0167-4048.

[2] S. Andrew, S. Watson, T. Oh and G. W. Tigwell. 2020. A review of literature on accessibility and authentication techniques. In *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '20). Association for Computing Machinery, New York, NY, USA, Article 55, p. 1–4.*

[3] P. Whittington and H. Dogan. 2023. Authentibility Pass: An accessible authentication gateway for people with reduced abilities. In *Proceedings - 2023 IEEE International Conference on e-Business Engineering, ICEBE, pp. 155-162.*