LCS_PCOM7E August 2023 End of Module Assignment
30 October 2023 Word Count: 2,012

NEC's Face Recognition Technology as Used in My Number IDs: Benefits, Drawbacks, and Proposed Technologies For Improvement

Background

Business and commerce done digitally, according to the Financial Action Task Force (FATF), have seen an annual growth of 12.7% (Slavin, 2023). One example of this is the utilisation of My Number digital identification (ID) cards in Japan. The Japanese government has been rolling out digital My Number cards, a 12-digit identification that holds details of Japanese citizens and residents, in order to centralise government services such as taxation and social security, since 2016 (Fee, 2022). Currently, it is estimated by Kyodo News (2023) that 71%, which is roughly 89 million individuals, have acquired the aforementioned ID in Japan. The Japan Agency for Local Authority Information Sytems (J-LIS) (N.D.) informs us that the IC chips in the ID store not just the photograph, but also the name, domicile, birthday, and sex of the holder. They go on to say that it can be used for availing administrative services, personal authentication, and online document applications.

Selected Organisation

NEC Corporation (NEC), a company established in 1899 and whose headquarters is in Tokyo, lists IT service as one of its main business functions (NEC, N.D.). According to Forbes (N.D.), NEC supplies hardware and software technology, as well as

solves Information Technology (I.T.) problems of various fields like that of the service industry. To confirm the identity of a My Number ID holder, Komatsu et al. (2019: 33) informs us that NEC provides J-LIS the Face Recognition Technology (Face Recognition), which is recorded in its IC chip. IC chips, which hold the data in the My Number, are defined by Rouse (2014) as the foundation of gadgets and machines, made out of “fabricated transistors, resistors, and capacitors” that are stored in a tiny chip.

Adapting Face Recognition Technology for eKYC

Ever since NEC implemented the use of Face Recognition for use in the finance sector, it has simplified identity verification over the internet called the electronic Know Your Customer (eKYC) (Shimizu et al., 2021). They also mention how this process has been particularly useful during COVID-19, when face-to-face medical appointments were difficult, but online consultations were made possible just by providing the My Number card of an individual. Takaragi et al. (2023) explains that eKYC is the process of handling and disclosing data of persons to businesses for various transactions. They also add that these profiles can be stored in certificates and national IDs. Arner et al. (2019:56) sums up eKYCs as the “online footprint” and “identification[...]converted into an electronic form[...]” of a person.

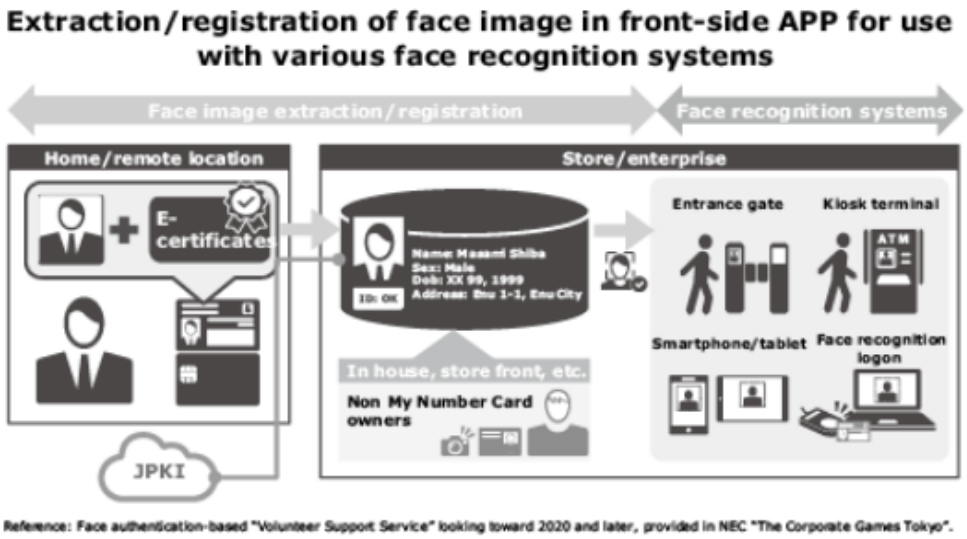

Figure 1: This figure simplifies when and where the Face Recognition Technology of NEC can be used (Komatsu et al., 2019)

