

# Investigation Study on Awareness of Privacy Issues in General Community

R Chandraprakash<sup>1#</sup>, KDRM Munasinghe<sup>2</sup>, N Wedasinghe<sup>3</sup>

<sup>1,2,3</sup>Department of Information Technology, Faculty of Computing,  
General Sir John Kotelawala Defence University, Sri Lanka.

# [38-bit-0045@kdu.ac.lk](mailto:38-bit-0045@kdu.ac.lk)

**Abstract**— The rise in technology and computer science has undoubtedly brought benefits to society; however, it has also given rise to potential risks, such as the loss of key data, the disclosure or misuse of personal information leading to significant losses to human society. This survey included largely undergraduates and lecturers, as well as a few people from different professions in Sri Lanka. Altogether the survey was passed on to 350 individuals and 312 responses were grabbed. This study provided information about people's frequent use of personal data when utilizing technological equipment. Additionally, a study on 15 research papers was done to determine how users can exercise caution when using personal data to protect their privacy. The paper explains how regular people utilize their personal information online, whether they are aware of the hazards involved, and how to proceed cautiously.

**Keywords**— Privacy, Rise in technology, technological equipment, Personal Data

## I. INTRODUCTION

The rise in technology has been one of the most significant developments in human history. From the invention of the wheel to the creation of smartphones, technology has transformed every aspect of our lives. The impact of technology can be seen in almost every field, from medicine to education, transportation to communication.

One of the most significant benefits of technology is its ability to improve efficiency and productivity. With the help of machines and automation, we can accomplish tasks that would have taken hours or even days in a matter of minutes. This has led to increased output and reduced costs across various industries.

Another advantage is that technology has made communication easier than ever before. With just a few clicks, we can connect with people from all over the world and share information instantly. This has not only brought people closer together but also facilitated global trade and commerce. However, there are also some downsides to this rapid technological advancement. One major concern is about privacy and security as more personal information is stored online.

The use of technological devices such as mobile phones, laptops, personal computers etc. has been increasing. The advent of technology has brought about a significant increase in the number of technological devices available to individuals. From smartphones to laptops, these devices have become an integral part of our daily lives. However, with the increased use of these devices comes the risk of personal data being accessed and used without consent. With the rise in cybercrime and identity theft, it is important that we take steps to protect our personal information. Unfortunately, many people are unaware of the risks associated with using technological devices and do not take adequate measures to protect their privacy.

## II. LITERATURE REVIEWS

In the research study on “Technology: A Tangible Threat to Our Privacy”, The author argues that the rise of technology has made it easier for our personal data to be collected and used without our knowledge or consent. This can have several negative consequences, including identity theft, stalking, and online victimization. The paper discusses the ways in which technology can be used to invade our privacy, and the concerns that people have about their privacy. The paper also discusses the ways in which we can protect our privacy. The paper's findings suggest that the rise in technology is a threat to the privacy of common people. However, the paper also suggests that there are steps that we can take to protect our privacy. This provides a good overview of the complex issue of privacy and technology. It highlights the potential risks of technology, but it also acknowledges the potential benefits. It is important to consider all of these factors when thinking about how to protect our privacy in the digital age. (Vijay Grover, 2015)

Research finding on “Examining the breaching of personal data in cyberspace from the perspective of psychological violence” discusses the psychological effects of data breaches on individuals. The paper argues that data breaches can cause emotional trauma, which can sometimes be more severe and irreversible than physical effects. The paper also discusses the importance of data security and the need for individuals to be aware of the risks of data breaches. This relates to our study because it highlights the potential psychological effects of data

breaches. The paper also discusses the importance of data security, which is a key issue in the debate about privacy and technology. And it discusses the different ways in which data breaches can cause emotional trauma concludes by arguing that data security is an important issue in the debate about privacy and technology.(Akça, 2023)

“Evolution of Concepts of Privacy and Personal Data Protection under the Influence of Information Technology Development” study discusses the historical evolution of privacy and the impact of technological advancements on the development of data protection laws. The paper argues that the rise of technology has made it easier for our personal data to be collected and used without our knowledge or consent. This has led to a growing concern about privacy and has prompted governments to enact laws to protect our personal data. The paper is relevant to our study because it highlights the potential threats to our privacy posed by technology. The paper also discusses the importance of data protection laws, which are a key tool for protecting our privacy in the digital age.(Gurung and Raja, 2016)

