Abertay University

School of Design and informatics

Independent ATM Authentication for Care Home Residents

Andrew R. Calder

1503321

21st March 2022

Contents

List of Figures **2**

1 Introduction **1**

2 Background **1**

3 Recommendation **3**

4 Machine Learning **4**

5 Experiment Outline **5**

6 Limitations & Challenges **6**

7 References **6**

List of Figures

1 Primary Display (Unauthenticated) 3
2 Bootstrap-based sign up 3
3 Sign-up With Code 4
4 Authenticate user (sign-up/login) 4
5 Withdrawal (adaptive interface) 5

1 Introduction

The UK population is ageing – in 2017 roughly 18.2% of the population (henceforth referred to as the elderly) were aged 65 or above; according to projections the elderly will number 20.7% by 2027 (*Overview of the UK population: November 2018* 2018). As the population ages, the demand for appropriate care services will also rise. There are two main types of care home services available in the UK; 'Care Homes' - which provide personal care such as assistance washing, dressing, medicating et cetera, and 'Nursing Homes' - which offer assistance from qualified nurses as well as personal care. According to the National Institute for Health and Care Excellence, a reasonable level of independence is essential to mental well-being in the elderly (*Older people: independence and mental wellbeing* 2015). This independence may take a variety of forms but one that particularly lacking at the moment is financial.

The current lack of financial independence in care environments is not without reason; the elderly make excellent targets for cybercrime and extortion; senior citizens are the most likely to own their own home, have excellent credit, and savings(*Fraud Against Seniors* 2016). Typically the elderly are much less likely to report such crime because they don't know how to report it, are ashamed that they might have been scammed, or are concerned that their financial independence will be restricted if they do report it - all of these factors are attractive to those with malicious intent (*Fraud Against Seniors* 2016). According to Aviva, around 75% (3,423,466) of surveyed elderly have been targets of email scams and 4% (136,939) had fallen victim. Additionally, 66% had been targeted by telephone-based scams with 5% reporting to have fallen victim (plc 2017). While the majority of those targeted did not fall victim to the scams, it is clear that a significant portion of the population would benefit from more context-intelligent financial security systems - be that at a bank or at an ATM. Financial abuse of the elderly does not only happen through external actors, in some cases those who are trusted to act in the best interests of a vulnerable elder abuse their position of trust and power to defraud them. These abusers could be a relative, neighbour, or even a health or care professional in their home environment (*Abuse and neglect of vulnerable adults* 2018). With traditional ATM security it would be very hard to detect such abuses of trust and/or power.

Aside from the social/security challenges, there may be other factors such as age-related infirmities limiting financial independence. With age come cognitive issues; maintaining attention for a period of time becomes more challenging (Stankov 1988), rate of learning is impeded (Salthouse, Birren and Schaie 1985), and short term memory can become limited (Akatsu and Miki 2004). The onset of these issues can be caused by common health issues. For example, dementia can lead to difficulties remembering, a lack of patience, and confusion. The elderly also face physical challenges; arthritis (and similar conditions) can cause pain when typing, tremors, and coordination problems - all of which would make use of a traditional ATM interface a challenge.

When designing a financial access point for the elderly many factors should be considered. In this paper an ATM prototype is proposed which aims to mitigate external attacks, minimise the risk of abuse by trusted individuals, and improve physical and cognitive accessibility.

2 Background

It is widely accepted that intelligence in older adults should be measured differently. In (Cavanaugh and Blanchard-Fields 2018), Cavanaugh states older adults "search for less information, requires less information, and rely on preexisting knowledge structures in making everyday decisions" -they cope well with the familiar. As expected -conversely, in "unfamiliar situations, and when the decision task requires high cognitive load" older adults tend to perform poorly. Additionally, maintaining attention becomes more challenging (Stankov 1988), and short term memory (Akatsu and Miki 2004) and rate of learning are impeded. When designing an interface for this group, their specific needs should be considered.

