Slide 1 - Title (NO AUDIO)

Slide 2 - Research Problem (AUDIO)

Our daily lives now cannot function without mobile gadgets. We use mobile gadgets to access private information, perform transactions, and communicate with others. These daily activities associated with mobile devices raise security and privacy concerns. Authenticating mobile devices to ensure maximum security is one of the major issues. For decades, safeguarding mobile devices has relied on conventional authentication methods like passwords and PINs (Patel et al., 2016, P 54). If a device is lost or stolen, they are only sometimes successful in preventing unauthorized access. Additionally, people frequently select weak passwords that are simple to guess, which jeopardizes the security of their devices.

Continuous user authentication is a new strategy that can improve mobile device security and privacy. As consumers use their devices, this security feature continuously verifies their identities. This procedure can use various techniques, including biometric authentication, behavioral authentication, and location-based authentication. Compared to conventional authentication methods, continuous user authentication can offer mobile device users higher security and privacy (Feng et al., 2012, P 454). The importance of this research rests in its contribution to the creation of a mobile device authentication method that is more secure and enhances privacy. This study aims to design a continuous user authentication model for mobile devices and examine the efficacy of continuous user authentication techniques. This model will be created to overcome the drawbacks of conventional authentication procedures and offer mobile device users higher security and privacy (Mombeuil and Uhde, 2021 P 102384).

By examining the efficacy of continuous user authentication as a security technique, this research will contribute to the broader field of cybersecurity. The results of this study will offer

information about how well continuous user authentication improves user security and privacy, which can help developers of other systems and apps create security measures (Ismagilova et al., 2020, P 8). The study will also shed light on user attitudes and views of continuous authentication. User authentication must be well received by users to be successfully implemented. Therefore, it is crucial to understand user attitudes and views of this method to create effective continuous user authentication models that mobile device users widely embrace. Additionally, this research will help develop ethical considerations for continuous user authentication design and implementation. Continuous user authentication can improve security and privacy and raise questions about collecting and using user data (Martínez-Pérez et al., 2015, P 6). This study will examine the moral ramifications of continuous user authentication and offer recommendations for its ethical application.

Slide 3 - Research Questions (AUDIO)

1. How can users' security and privacy be improved by implementing continuous user authentication on mobile devices?
2. What continuous user authentication techniques improve mobile device security and privacy most?
3. What are the moral ramifications of continuous user authentication, and how many rules for its proper application are created?
4. In terms of security and user experience, how effective is continuous user authentication as a mobile device security mechanism, and how does it compare to more conventional authentication methods?

Slide 4 – Objectives (AUDIO)

This research investigates continuous user authentication's effectiveness in enhancing mobile device users' security and privacy. To achieve this aim, the following specific objectives will be pursued:

1. To review existing literature on continuous user authentication for mobile devices.
2. To evaluate the effectiveness of existing continuous user authentication methods.
3. To develop and test a continuous user authentication model for mobile devices.
4. To evaluate the developed model's effectiveness in enhancing mobile device users' security and privacy.

Slide 5 - Literature review (AUDIO)

The literature review will cover the following topics

Mobile device security and privacy risks.

Since mobile devices have become essential to daily life, they now hold sensitive financial and personal data. Security and privacy issues have increased along with the popularity of mobile devices. These dangers include losing or stealing a device, malware infections, phishing attempts, and unauthorized access to sensitive information (Jose and Rajasree, 2023, P 1360).

Traditional authentication measures and their limitations.

Mobile device security has long been achieved via conventional authentication methods like passwords, PINs, and biometrics. The drawbacks of these security measures include the potential for password forgetfulness, weak passwords, and the theft or duplication of biometric data. These methods do not continuously authenticate the user; they simply offer authentication at the point of admission (Chin et al., 2012, P 8).

Continuous user authentication methods and their effectiveness.

The shortcomings of conventional authentication techniques are intended to be addressed by continuous user authentication approaches. These techniques constantly authenticate the user through location, activity, and behavioral biometrics. This strategy lowers the possibility of illegal access to personal data while enhancing user security and convenience (Skalkos et al., 2021, P 748).

Mobile device security and privacy regulations and standards.