The study discusses the use of security alert sharing platforms by Computer Security Incident Response Teams (CSIRTs) to protect data and privacy. The paper argues that the use of these platforms can lead to additional processing of personal data, which may cause new privacy risks. The paper also discusses European data protection law, which sets out strict rules on the processing of personal data. The paper is relevant to our study because it highlights the potential threats to our privacy posed by technology. The paper also discusses the need for balance between privacy and security, and the importance of complying with data protection laws. As of the key points the paper discusses the different ways in which personal data can be processed by security alert sharing platforms, the legal requirements for processing personal data under the GDPR.(Stupka, Horák and Husák, 2017)

The findings discuss the protection of personal data on the Internet, focusing on the legislative approach, IT security, and managing databases of sensitive information. The paper argues that the rise of technology has made it more important than ever to protect personal data. The paper also discusses the importance of legislation and IT security in protecting our privacy. The paper discusses the different ways in which personal data can be collected and used on the Internet, discusses the legal requirements for protecting personal data under various laws, such as the General Data Protection Regulation (GDPR).And concludes by arguing that there

is a need for strong legislation and IT security measures to protect personal data on the Internet.(Skwarek, 2016)

The Research findings explore the urgent need to enhance personal information security (PIS) in the face of technological progress and the inherent risks associated with the development and use of personal information in the information society. It focuses on the relationship between big data and PIS, highlighting the challenges and causes of personal information protection within big data operations. Additionally, this study presents measures to strengthen PIS during big data operations Addressing these issues is crucial for maintaining privacy and trust in the digital age.(Xu and Nie, 2020)

The research on “Security of Personal Information in the Era of Big Data” delves into the challenges posed by the advent of the big data era, which has brought intelligence and convenience to people's lives while simultaneously raising concerns about personal information security. In this context, the continuous input of massive amounts of personal information has created fertile ground for the illegal acquisition, dissemination, and misuse of data. This study discusses the concepts of personal information and examines the sources of risks associated with its collection, dissemination, and application. This paper offers valuable theoretical support for addressing personal information security concerns in the era of big data.(Xu and Nie, 2020)

Data-driven risk assessment approach for protecting personal data in the context of privacy and security issues. The study proposes the use of extended data flow diagrams (DFDs) to model the flow of collected personal data, allowing organizations to identify scenarios of data collection and usage. By assessing associated components and potential incidents related to each personal data, the proposed approach enhances the accuracy of risk evaluation and diminishes risks to assets associated with sensitive personal data. Compared to traditional asset-oriented and process-oriented approaches, this method ensures comprehensive protection of sensitive data and assists organizations in adopting appropriate security safeguards.(Cha and Yeh, 2018)

The findings on intersection of technology advancements, privacy concerns, and cybersecurity standards in relation to the threat posed to personal data of common people begins by comparing existing cybersecurity standards and regulations, such as those provided by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). It then delves into more specific and recent standards, including those governing cryptocurrency markets and

blockchain technologies. The study highlights the need for adaptation in cybersecurity practices to ensure the security of personal data and the continuity of operations. The findings emphasize the lack of close cooperation between major Western blocks (US and EU) in cybersecurity standards, particularly in areas such as cryptocurrencies, the Internet of Things (IoT), and blockchain technologies. (Radanliev, 2023)

The adoption of Personal Health Records (PHRs) and its relationship with privacy and security concerns in the context of technological advancements study examines the influence of self-determination in health management on individuals' intention to implement a PHR system, emphasizing the need for active participation in healthcare processes. By applying an extended Technology Acceptance Model (TAM), the researchers empirically tested a model explaining public adoption of PHRs. The findings highlight that perceived ease of use, perceived usefulness, and security significantly impact PHR system usage and intention to use. Moreover, privacy is identified as a moderating factor for PHR adoption, while usability moderates various aspects of the adoption process. (Alsyouf *et al.*, 2023)

Research study examines the privacy and security concerns associated with the use of mobile devices, specifically in the context of medical education. The study focuses on third-year medical students and aims to gather baseline information regarding their mobile device use and knowledge of privacy and security issues. A survey was conducted among 67 medical students, assessing their mobile device usage patterns, knowledge of information protection, and concerns about privacy and security. This review sheds light on the importance of incorporating privacy and security education into medical curricula to equip future healthcare professionals with the necessary knowledge and skills to protect patient data in an increasingly mobile-dependent environment. (Whipple *et al.*, 2010)