Pohl discusses the need for individualized learning interfaces through the use of user modeling and machine learning in (Pohl 1996). User modelling allows an application to "try to adapt their behaviour to their users' individual characteristics", in turn the interface "becomes gradually more effective as it learns the user's interests, habits and preferences". Given the possibility of cognitive decline in the residents, providing an interface tailored to their usage and needs could drastically improve accessibility. In (Bilgi and Tugrul 2018), Bilgi proposes a graphical user authentication system "based on the principle that people remember visual objects more than texts". The method described was specifically designed to prevent shoulder-surfing; when an individual observes your interaction with the interface they will see something different to what you have seen. This is achieved through

the use of hybrid images which "are created by mixing different features of two images". The individual looking directly at the image sees the primary image whereas the anyone looking at it from another angle sees the secondary image. While this seems like a good solution to the shoulder surfing problem, it may not be the most fitting solution for the elderly as the ability to filter extraneous detail out deteriorates with age (Hawthorn 2000).

Suru conceptualizes a hybrid graphical authentication system consisting of "property based authentication systems which adopt the use of image properties for user authentication, rather than specific images as used in existing systems" in (Suru 2018). Suru notes that that "humans are better able to memorise images than text"; as short term memory can become limited (Akatsu and Miki 2004) in old age, selecting a method of authentication that is easier to remember could improve accessibility and usability. However, Suru also states that graphical authentication systems demonstrate some of the same flaws as passwords and pins - "These flaws include predictability, vulnerability to observational attacks and the inability of systems to efficiently combine security with usability". Passwords lack usability, but graphical authentication methods lack security. In (Renaud and Ramsay 2007), Renaud proposes another graphical authentication system - 'Handwing'. The Authentication system relies on handwriting recognition and was tested on church members over the age of 60. A user "must provide his or her handwritten digits and postcode. He or she also provides a hand-drawn doodle.", this is then used instead of a password upon login but a username or email address is still required to identify the user. Despite users perceptions of security - complete satisfaction - Renaud notes that "The HandWing mechanism is weaker, more memorable and definitely more usable than passwords". This authentication system might be suitable for a low risk account login; however, for a system that will provide direct access to a residents finances it would not be sufficient unless limitations were made.

While images might be easier to memorise than passwords (or PINs), they still relies on remembering new information and so the same memory-related issues may still prevail. A convinving alternative is described in (Romanowski et al. 2016), in which Romanowski reviews the security and accessibility of palm vein scanner implementations. Romanowski notes that the original palm vein research was conducted back in 2000 by a Korean research team who "achieved a reliability rate of 99.45% with a delay speed of 150 ms" (per scan). Since then the technology has further developed for commercial use; Fujitsu announced *PalmSecure* which was intended for a variety of uses, and the Bank of Tokyo-Misubishi created the Super-IC Card VISA card which could be used with the technology. The *PalmSecure* system has actually already been implemented in ATM systems - "the Suruga Bank and the Bank of Tokyo-Mitsubishi in Japan deployed the *PalmSecure* contactless system for use in account security services". Due to the physiological principles involved palm vein scans (unlike facial and fingerprint biometric alternatives) are extremely difficult to spoof, and additionally they are highly unlikely to change over time. Given that palm vein scanners have already been used in ATMs, they are fast, secure, consistent and accurate, palm vein scanners seem to be the most practical choice for authentication.

Some biometric authentication methods become less accurate in aging populations due to physical changes for example, "elderly people lose collagen which makes their fingerprint difficult to read" ('Multimodal Biometrics: A Measure for Enhancing Authentication'). In constrast, vein patterns can still be used to authenticate even when changes in temperature decrease blood-flow, or tissue diseases cause damage; "vein patterns can be used throughout the year to identify patients with connective tissue diseases, but some attention is needed for patients with advanced disease such as Systematic Sclerosis" (Kono et al. 2015).