Benefits of Face Recognition

M. Watanabe (2021) states some benefits of NEC's Face Recognition technology, such as the ease of bank enrolment and "purse-free payments" during shopping, when one only has to show his or her face for identification confirmation. In addition, Gallagher (2021) exemplified how the technology can be used to enhance security in establishment and building entrances. Another benefit of Face Recognition technology is the ease of applying for a My Number card, which can be sent online instead of by traditional mail (Udagawa et al., 2017). This fact is supported by Takaragi et al. (2023), as they emphasise the practicality that eKYC has brought to filing documents virtually. The COVID-19 pandemic also hastened the development and proved the efficacy of Face Recognition technology, since they are able to recognise people despite masks being worn over the face during verification, just by focusing on the exposed areas

around the eyes (Gallagher, 2021). Overall, it has made not just applications, but also verification of personal digital identity, convenient and practical.

Drawbacks of Face Recognition

Udagawa et al. (2017) explains personal data being compromised by malicious attackers as one of the drawbacks that may occur when gathering My Number photos. Slavin (2023) also mentions the misuse of identity once it is stolen, for example, in availing services unbeknownst to the original ID holder. In fact, Do et al. (2022) states that videos and pictures can be maliciously used to override the security of Face Recognition technologies during confirmation of identity or application filing. This raises a cause for alarm since as mentioned earlier, the face data of users are stored in My Number.

Data Privacy Concerns with My Number

It is therefore important to note that privacy and cybersecurity issues have been sparking concerns for the My Number recently. Exum (2023) reports that the details of 7,312 persons were wrongly linked to someone else from the months between October 2021 to November 2022. This also happened with the medical records of several citizens and residents (Kyodo News, 2023). We learn from The Asahi Shimbun (2023) that other people can retrieve these private data, which has lead to the bearers surrendering their IDs due to them losing confidence with the system. Therefore, we can conclude that the IC chip of the MyNumber, which also stores the face authentication system provided by NEC, is vulnerable due to the aforementioned exposures to outside threats. As a consequence, personal information of My Number ID holders are susceptible to data leakage or mishandling.

Proposed Technologies

In order to strengthen the cybersecurity of the My Number cards that hold valuable personal data such as the photo and information of Japanese citizens and residents, a combination of two technologies are hereby proposed. First, is by making use of the mobile app called Sora Identity System (Sora). It is explained by Takemiya and Vanieiev (2018) as a blockchain built on Hyperledger Iroha that gives users the liberty and freedom of choice on what data to create and share about themselves. Panait et al. (2020) indicate that in order to avert misplacing keys, they are concealed in a central server, and that in the blockchain, user-generated cached keys and salted hash are stored. The password selected by the user consists of 8 figures that mix numbers and capitalisation of letters (Kaneriya & Patel, 2020). This was one dilemma with The My Number, as H.R. Watanabe (2021) discusses how ID holders did not have the capability to replace forgotten passwords online when they were applying for the COVID-19 cash handout from the Japanese government.

Having this kind of control over their digital identity will most probably regain the trust of My Number users, as they can choose what information to divulge during different transactions. For example, if they need a residence certificate, only their address will be revealed. No other unnecessary information has to be printed out. This is supported by Kaneriya and Patel (2020), when they mentioned that Sora enables users to separate the information they want to share to various enterprises or government agencies.