The privacy and security concerns arising from the permissions model in the Android operating system study explores the impact of evolutionary increments in permission requests from both user and developer perspectives and proposes remedies to address the erosion of users' privacy. The findings highlight that current smartphone operating systems, including Android, do not provide adequate protection for personal data. However, the review presents ideas that can significantly improve the situation and mitigate privacy concerns. Although focused on Android, the implications of the study extend to other operating systems. This review contributes to identifying shortcomings in permissions models and suggests responsible and transparent

practices to protect users' privacy in the context of smart devices. (Tsavli, Efraimidis and Katos, 2014)

With the advancements in information technology and increased connectivity, the invasion of personal space and privacy violations have become prominent issues. IT users are increasingly worried about their personal information being used for purposes other than security. The outsourcing of data processing and sharing of information with third parties further exacerbates these concerns. The study investigates IT users' attitudes towards sharing personal information with government agencies, secure organizations, private websites, and social media platforms. The findings indicate that participants exhibit a deep knowledge of privacy and are highly concerned about sharing personal information with third parties. The privacy concerns of IT users in an increasingly interconnected society, shedding light on their preferences and attitudes towards sharing personal data with different entities. (Rahman *et al.*, 2016)

While there are numerous location-based recommendation algorithms and systems, the privacy issues surrounding the published data have not received sufficient attention and protection. The research findings provide an overview of the research status in security and secrecy, explores the role of users in data security, and introduces classic privacy security modules. Furthermore, it proposes a geographic location-based privacy protection scheme in mobile cloud, analyzing its effectiveness through privacy analysis, sensitive attribute generalization, and route synthesis experiments. This paper contributes to the understanding of privacy challenges and potential solutions in location recommendation systems, shedding light on the importance of safeguarding personal data in the era of advancing technology. (Han, 2021)

The study on "Security and Privacy Concerns in Wireless Networks" focuses on raising awareness regarding security and privacy concerns in network communication among machines, emphasizing the potential threats at both personal and organizational levels. By conducting a survey-based study, the research collects user viewpoints on general awareness and the importance of these issues. The results aim to emphasize the need for networks to prioritize user satisfaction and data protection. Additionally, the paper discusses methodologies and strategies to enhance security and privacy measures, enabling developers and engineers to improve overall protection against potential attacks. This review contributes to understanding the importance of addressing security and privacy challenges in network communication, providing insights for developing effective strategies to safeguard personal data in the

evolving technological landscape.(Soon and Concerns, 2020)

### III. METHODOLOGY

The objective of this paper is to finalize the outcome of the privacy of personal data when using technological devices while connected to the internet. A survey was created to get enough responses covering undergraduates, lecturers, and some other different professions. This survey involved individuals only within Sri Lanka. The contribution of this study is to review whether the individuals who use technological devices agree with the topic of this study and still seem to cooperate with it.

We have been addressing the research topic based on potential risks to the privacy of personal data since the very beginning of the survey. Determine the contents of the research articles that were used to identify proactive approaches to stop people from abusing the privacy of personal data in the second phase. We choose to conduct a survey based on the research topic in the third phase which consisted of questions which was made up by clearly referring from the research papers found on the web related to the research topic. The fourth phase consisted of gathering the survey data that had been examined. Based on the survey, the result was determined in the last phase.

At first, testing was done to determine the facilities of the individuals and whether they had adequate materials to access the internet. And looked up whether they had an idea of the survey they were doing by including the research topic in the survey. The questionnaire consisted of using technological devices that can connect to the internet. All the collected data was derived into an Excel sheet as a fine database to organize it into information. A total of 312 responses were collected throughout the survey.

The audience consists of various age limitations and majority (80.1%) is between 18 years and 25 years old. The rest divides as 11.2% are below 18, 7.7% are between 25 and 35 years old and the least count is in between 25 - 35 years old. We learned from the quantitative data that most of our responses were from undergraduates (80.4%). And the rest of the respondents were varied into several other professions.