Last year, Fujitsu detailed an update to their *PalmSecure* system in a press release (*Fujitsu Develops Non-contact Biometric Integration Technology as an Optimal Solution for a Cashless Society* 2018). Intended for release in 2020, Fujitsu announced they will be combining facial recognition with their *PalmSecure* technology enabling "wallet-free payments without the need to show IDs". This technology will initially provide real-time "ID-less authentication on a one million user scale", without a requirement for additional personal information, such as "cards or other types of information, while controlling the increase of computing resources needed for the authentication server". As an authentication method, this is by far the most secure of those reviewed; it solves all issues relating to user identification. However intelligent context-based security would still be required as merely authenticating the user may not be enough; they could been mislead or forced.

3 Recommendation

As outlined in the client specification, the authentication system used in the prototype ATM must be suitable for all residents; only half have smartphones, many have hearing difficulties, and some suffer from typical age related infirmities; these may be physical or cognitive in nature. To meet these requirements a number of design decisions were made.

Firstly, the authentication system will not use any mechanisms that rely on memory; short term memory is often impeded in older adults as noted in (Akatsu and Miki 2004). Despite graphical authentication systems being *easier* to remember, they still rely on memory and as such are still not suitable. Password and PIN complexity requirements are more likely to encourage bad practice than good security as noted in (*NIST SP 800-63 Digital Identity Guidelines* 2017) - "Humans, however, have only a limited ability to memorize complex, arbitrary secrets, so they often choose passwords that can be easily guessed". Instead of using a traditional method, the proposed authentication system will make use of multi-factor biometrics.

As reviewed in (Romanowski et al. 2016), palm vein scanners are an extremely accurate biometric authentication method; early prototypes achieved "99.45%" reliability and took a fraction of a second to process scans. Manufacturers such as Fujitsu already produce vein scanners which are used to authenticate users on some ATMs in Japan, although these systems still require the user to insert their bank card. However, as revealed in their press release, Fujitsu will soon be offering a payments system that does not require card and instead uses facial recognition in combination with their palm scanner technology -*PalmSecure* (*Fujitsu Develops Non-contact Biometric Integration Technology as an Optimal Solution for a Cashless Society* 2018). By combining multiple biometric systems an extremely accurate user identification can be made; even more so than the traditional chip and PIN method. Furthermore, foregoing chip and PIN reduces risk in that if residents didn't need cards and pins/security numbers on the back, they would have no info to provide when scam attempts are made.

The proposed authentication system for the care home ATM prototype will make use of both palm vein and facial recognition. Instead of inserting your bank card into the ATM, you stand in front of it and look at the screen; the facial recognition will partially identify you - this will effectively act as your username. Next you will will hold hold a hand above a palm vein sensor - this will serve as the password and complete the sign in authentication. Because there is no bank card to remove and because facial recognition serves as the login, the logout sequence could be triggered after the user has looked away for more than a given period of time e.g. five seconds. To reduce the chance misuse, transactions will require an additional palm vein scan to confirm. In order to make the system available to all users it should be institution agnostic; it shouldn't rely on the user being with a specific bank. To make the platform institution agnostic, the banking information of the individual would be required on sign up - this might make some users uncomfortable. A possible solution to this is to allow sign ups externally, and provide users with a one-time code they can use at the ATM to quickly register their biometric markers with their account an example of what this interface could look like can be seen in figure 3 and figure 4.

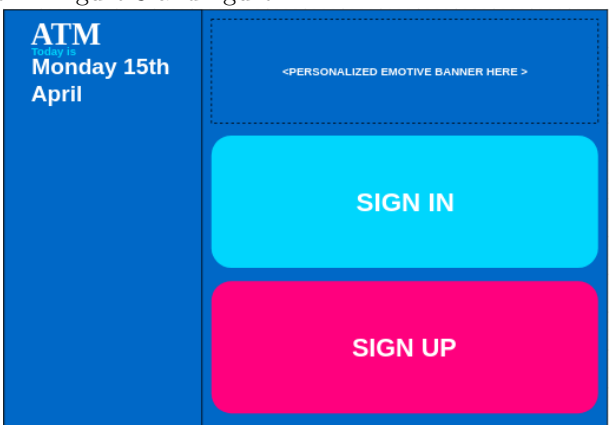

Figure 1: Primary Display (Unauthenticated)