Second, is the solution that Do et al. (2022) are proposing, which is embedding a series of tests that would require a variety of expressive face movements, such as looking up and blinking, during application and confirmation of identity to combat Deepfakes. Almars (2021) describes Deepfake as the doctored videos and photographs generated by Deep Learning (DL) technology that can easily deceive the viewer of that media. This Facial Recognition Test, which serves as an identity authenticator, can add extra security whenever the My Number is being used. These test prompts will be given at random, different during each validation. This authentication must be run for all kinds of transactions to ensure data privacy and security.

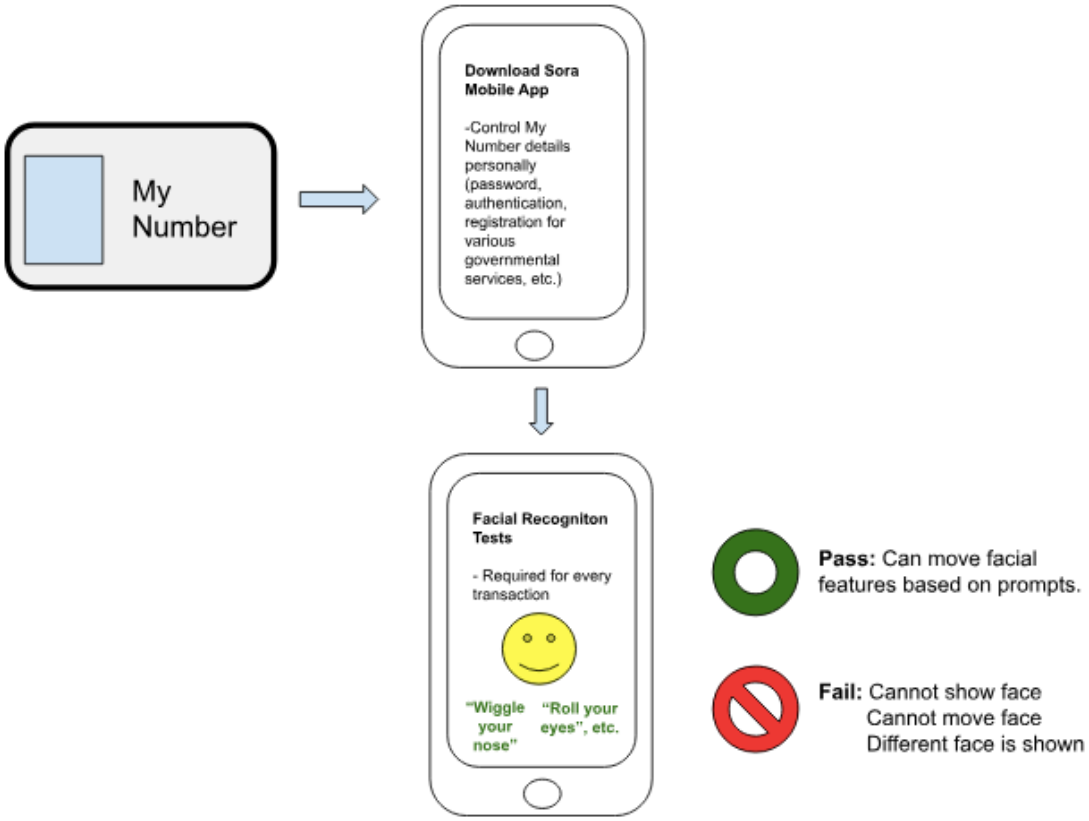

Figure 2: Proposal of downloading Sora Mobile App that is connected to My Number, enhanced with Facial Recognition Tests

The Technology-Organization-Environment (TOE) Framework, as we discover from Park and Choi (2019), point out that the aforementioned words that stand for T, O, and E, are what constitutes adaptation to technological advances. On the other hand, Diffusion of Innovation Theory (DoI) characterises that even though the acceptance of humans to innovations come in different waves, they would eventually come to accept and use them in due course (Turin et al., 2023).

