Table of Contents

[PART-1: Reflective CPD 2](#_Toc71479912)

[1.1: Self-Reflection on past achievements 2](#_Toc71479913)

[1.2: Personal SWOT Analysis on my Current Experience 2](#_Toc71479914)

[1.3: Future Personal Development Plan 3](#_Toc71479915)

[PART-2: Research Log 4](#_Toc71479916)

[2.1: Research Topic: Penetration Testing of Web Applications 4](#_Toc71479917)

[PART-3: Project Proposal 7](#_Toc71479918)

[3.1: Introduction 7](#_Toc71479919)

[3.2: Literature Review 9](#_Toc71479920)

[3.3: Research Methodology and Planning 11](#_Toc71479921)

[3.4: Conclusions 13](#_Toc71479922)

[Appendix 14](#_Toc71479923)

[References 16](#_Toc71479924)

# PART-1: Reflective CPD

## 1.1: Self-Reflection on past achievements

Born a passionate problem solver and an appreciator of private space, I am on a trajectory towards solving the perennial cyber security issue of hacking. It emerges as a sensitive cybersecurity issue in the contemporary world. My early life in Delhi, which is the most affected city in the India by gross hacking, ostensibly fueled within me a more profound yearning for improving the web application security of various technologies used in the contemporary generation. As a young lad, I grew up witnessing the gross suffering of the Delhi City residents as most were victims of cybercrimes that were mainly caused by vulnerable security application deployed in protecting computer systems from hacking.

I graduated with a 79.5 mean mark in my K 12 course, and the results helped me secure a place at the Jericho Senior High School. Later, I joined my current University. Upon entering the institution, I enrolled with the 'current technology affairs' club, where I served as a secretary in my second year of study and later as the chairperson. During my tenure as the club's chairperson, seventeen projects related to current technological affairs were proposed and articulated. Among these seventeen projects, ten were related to reducing cyber-related crimes through penetration testing. One of these projects, titled ‘Penetration testing and Cyber Security deficiencies.’ It postulated an existing gap of coordination between vulnerabilities exposed through penetration testing of web application and cyber security interventions adopted. This conclusion intrigued me to research on the moderlities of improving penetration testing of web application as an initiative towards solving contemporary cyber security issues.

Besides, I earned the University's honors award of 'the innovator of the year 2017' after a successful project aimed at developing simple client side penetration tests, social engineering tests, and wireless computer system test applications. Moreover, the success of developing these armature applications awaken my consciousness of the potential that I held in solving the contemporary cyber crimes emanating from untamed hacking technologies. This notion incited early motivation for research to establish the loopholes that the current cyber security measures and technologies have through conducting penetration testing to expose their vulnerabilities against contemporary hackers.

## 1.2: Personal SWOT Analysis on my Current Experience

In my current professional position and my pursuance for a Doctorate, various engagements have awakened my consciousness regarding my Strengths, Weaknesses, Opportunities, and Threats that define my professional wholeness.

*Strengths:*

I am a passionate problem solver. Since my early education life, I have developed an intrinsic urge to create solutions to humankind's problems in society. I find pleasure in sourcing for the root cause of humanity's challenges and creating palatable responses that could reverse these challenges. My Curriculum Vitae (CV) reflects my unmoved passion for creating a sustainable solution to the cyber techniques that limit the relevance of technology to contemporary society. In my CV, I take pride in piloting seven projects to respond to the theory of cyber-attacks that grace the current generation.

Moreover, I am a team player and a deep believer in coordination. My current position as a student exposes me to joined projects and peer discussions through which we exchange ideas and intuitions developed in learning. Besides, my CV testifies various bound tasks such as the ‘Penetration testing and Cyber Security deficiencies’ that was honored as the best project of the school 2004. I have bold regard towards joint efforts and relentless dedication to group work irrespective of my position in the group.

Also, I am a critical thinker and a thorough decision-maker. I have encountered situations that necessitate essential thinking and conscious decision-making in my past and current experiences. I own two projects in which I deployed my necessary thinking abilities to develop amatuter client side penetration tests, social engineering tests, and wireless computer system test applications for usage in my former high school’s computer system security management. Besides, through my critical thinking, I can notice that there are various loopholes in the software applications and computer system security systems that promote the theory of cyber-attacks in contemporary society. I am a good chess player too. Besides broadening my critical thinking, it confirms my psychometric margins as a developing scholar.

***Weakness:***

However limited, my over-reliance on past technologies as the drawing board for future innovations limits my innovation potency. For instance, the social engineering tests, and wireless computer system test applications reflected in my CV are improvements of past creations. Whereas I take pride in developing these outstanding projects, I am conscious of their influence in limiting my creativity and innovation.

***Opportunities:***

My current position as a student exposes me to an opportunity of solving the overall concept of cyber-attacks owing to ill developed web application security technologies. The cybersecurity theory of cyber-attacks points out that most cyber-crimes are perpetrated because of underdeveloped technologies in upholding web application security. This scenario presents me with an opportunity to find solutions to the limitations of computer system, network, and web application security technologies deployed in combating imminent hackers’ attacks.