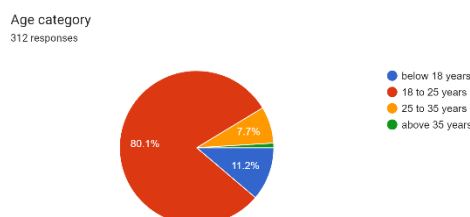


Figure 1: Age Category of Respondents

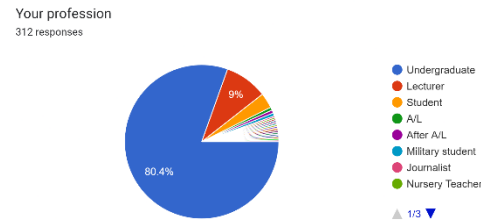


Figure 2: Profession of Respondents

### IV. RESULTS AND DISCUSSION

The existing research papers gave an overall view on whether the rise in technology a threat to the privacy of personal data. But they didn't provide sufficient information whether it was a threat to privacy of personal of common people or the awareness of common people of the threat which can be caused by the rise in technology. Therefore, a well analysed survey is the best option to discuss the results and the modern condition. The objective of the survey is to learn more about the technological devices used by regular people, how they use the internet, how they use their personal data to access it, whether they are aware that their personal data is being misused, and what efforts they take to stop it. Since this questionnaire was primarily intended for undergraduates, lecturers, and a few other people in various occupations, responses were mostly provided by undergraduates. The questionnaire contains 8 main questions mainly focusing on undergraduates, lecturers, and few other professions.

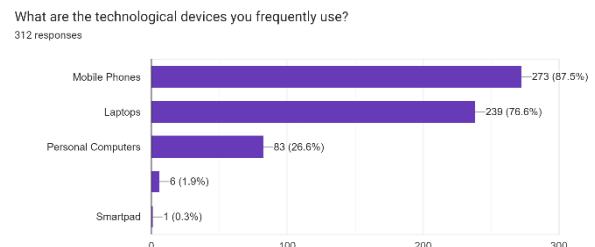


Figure 3: Use of Technological Devices by respondents

The questionnaire was distributed among colleagues and friends, and we were capable of receiving 312 responses.

According to the results the majority are undergraduates with a percentage of 80.1% while the lecturers are 9% and other professions with 10.6%. It is a normal situation

Figure 3: Percentage of Respondents connecting to the internet.

that the majority are undergraduates as the questionnaire was mostly passed among colleagues and friends of the same age category.

# Awareness of Privacy Issues in the General Community: An Investigation Study

During the survey we were also able to collect data regarding the use of technological devices, the use internet,

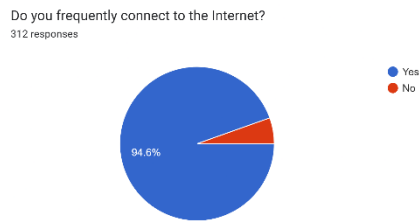


Figure 4: Percentage of Respondents connecting to the internet.

The use of personal data when connecting to the internet, the knowledge on the topic of the research, awareness on whether the personal data is being misused when using the internet and the steps to secure the privacy of personal data.

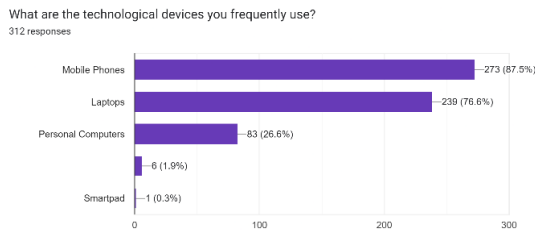


Figure 5: Use of Technological Devices by respondents

In this research the user's personal data to be used the respondents must have adequate internet and a technological device capable of connecting to the internet. Out of all respondents 94.6% of respondents connect to the internet frequently. Most respondents use mobile phones frequently with 87.5%, then laptops (76.6%) and Personal Computers (26.6%). Only one respondent has replied with the device Smart pad. 55.8% of respondents agree that there are threats with the privacy of personal data due to the rise of technology. 10.6% of respondents strongly agree with the statement and 21.2% respondents are neutral. And rest of the respondents do not agree with the statement. The survey showed that 65.7% of respondents think that personal data is being exploited when using the internet. 9% of respondents think that

personal data is not being exploited, while 25.3% are not that sure that their personal data is exploited which they have respondent with the option "maybe". Also steps required to secure the privacy of personal data was also discussed in the questionnaire.