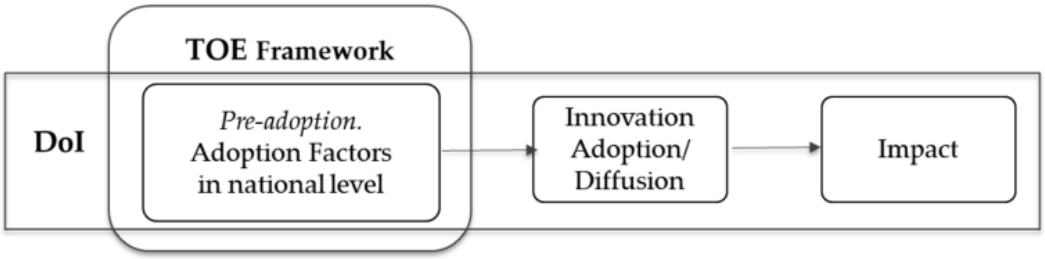

Figure 3: Incorporating DoI and TOE Framework (Park & Choi, 2019)

It is therefore recommended for NEC, in cooperation with J-LIS, to incorporate these two models proposed by Park and Choi (2019) to promote confidence in the use of Face Recognition and My Number Cards. The process would then be: 1) Pre-adoption: Connecting Sora to My Number that is secured with Facial Recognition Tests, 2) Diffusion: Japanese My Number individuals downloading Sora Mobile App that would enable them to control their digital identity when using the ID, and 3) Impact: Trust in the My Number system will be gained, which would entail more users acquiring the ID, resulting in e-Governance efficacy in Japan.

Challenges to The Proposed Technologies

A possible challenge to the expressive Facial Recognition Test is Deepfake. The development of Deepfake at this time is meteoric. Humans have to be more wary and discerning as they can be greatly misused and abused in order to distort the truth and spread lies, though it is important to take note they are not always used negatively (Rafique et al., 2023). For Sora, Panait et al. (2020) discuss that decentralisation is difficult due to their location in the central server. This agrees with the report of Slavin (2023), who values the decentralisation of digital IDs, because it can successfully give users full control of their personal information. Lastly, Kaneriya and Patel (2020) also point out that passwords chosen by the user are susceptible to hacking.

Recommendations to Protect The Proposed Technologies from Challenges

Despite generating Deepfake, Deep Learning, according to Almars (2021) can be used to identify when it acts as a threat, as it is a type of machine learning that gathers raw and unlimited hidden layers producing sophisticated results. According to Conrad (2023), a DL model that is often used in examining graphics, photographs, and videos is The Convolutional Neural Network (CNN). Its cutting-edge technology yields both the high and low level attributes of the database, enabling it to master characteristics and reduce the photographic layers it collects (Rafique et al., 2023). The two stages CNN undergoes when catching Deepfakes according to Ding et al. (2020, as cited in Rana et al., 2022: 25506) are: 1) using both real and false photographs to select certain characteristics from compacted layers that contain fake media, and 2) analysing the legitimacy of the media after deep learning.

Beyond the Face Recognition Technology of NEC, improving the security of the IC chip in My Number IDs can also be discussed in future research. One recommendation is from Nagata et al. (2022), stating that attacks can be discerned using on-chip circuits that are specifically designed for looking out for threats. This entails the hardware side of the ID. Securing IC chips from external attacks is important in enhancing the overall security of My Number.

Conclusion

The Face Recognition Technology of NEC is groundbreaking in authenticating personal data online. Digital applications and transactions can be processed efficiently, and these benefit not just the individual, but also various government agencies and business sectors. Its practicality was even more evident during the advent of COVID-19, when in-person transactions were sometimes impossible. In Japan, they have a national ID that is referred to as My Number. It streamlines digital applications and identity verifications. NEC provides the Face Recognition in My Number, which is stored in its IC chip, for personal identity validation. Unfortunately, cybersecurity issues such as data leakage, have been plaguing the IDs as of late. In order to protect the digital persona of those enroled in the My Number, Sora Identity Mobile App with an integrated Facial Recognition Test, is the technology proposed by the author. It adapts the combination of the Diffusion of Innovation and Technology-Organization-Environment Framework. However, this proposed solution has potential challenges, such as the threat of Deepfake during face authentication. Therefore, adding security measures in My Number, an example of which is integrating on-chip circuits that look out for threats in IC chips, can be considered for future developments to the proposed technology.