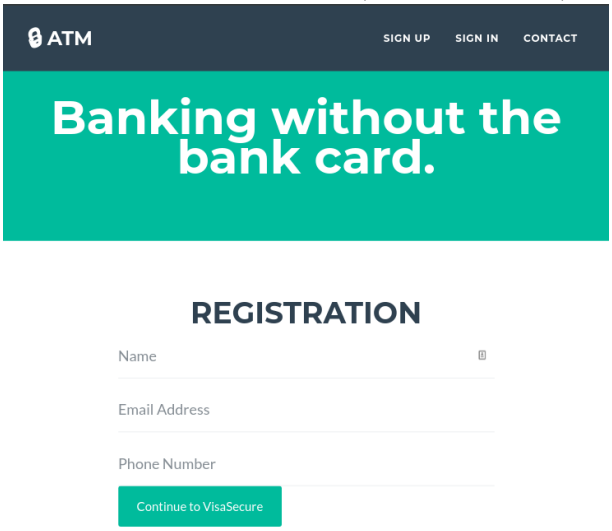

Figure 2: Bootstrap-based sign up

The registration page would be fairly simple, a modern bootstrap-based sign up form on a website that could be

accessed from a computer or mobile phone, a rough example of which can be seen in figure 2. To register their biometric markers (face and palm veins) with their account, users would enter the provided code, which would be a unique randomly generated alpha-numeric string into the ATM using an on screen keyboard. An example of what this interface could look like can be seen in figure 1. Both screens make use of very large buttons with large text, meaning it should be easy to read with bad eyesight and easy to use even with unstable hands. The colours used in the example are merely a mock-up, in the ATM itself the colours could be change on a per user basis - for instance if a user had Protanopia the pink and blues tones would be indistinguishable (*Color blindness: how to design an accessible user interface* 2018).

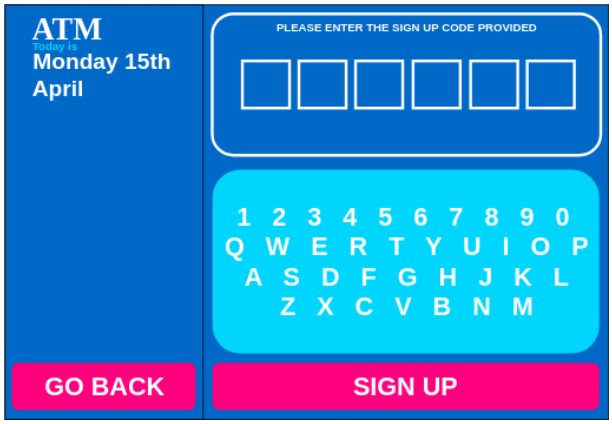

Figure 3: Sign-up With Code

The interface to actually login would be in a very similar style to the examples shown, except it would direct the user to look towards the screen and place their hand over the scanner, a mock up of this interface can be seen in figure 4. Doing so would authenticate them, and allow them to access regular ATM services - Balance check & Cash withdrawal. However, in the case of particularly vulnerable users, merely authenticating them may not be enough.

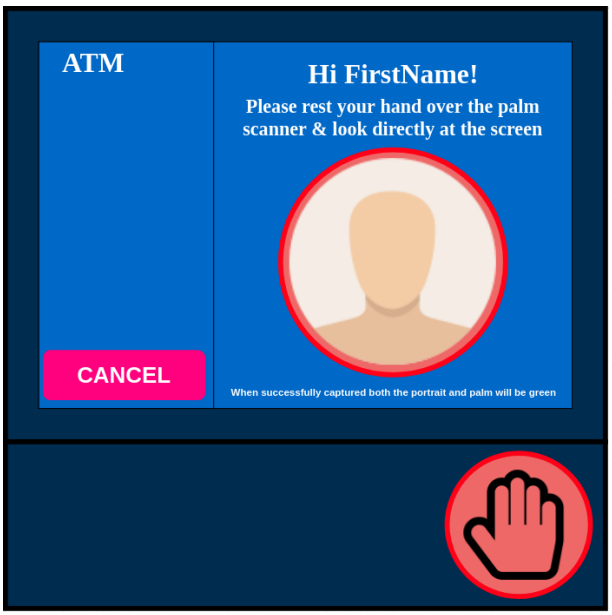

Figure 4: Authenticate user (sign-up/login)