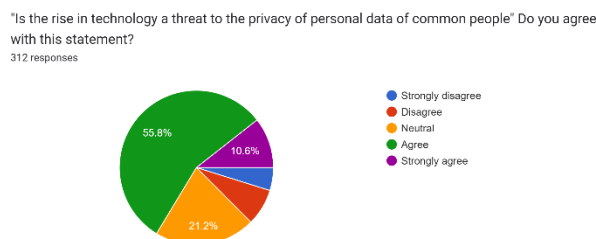


Figure 6 : Respondents' familiarity with the subject of the research

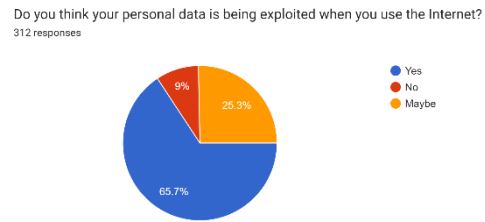


Figure 7 : Respondents' awareness of data being exploited

The options provided for the respondents to select in the questionnaire was derived from the research papers used in the literature review. 77.9% of respondents use high security passwords, 68.6% of respondents use privacy protection tools, 53.5% of respondents use secure folders and, 26% of respondents use VPN when connecting to the internet. By considering the overall results of the survey and existing research papers we can come to a conclusion that the rise in technology can be a threat to the privacy of personal data of common people. The survey provides a clear understanding on the knowledge the respondents have on the threat which can be caused by the rise in the technology. It also implies that the respondents take necessary measures to secure the privacy of personal data.

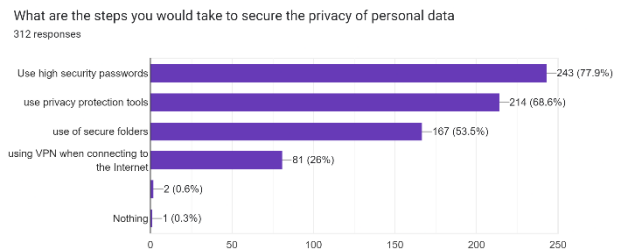


Figure 8: Steps to secure privacy of personal data

## V. CONCLUSION

In today's digital age, technology has become an integral part of our lives. With the rise of technology, we have witnessed a significant increase in the collection and storage of personal data. While this has undoubtedly brought about numerous benefits, it has also raised concerns about privacy. The rise in technology has made it easier for companies to collect and store vast amounts of personal data.

Overall, the results of the literature studies and survey emphasize the importance of individuals being attentive to protecting their personal data in the digital age. It is critical to create awareness, educate individuals about privacy risks, and advocate safe internet and technical device use. Governments, businesses, and individuals should collaborate to create strong legislation, implement effective security measures, and build a

privacy-protection environment. As technology advances, it is critical to remain knowledgeable about the changing privacy and security landscape and to react accordingly. We may mitigate risks and enjoy the benefits of technology while safeguarding our privacy and security by taking proactive efforts to secure personal data.

After carefully examining the data from numerous research papers and the survey results, we were able to conclude that the development of technology poses a threat to the privacy of people's personal information. The research-on-research articles was useful in identifying the privacy concern and the need for users to take precautions to secure their personal information. Some ways of safeguarding our privacy were mentioned in the research papers. These precautions involve using caution when disclosing information, employing privacy protection technologies, creating complex passwords, and supporting privacy protection laws, and several others. We were able to draw the conclusion from the survey that the user was aware that utilizing the internet might have exposed their personal information owing to the development of technology. However, they showed no concern about the dangers and outcomes that could result from data privacy leaks. This study's contribution is to raise people's knowledge of the need to be cautious and aware of potential risks when using personal data to access the internet. For the time being, the research statistics are based on Google Form Analytics, but we will be employing more complex statistical tools for calculations (SPSS, Minitab) in the future to obtain more accurate data that can be depended on for more efficient results.