References:

Almars, A.M. (2021) Deepfakes Detection Techniques Using Deep Learning: A Survey. *Journal of Computer and Communications.* 9(5): 20-35. DOI: https://doi.org/10.4236/jcc.2021.95003.

Arner, D.W., Zetzsche, D.A., Buckley, R.P. & Barberis, J.N. (2019) The Identity Challenge in Finance: From Analogue Identity to Digitized Identification of Digital KYC Utilities. *European Business Organization Law Review* 20:55-80. DOI: https://doi.org/10.1007/s40804-019-00135-1.

Conrad, D. (2023) A Machine Learning Approach to Deepfake Detection. Bachelor of Science Thesis, Minnesota State University. Available from: https://cornerstone.lib.mnsu.edu/cgi/viewcontent.cgi?article=1005&context=undergrad-theses-capstones-all [Accessed 29 October 2023].

Do, T.L., Tran, M.K., Nguyen, H.H. & Tran, M.T. (2022) Potential Attacks of DeepFake on eKYC Systems and Remedy for eKYC with DeepFake Detection Using Two-Stream Network of Facial Appearance and Motion Features. *SN Computer Science* 3(464). DOI: https://doi-org.uniessexlib.idm.oclc.org/10.1007/s42979-022-01364-x.

Exum, A.O. (2023) Fujitsu halts residence certificate system as issues over My Number cards mount. Available from: https://www.japantimes.co.jp/news/2023/06/30/national/my-number-cards-fujitsu-system/ [Accessed 5 September 2023].

Fee, W. (2022) The government wants you to get a My Number Card. Should you? Available from: https://www.japantimes.co.jp/news/2022/10/23/national/my-number-card-explainer/ [Accessed 5 September 2023].

Forbes. (N.D.) NEC. Available from https://www.forbes.com/companies/nec/?sh=27dd0da91575. [Accessed 24 October 2023].

Gallagher, C. (2021) Masks no obstacle for new NEC facial recognition system. Available from: https://www.reuters.com/article/us-health-coronavirus-japan-facial-recog-idUKKBN29C0JZ [Accessed 27 October 2023].

Kaneriya, J. & Patel, H. (2020) A Comparative Survey on Blockchain Based Self Sovereign Identity System. *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS).* Thoothukudi, India, 2020. IEEE. 1150-1155. DOI: http://dx.doi.org/10.1109/ICISS49785.2020.9315899.

Komatsu, M., Sakamoto, S., Nakano, T., Enomoto, K., Igarashi, N., Tsukamoto, S. & Maeda, N. (2019). Use of Face Authentication Systems Associated with the " My Number Card." *NEC Technical Journal* 13(2): 33-36. Available from: https://www.nec.com/en/global/techrep/journal/g18/n02/pdf/180207.pdf [Accessed 27 October 2023].

Kyodo News (2023) Japan PM calls for review of all "My Number" card data by end of Nov. Available from: https://english.kyodonews.net/news/2023/08/c71f87aebf48-japan-pm-calls-for-review-of-all-my-number-card-data-by-end-of-nov.html [Accessed 5 September 2023].

Nagata, M., Miki, T. & Miura, N. (2022) Physical Attack Protection Techniques for IC Chip Level Hardware Security. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 30(1): 5-14. DOI: https://ieeexplore.ieee.org/document/9424027/.

NEC. (N.D.) Profile: Corporate profile. Available from: https://www.nec.com/en/global/about/profile.html [Accessed 24 October 2023].

Panait, A.E., Olimid, R.F. & Stefanescu, A. (2020). Identity Management on Blockhain-Privacy and Security Aspects. *Proceedings of the Romanian Academy, Series A* 21(1): 45-52. Available from: https://academiaromana.ro/sectii2002/proceedings/doc2020-1/06-Panait.pdf [Accessed 27 October 2023].