4 Machine Learning

In network security there is a concept known as AAA (authentication, authorization, and accounting), it describes a framework that identifies, provides (or does not provide) access, and logs transactions. For particularly vulnerable residents an AAA-esque mechanism may provide financial independence with the guidance and limitations they require. A resident may physically be themselves but they could be emotionally or mentally compromised, in such situations they may pose a threat to their own finances; mislead, scammed or experiencing a moment of confusion. For residents at risk of said situations, additional security mechanisms could be added to the ATM; authorization and accounting. The banks themselves have a duty of care and should systems in place to pick up anomalous transactions (e.g. will check or block cards where unusual transactions), the proposed system does not seek to replace these systems but work in collaboration with them.

In the prototype ATM system, authorization would act as verification of a transaction. If user behaviour was outwith normal parameters, the authorization mechanism would kick in, blocking the transaction until approval was given. A potential solution to the authorization problem could be derived from (Chakraborty, Lakshminarayana and Ponnapalli 2018). In this patent, Chakraborty describes a secondary user authentication system in which "the user is authenticated based on distributed trust of a set of randomly selected trusted contacts from a large set of trusted contacts". During enrolment, multiple contacts

are selected as *affirmers* which provide the user additional authentication information required to fully authenticate. While this mechanism relates to computer systems, the principles could still be applied. For instance, the trusted contacts required during enrolment of a resident could be a member of staff and member of family. Instead of these contacts providing additional authentication information, they could provide authorization for cash withdrawals that exceed agreed limits or can otherwise be classed as abnormal. The user-user modeling discussed by Pohl in (Pohl 1996) was designed to adapt interfaces to user needs. However, it could also be used to identify normal and abnormal behaviour. For example, if a user usually withdraws cash valuing between £10 and £30 and one day tries to withdraw £100; that could be classed as abnormal behaviour, this information could then be used to drive the AAA system and the personalized *favourite withdrawals* interface as seen in figure 5. The model could either be trained with each individual residents transaction history, or by generating a 'average user' model across all the residents which could act as a base for training data. Either of these models could be used to compare current usage with expected usage; to classify transactions as 'suspicious' or 'normal'. Finally, the accounting system would provide a history of all transactions, including who (if at all) approved or denied transactions requiring authorization - which in turn makes staff and family members more accountable if trust is abused. While tracking value withdrawn might introduce accountability to some abuse of trust situations, it would not do so in the case of scammers.

Figure 5: Withdrawal (adaptive interface)

When a person is feeling a particular way, their face often displays tell-tale signs of the particular feeling or emotion. Affective computing is the way a computer can recognize, interpret or monitor emotion and/or other affective persona (Picard 1999). As the proposed system already uses facial recognition, a camera will be present; said camera could also be used with emotion recognition solution, which would in turn provide information on the state of mind a resident is in while making a transaction. If the resident appears scared, nervous or uneasy that may be a sign that they have been tricked or forced to make a withdrawal; such an event would trigger the authorization system regardless of the user settings, as anyone could be tricked, scammed or defrauded - regardless of mental or physical capability.

5 Experiment Outline

To test the usability of the recommended mechanism a number of factors should be considered. Firstly, ease of adoption - how quickly were users able to effectively use the system. There are several ways this could be measured; how quickly is a user able to complete a transaction, how often did the have to use the back button, and did they have to make any other withdrawals shortly after - this would suggest they were unable to do what they intended in a single transaction. The ease of adoption statistics would compare user usage from the first day, first week, and then the first month. This would demonstrate if the system unfamiliarity was a barrier to acceptance in the elderly residents. Across a similar time frame, the emotive response of the residents could be tracked; were they ever frustrated or upset when using the system, and was there any other user input that would suggest discontent with the system? It would also be worth asking both residents and staff if any assistance was needed when using the ATM - were they able to complete their intended transaction without help. Finally, the users would be surveyed - questions would include how they liked the ATM system and how easy the found it to use in comparison to a traditional chip and PIN ATM.