### VI. REFERENCES

- Akça, B. (2023) 'Examining the breaching of personal data in cyberspace from the perspective of psychological violence', pp. 205–220.
- Alsyouf, A. *et al.* (2023) 'The Use of a Technology Acceptance Model (TAM) to Predict Patients' Usage of a Personal Health Record System: The Role of Security, Privacy, and Usability', *International Journal of Environmental Research and Public Health*, 20(2), pp. 1–24. Available at: <https://doi.org/10.3390/ijerph20021347>.
- Cha, S.C. and Yeh, K.H. (2018) 'A data-driven security risk assessment scheme for personal data protection', *IEEE Access*, 6(c), pp. 50510–50517. Available at: <https://doi.org/10.1109/ACCESS.2018.2868726>.
- Gurung, A. and Raja, M.K. (2016) 'Online privacy and security concerns of consumers', *Information and Computer Security*, 24(4), pp. 348–371. Available at: <https://doi.org/10.1108/ICS-05-2015-0020>.
- Han, L. (2021) 'Personal Privacy Data Protection in Location Recommendation System', *Journal of Physics: Conference Series*, 2138(1). Available at: <https://doi.org/10.1088/1742-6596/2138/1/012026>.
- Radanliev, P. (2023) 'Review and Comparison of US , EU , and UK Regulations on Cyber Risk / Security of the Current Blockchain Technologies : Viewpoint from 2023', *The Review of Socionetwork Strategies* [Preprint], (0123456789). Available at: <https://doi.org/10.1007/s12626-023-00139-x>.
- Rahman, H.U. *et al.* (2016) 'Privacy and Security - Limits of Personal Information to Minimize loss of Privacy', *Springer Nature Singapor*, (August), pp. 1–8. Available at: <https://doi.org/10.1007/978-3-030-12385-7>.
- Skwarek, Z. (2016) 'Considerations on Personal Data Security', (4), pp. 2–3. Available at: [https://www.researchgate.net/publication/332319399\\_Considerations\\_on\\_Personal\\_Data\\_Security%0A](https://www.researchgate.net/publication/332319399_Considerations_on_Personal_Data_Security%0A).
- Soon, A.K. and Concerns, P. (2020) 'Security and Privacy Concerns in Wireless Networks : A Survey'. Available at: [https://www.researchgate.net/publication/341738673\\_Security\\_and\\_Privacy\\_Concerns\\_in\\_Wireless\\_Networks\\_-\\_A\\_Survey](https://www.researchgate.net/publication/341738673_Security_and_Privacy_Concerns_in_Wireless_Networks_-_A_Survey).
- Stupka, V., Horák, M. and Husák, M. (2017) 'Protection of personal data in security alert sharing platforms', *ACM International Conference Proceeding Series*, Part F1305(August). Available at: <https://doi.org/10.1145/3098954.3105822>.
- Tsavli, M., Efraimidis, P.S. and Katos, V. (2014) 'Reengineering the user: Privacy concerns about personal data on smartphones', *Proceedings of the 8th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2014*, (February 2017), pp. 80–89. Available at: <https://doi.org/10.1108/ics-10-2014-0071>.
- Vijay Grover (2015) 'Technology: a tangible threat to our privacy', *Journal of sociology*, 3(3), pp. 1–9. Available at: [https://www.researchgate.net/publication/277138801\\_Technology\\_A\\_Tangible\\_Threat\\_To\\_Our\\_Privacy](https://www.researchgate.net/publication/277138801_Technology_A_Tangible_Threat_To_Our_Privacy).
- Whipple, E.C. *et al.* (2010) 'Third Year Medical Students' Knowledge of Privacy & Security Issues Concerning Mobile Devices', pp. 1–19. Available at: [https://www.researchgate.net/publication/223971499\\_Third-year\\_medical\\_students%27\\_knowledge\\_of\\_privacy\\_and\\_security\\_issues\\_concerning\\_mobile\\_devices](https://www.researchgate.net/publication/223971499_Third-year_medical_students%27_knowledge_of_privacy_and_security_issues_concerning_mobile_devices).
- Xu, W. and Nie, Y. (2020) 'Research on the legal protection of personal information security in the era of big data', *Journal of Physics: Conference Series*, 1648(3), pp. 1–6. Available at: <https://doi.org/10.1088/1742-6596/1648/3/032067>.

### ACKNOWLEDGMENT

This effort could not have been completed without the assistance of numerous other people. Their assistance to this topic is much appreciated and thanked. We would also want to express their gratitude and appreciation,

especially to Dr. (Mrs.) Nirosha Wedasinghe, for her encouragement and support of this work. It was an honour for us to be able to do research with her under her supervision and instruction. A heartfelt thank you goes out to everyone who helped us finish this paper.

### AUTHOR BIOGRAPHIES



R Chandraprakash is a 3<sup>rd</sup> year undergraduate student of the Information Technology department at General Sir John Kotelawala Defence University. He was actively involved in creating the survey based in the topic and focused on the results and discussion in this paper. He also covered the area of completing the abstract and introduction.



KDRM Munasinghe is a 3<sup>rd</sup> year undergraduate student of Information Technology at General Sir John Kotelawala Defence University. Her work mainly focused on the literature review. She also covered the area of completing the methodology and the conclusion in this paper.



N Wedasinghe obtained her (MPhil)/PHD Degree in Information Technology in the year 2012. She is currently working as a full-time senior lecturer at General Sir John Kotelawala Defence University.