Communication institutions have created standards and laws for mobile device security and privacy to address their associated dangers. Personal data is protected by implementing security and privacy measures guided by specific laws and regulations (Sicari et al., 2015, P 254). General Data Protection Regulation (GDPR) is an example of these regulations and standards. Another example of these regulations is the National Institute of Standards and Technology (NIST).

User attitudes and perceptions towards continuous user authentication.

The acceptance of continuous user authentication by users and how they view it are key factors in the success of such methods. Users could be worried about how their personal information is collected and used, how it affects battery life, and how inconvenient it is to verify themselves constantly. In order to create continuous user authentication models that are user-friendly, safe, and privacy-preserving, it is essential to understand these attitudes and perceptions (Shabtai et al., 2010, P 38).

Slide 6 - Research Methodology (AUDIO)

The primary foundation of the research approach for this study will be a quantitative research design. Using this strategy, we can gather numerical data that can be statistically examined to

find trends, patterns, and connections between variables. We will carry out a survey using an online questionnaire to gather data. Users of mobile devices who are willing to participate in the survey will receive the questionnaire (Abomhara and Køien, 2014, P 6). Data on user attitudes and perceptions of continuous user authentication, mobile device security and privacy hazards, and user demographics will be gathered through the poll.

Google Forms permits convenient survey dissemination to participants via email or social media. With an estimated completion time of about fifteen-twenty minutes for respondents and complete confidentiality assured throughout the process, it is hoped that participants will provide open and truthful feedback via the survey. The survey questions will be created to guarantee that all facets of the study questions are covered. According to La Polla et al. (2012 P 454), conducting a preliminary test with a limited number of participants is important to ensure clarity and accuracy while designing surveys. SPSS and Excel are among the software tools we will employ to study our collected data. A summary report containing descriptive statistics, including means and standard deviations for frequencies, is what we will arrive at after analyzing the data. Regression analysis and ANOVA are examples of inferential statistics that will be used to determine relationships between variables.

A thorough analysis of the literature pertinent to the study issues will also be done. To identify significant research papers, our approach involves conducting a systematic review by searching through various electronic databases such as Google Scholar, Scopus, and Web of Science, and our research focuses on exploring the potential dangers posed by issues like continuous user authentication and mobile device security as they relate to privacy risks. In order to find other pertinent studies, we will also consult the reference lists of the publications we have already found (Patel et al., 2016, P 54). To guarantee that all relevant studies are located and thoroughly

scrutinized during the literature review process, they will be conducted methodically and meticulously.

A comprehensive evaluation of rules relating to mobile device safety measures within the target region shall involve reviewing relevant standards, particularly those that are stipulated under General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIDEPA), in addition to California Consumer Privacy Act (CCPA), and conclusion, we aim to obtain thorough knowledge regarding the perceptions and beliefs held among members belonging from group(s) using mobile devices via conducting semi-formal interviews for collecting as well as doing analysis on qualitative information which would be our final phase (Feng et al., 2012 P 454). The data from these interviews will be transcribed and analyzed using qualitative analytic tools like NVivo, whether the interviews are performed in person or by video conferencing.

Slide 7 - Ethical Considerations and Risk Assessment (AUDIO)

Addressing risk assessment and ethical considerations is crucial to ensure the welfare and security of study participants in any research project. This research assesses how effective continuous user authentication methods are at improving mobile device security and privacy measures. Risk assessment and the ensuing ethical issues will be taken into account:

Participants will get information about the research study and its goals before enrolling. Before data is gathered, they will be requested for written consent.

Privacy: Participants' privacy will be respected and maintained throughout the study. To protect the participants' privacy, all information gathered will be kept confidential and anonymous (Chin et al., 2012, P 8).

Data Protection: Following GDPR legislation and university data protection policies, the data gathered for this project will be maintained and secured. The final data analysis will not contain any information that might be used to identify participants (Sicari et al., 2015, P 154).

Risk Assessment: Study-related risks will be evaluated and handled to minimize injury to study participants. The primary dangers of this study are the possibility of a privacy invasion and the potential for unauthorized access to participants' personal information. Following data protection laws, preserving data security and confidentiality, and getting participants' informed consent will reduce these dangers (Ismagilova et al., 2020, P 8).

Ethical Approval: The appropriate ethical committee will be consulted before the study is carried out to obtain ethics approval. The research team will ensure that the study complies with the ethical criteria established by the committee and will alter it as necessary (Chin et al., 2012, P 8).