To encourage adoption of the system the benefits would be summarized; it enables financial independence, it is more secure than chip and PIN, and doesn't require any additional fancy devices or extensive training - just you. While financial independence will be a point of encouragement for users who traditionally would not be able access/manage their own finances, the benefits the research may or may not bring will likely be of little interest to unrestricted users - without some form of external motivation. The *external motivation* could take the form of a bonus starting balance, a day trip or some other form of group activity for the residents if x many people register for the ATM prototype tests.

6 Limitations & Challenges

This paper discussed the hypothetical situation where an ATM is going to be deployed in a nursing home. The elderly are a particularly challenging group to cater for especially when factoring in physical and mental health issues, and conditions that come with those including (but not limited to); difficulties remembering, a lack of patience, confusion, pain when typing, tremors, and coordination problems- all of which would make use of a traditional ATM challenging. It is worth noting that nursing homes are typically cash-free; residents paying for goods or services usually do so through their monthly direct debit which is harder to abuse than cash, however the financial independence this solution offers make it an attractive alternative. The proposed solution is not the be all, end all solution to financial independence issues faced by residents, for example anyone with Dementia/mental incapacity is unlikely to be able to have full financial independence and an ATM can't change that, but it can at least provide a partial solution through its use of authentication, authorization, accounting (AAA) and card-less authentication.

As intelligence in older adults is different, the solution must be specially tailored for their needs to ease adoption and continual use. In making everyday decisions older adults cope well with the familiar, but may struggle to use systems which require new ways of thinking (Cavanaugh and Blanchard-Fields 2018), maintaining attention (Stankov 1988), or rely on short-term memory (Akatsu and Miki 2004). The obvious solution to this problem is to remove the thinking, remembering, concentrating part of the process and use some form of biometrics to access the system. Additionally, through the use of biometrics there is less of a learning curve as the resident only needs to present their palm and look towards the screen; there is little to confuse or complicate which should minimise resistance to the new technology.

It may be argued that biometrics only provide identification, not authorization. Currently the chip and PIN method does not provide identification - there is currently no way to prove that the person using the card is the owner. The backbone of the proposed ATM system is the reliance on extremely accurate identification - can say without doubt that a specified person is interacting with the ATM. This identification method in combination with the machine learning based user modeling, *AAA* and user emotion tracking provides a solution that is not only protected against malpractice within the care home, but also malicious intent outwith - be that phishing scams -such as the HRMC tax scams (*Examples of HMRC related phishing emails and bogus contact*), or even family and *friends* seeking to take advantage of the individual. That being said, no system is perfect; there may be some false positives - innocent transactions flagged as suspicious, however, it is better to have false positives than false negatives when dealing with financial security.

Proving ease of use may be quite time consuming - especially when seeking feedback from the users. That being said, the user-user modeling system could provide detailed interaction history for each user which would in turn provide continual feedback to both the dynamic interface and the research team; morphing the interface into one that better meets that users needs and supplying critical information on the user interaction - for example, if something didn't work as expected - what *specifically* went wrong?

With support from companies like Fujitsu and commercial role out estimated for 2020 (*Fujitsu Develops Non-contact Biometric Integration Technology as an Optimal Solution for a Cashless Society* 2018), palm vein and 3D facial recognition is a combination that is already used elsewhere in the world (Japan) to authorize transactions. As such the technology is easy and cheap to source - some consumer grade laptops now implement small palm vein scanners, making it good not just for the residents, but also for the ATM designer. With the immense ease of access improvements over traditional chip + PIN and no memory requirements à la graphical systems, the proposed solution is the perfect choice for a care home ATM system.