Park, H.J. & Choi, S.O. (2019) Digital Innovation Adoption and Its Economic Impact Focused on Path Analaysis at National Level. *Journal of Open Innovation: Technology, Market, and Complexity* 5(56). DOI: http://dx.doi.org/10.3390/joitmc5030056.

Rafique, R., Gantassi, R., Amin, R., Frnda, J., Mustapha, A. & Alshehri, A.H. (2023) Deep fake detection and classification using error-level analysis and deep learning. *Scientific Reports* 13(7422). DOI: https://doi.org/10.1038/s41598-023-34629-3.

Rana, M.S., Nobi, M.N., Murali, B. & Sung, A.H. (2022) Deepfake Detection: A Systematic Literature Review. *IEEE Access* 10: 25494-25513. DOI: http://dx.doi.org/10.1109/ACCESS.2022.3154404.

Rouse, M. (2014) Integrated Circuit. Available from: https://www.techopedia.com/definition/2366/integrated-circuit-ic [Accessed 27 October 2023].

Shimizu, T., Miyakawa, K., Ooishi, M., Toriyama, S., Arai, M. & Horiuchi K. (2021) NEC'S Online Personal Identification Service Accelerates Innovations Toward New Normal Era. *NEC Technical Journal* 15 (1): 119-123. Available from: https://www.nec.-com/en/global/techrep/journal/g20/n01/200122.html [Accessed 9 September 2023].

Slavin, A. (2023) *Reimagining Digital ID.* Cologny/Geneva, Switzerland: World Economic Forum. Available from https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf [Accessed 27 October 2023].

Takaragi, K., Kubota, T., Wohlgemuth, S., Umezawa, K., & Koyanagi, H.(2023) Secure Revocation Features in eKYC - Privacy Protection in Central Bank Digital Currency. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.* E106-A (3): 325-332. DOI: https://doi.org/10.1587/transfun.2022CIP0008.

Takemiya, M. & Vanieiev, B. (2018) Sora Identity: Secure, Digital Identity on the Blockchain. *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC).* Tokyo, Japan, 2018. IEEE. 582-587. DOI: 10.1109/COMPSAC.2018.10299.

The Asahi Shimbun (2023) Many returning cards in problem-plagued My Number system. Available from: https://www.asahi.com/ajw/articles/14947254
[Accessed 5 September 2023].

The Japan Agency for Local Authority Information Systems. (N.D.) About an Individual Number Card. Available from https://www.kojinbango-card.go.jp/en-kojinbango/ [Accessed 27 October 2023].

Turin, T.C., Kazi, M., Rumana, N., Lasker, M.A.A. & Chowdhury, N. (2023) Employing diffusion of innovation theory for 'not missing the mass' in community-engaged research. *BMJ Open* 13(e069680). DOI: http://dx.doi.org/10.1136/bmjopen-2022-069680.

Udagawa, H., Masuda, T., Iwamoto, K. & Akiyama, T. (2017) "My Number" Collection Service Utilizes Several Key Image Recognition Technologies. *NEC Technical Journal* 12(1): 78-82. Available from: https://www.nec.com/en/global/techrep/journal/g17/n01/pdf/170116.pdf [Accessed 27 October 2023].

Watanabe, H.R. (2021) Coronavirus Pandemic and Online Services in Japan: Urgent Need for Digitalization. 産研論集（関西学院大学）48:37-46. Available from: https://www.academia.edu/90083138/Coronavirus_Pandemic_and_Online_Services_in_Japan_Urgent_Need_for_Digitalization [Accessed 29 October 2023].

Watanabe, M. (2021) Approach to Digital Finance in DX Era. *NEC Technical Journal* 15(1): 116-118. Available from: https://www.nec.com/en/global/techrep/journal/g20/n01/pdf/200121.pdf [Accessed 27 October 2023].