Slide 8 - Description of artifact (s) (AUDIO)

The main goal of this study is to determine how well continuous user authentication techniques may increase the security and privacy of mobile devices. However, no specific artifact will be produced due to this research. However, the study will produce fresh information and new perspectives on how well continuous user authentication techniques protect the privacy and security of mobile devices (Ismagilova et al., 2020, P 8). This information will support the research on mobile device security and privacy and educate users, device manufacturers, and regulators about the value of continuous user authentication techniques.

The study may also recommend deploying successful continuous user authentication techniques in mobile devices. For consumers, device manufacturers, or legislators, this can entail the creation of standards, best practices, or recommendations. These outputs, which will be based on

the study's findings, could help a larger audience by improving the security and privacy of mobile devices (Ismagilova et al., 2020, P 8).

In conclusion, mobile device use has ingrained itself into our daily lives, bringing security and privacy issues. Once effective authentication techniques, passwords and PINs are no longer adequate to safeguard sensitive data on mobile devices. The use of continuous user authentication, which constantly verifies the user's identity and provides a greater level of security and privacy, is suggested by this study. The study aims to create and assess the efficacy of a continuous user authentication model for mobile devices and to look at the moral ramifications and user perceptions of this strategy. The findings of this study can benefit the larger field of cybersecurity and aid programmers in developing more private and secure mobile device authentication techniques.

Slide 9 - Timeline of proposed activities (Audio)

The proposed timeline for the research is as follows.

The timeline may be subject to change depending on unforeseen circumstances.

Slide 10 - Timeline of proposed activities (NO AUDIO)

References List

Abomhara, M. and Køien, G.M., 2014, May, 'Security and privacy in the Internet of Things: Current status and open issues', In *2014 international conference on privacy and security in mobile systems (PRISMS)* (pp. 1-8). IEEE.

Chin, E., Felt, A.P., Sekar, V. and Wagner, D., 2012, July, 'We are measuring user confidence in smartphone security and privacy', In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-16).

Feng, T., Liu, Z., Kwon, K.A., Shi, W., Carbunar, B., Jiang, Y. and Nguyen, N., 2012, November, 'Continuous mobile authentication using touchscreen gestures', In *2012 IEEE conference on technologies for homeland security (HST)* (pp. 451-456). IEEE.

Ismagilova, E., Hughes, L., Rana, N.P. and Dwivedi, Y.K., 2020, 'Security, privacy, and risks within smart cities: Literature review and development of a smart city interaction framework', *Information Systems Frontiers*, pp.1-22.

Jose, C.J. and Rajasree, M.S., 2023, 'Implicit Continuous User Authentication for Mobile Devices Based on Deep Reinforcement Learning', *COMPUTER SYSTEMS SCIENCE AND ENGINEERING*, *44*(2), pp.1357-1372.

La Polla, M., Martinelli, F. and Sgandurra, D., 2012, 'A survey on security for mobile devices', *IEEE communications surveys & Tutorials*, *15*(1), pp.446-471.

Martínez-Pérez, B., De La Torre-Díez, I. and López-Coronado, M., 2015, 'Privacy and security in mobile health apps: a review and recommendations', *Journal of medical systems*, *39*, pp.1-8.

Mombeuil, C. and Uhde, H., 2021, 'Relative convenience, relative advantage, perceived security, perceived privacy, and continuous use intention of China's WeChat Pay: A mixed-method two-phase design study', *Journal of Retailing and Consumer Services*, *59*, p.102384.

Patel, V.M., Chellappa, R., Chandra, D. and Barbello, B., 2016, 'Continuous user authentication on mobile devices: Recent progress and remaining challenges', *IEEE Signal Processing Magazine*, *33*(4), pp.49-61.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S. and Glezer, C., 2010, 'Google Android: A comprehensive security assessment', *IEEE Security & Privacy*, *8*(2), pp.35-44.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A., 2015, 'Security, privacy, and trust in Internet of Things: The road ahead', *Computer networks*, *76*, pp.146-164.

Skalkos, A., Stylios, I., Karyda, M. and Kokolakis, S., 2021, ‘Users' privacy attitudes towards using behavioral biometrics continuous authentication (BBCA) technologies: A protection motivation theory approach’, *Journal of Cybersecurity and Privacy*, *1*(4), pp.743-766.