7 References

Abuse and neglect of vulnerable adults (2018). URL: `https://www.nhs.uk/conditions/social-care-and-support-guide/help-from-social-services-and-charities/abuse-and-neglect-vulnerable-adults/`.

Akatsu, Hiroko and Hiroyuki Miki (2004). 'Usability research for the elderly people'. In: *Oki Technical Review (Special Issue on Human Friendly Technologies)* 71.3, pp. 54–57.

Bilgi, Basak and Bulent Tugrul (2018). 'A Shoulder-Surfing Resistant Graphical Authentication Method'. In: *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*. IEEE, pp. 1–4.

Cavanaugh, John C and Fredda Blanchard-Fields (2018). *Adult development and aging*. Cengage Learning.

Chakraborty, Pinak, Nagasubramanya Lakshminarayana and Harigopal KB Ponnapalli (2018). *Distributed Trust as Secondary Authentication Mechanism*. US Patent App. 15/277,590.

Color blindness: how to design an accessible user interface (2018). URL: https://uxdesign.cc/color-blindness-in-user-interfaces-66c27331b858.

EmmahThomas, Victor, Taylor Onate Egerton and Matthias Daniel. 'Multimodal Biometrics: A Measure for Enhancing Authentication'. In:

Examples of HMRC related phishing emails and bogus contact. URL: https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-and-customs-examples.

Fraud Against Seniors (2016). URL: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/seniors.

Fujitsu Develops Non-contact Biometric Integration Technology as an Optimal Solution for a Cashless Society (2018). URL: https://www.fujitsu.com/global/about/resources/news/press-releases/2018/1004-01.html.

Hawthorn, Dan (2000). 'Possible implications of aging for interface designers'. In: *Interacting with computers* 12.5, pp. 507–528.

Kono, Miyuki et al. (2015). 'Personal Authentication Analysis Using Finger-Vein Patterns in Patients with Connective Tissue Diseases—Possible Association with Vascular Disease and Seasonal Change'. In: *PloS one* 10.12, e0144952.

NIST SP 800-63 Digital Identity Guidelines (2017). URL: https://pages.nist.gov/800-63-3/.

Older people: independence and mental wellbeing (2015). URL: https://www.nice.org.uk/guidance/ng32/resources/older-people-independence-and-mental-wellbeing-pdf-1837389003973.

Overview of the UK population: November 2018 (2018). URL: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/overviewoftheukpopulation/november2018.

Picard, Rosalind W (1999). 'Affective Computing for HCI.' In: *HCI (1)*. Citeseer, pp. 829–833.

plc, Aviva (2017). *UK: Over 1m over-45s have fallen victim to online scams as one in five feel vulnerable under the march of technology*. URL: https://www.aviva.com/newsroom/news-releases/2017/01/uk-over-1m-over-45s-have-fallen-victim-to-online-scams-as-one-in-five-feel-vulnerable-under-the-march-of-technology-17719/.

Pohl, Wolfgang (1996). 'Learning about the user–user modeling and machine learning'. In: *ICML*. Vol. 96, pp. 29–40.

Renaud, Karen and Judith Ramsay (2007). 'Now what was that password again? A more flexible way of identifying and authenticating our seniors'. In: *Behaviour & Information Technology* 26.4, pp. 309–322.

Romanowski, Joseph et al. (2016). 'A Biometric Security Acceptability and Ease-of-Use Study on a Palm Vein Scanner'. In: *Proceedings of Student-Faculty Research Day, CSIS, Pace University*.

Salthouse, TA, JE Birren and KW Schaie (1985). 'Speed of behavior and its implications for cognition, in Handbook of the Psychology of Aging'. In: *D. Van Nostrand, New York, NY, USA*.

Stankov, Lazar (1988). 'Aging, attention, and intelligence.' In: *Psychology and Aging* 3.1, p. 59.

Suru, Hassan U et al. (2018). 'Security and usability in a hybrid property based graphical authentication system'. PhD thesis. University of Salford.