***Threat:***

In my trajectory to developing my professional objective of solving the cybersecurity issue, I am aware of the threat of lack of literature provision in the field. Though various authors have explored cybersecurity, little has been done concerning the remedies towards vulnerable security technologies that expose the current generation to rampant cyber insecurity. Lack of exploration on the subject is a threat to this development. It intends to consult the perception of the existing literature.

## 1.3: Future Personal Development Plan

My trajectory towards the final project will assume several steps:

**Step 1:** will involve confirming the deficiencies in the security technologies deployed in the current computer systems, networks, and web applications to combat hacking. This stage will be articulated by examining the current technologies used to protect computer sytems from hackers through perfomaning controlled penetration testing of web application and computer systems security measures to expose the potential security vulnerabilities. This stage will be covered within two weeks. Relevant scholarly resources such as books and articles will be critically scrutinized to establish the potential causatives of securityl deficiencies in anti-hacking technologies adopted in the current generation.

**Step 2:** entails researching the specific security vulnerabilities existing in the platforms developed to web applications from hackers attacks. This stage will inspect the year of establishment for the versions of the technology, the market prevalence of the technologies, and their reliability in protecting web applications from potential hacking. This stage shall be covered in a week, within which extensive study on past similar projects touching on penetration testing of vulnerable web application security tehnologies will be done.

**Step 3:** will include finding solutions to the security vulnerabilities identified through the various penetration tests. This task will also be articulated through consulting the existing literature and professional advice. However, in the event of insufficient literature provision, relevant recommendations shall be made based on my personal, professional experience in the field. This section of the project shall be covered within two weeks.

**Step 4:** will entail testing the suitability of the above-proposed recommendations to improve web application security through performing penetration tests. The new web application security advancements will be tested by observing their performance when deployed against the 'hackers' technology. Various versions of technologies that hackers deploy shall be tried against the improved web application security technoliogiwes through penetration testing. These versions of 'hackers' technologies shall be sourced from the existing literature. This stage is scheduled for three weeks.

**Step 5:** will involve incorporating the new, improved web application security technologoies with the current technology. This stage is scheduled for two weeks. The approved technological advancements will be configured to match the current user technologies used in contemporary society to uphold web application and computer system security. The configuration pedagogy that will be deployed in this section shall be sourced from the literature and innovative classwork.

# PART-2: Research Log

## 2.1: Research Topic: Penetration Testing of Web Applications.

**Students name:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Research activity | Sources | Author | Notes |
| 1st June 2021- 8th June 2021 | Confirming deficiencies in web application security technologies | A process for data protection impact assessment under the European general data protection regulation | Bieker et al. 2016 | There various technological deficiencies amongst the data protection technologies used |
| 9th June 2021-12th June 2021 | Confirming technological deficiencies from existing secondary sources. | The privacy, data protection, and cybersecurity law review | Raul (2018) | The literature points out that critical deficiencies exist between data protection technologies and hackers' technology. |
| 12th June 2021-17th June 2021 | Investigating the limitations of tokenization as a cyber protection measure. | Cyber security and data privacy | Herrmann, et al. 2018. | Advanced configuration techniques expose data protected through tokenization. |
| 19th June 2021- 22nd June 2021 | Investigating cloud protection deficiencies | Data privacy and data protection insufficiencies. | Research author. | Technological advancements are gradually facing out cloud data protection. |
| 23rd June 2021-27th June 2021 | Investigating Firewall deficiencies from secondary sources | Application research of distributed Firewall based on intrusion detection. Microelectron Comput, | Hu et al. 2011 | Firewall cannot protect against internal attacks. |
| 28th June 2021-30th June 2021. | Investigating the deficiencies of password technique | Data privacy and data protection insufficiencies. | Research author | Password technology is fast facing out of relevance in data |
| 31st June 2021 -5th July 2021 | Investigating the deficiency of schedule backup | Weaknesses of Compliancy for Data and Storage | Goodman and Rowland, 2020. | The use of backup schedules belongs to an outdated generation. |
| 5th July 2021-8th July 2021. | Finding solutions to the cloud protection deficiencies identified. | Cybersecurity and data privacy. | Herrmann, et al. 2018. | Adjusting the current data protection techniques with the hackers' technology will boost cloud data protection. |
| 9th July 2021-12th July 2021 | Finding solutions to the Firewall deficiency identified | Application research of distributed Firewall based on intrusion detection. | Hu et al. 2011 | Scaling the developing technology adopted in Firewall will improve its performance against hackers. |
| 13th July 2021-15th July | Finding the solution to the password deficiency identified | The privacy, data protection, and cybersecurity law review | Raul, 2018. | Intensifying the complexity of password techniques will boost their performance against hackers. |
| 15th July 2021-20th July 2021. | Choosing the testing mechanism for the proposed technological advancements. | Deficiencies of Compliancy for Data and Storage | Goodman and Rowland, 2020. | The proposed technologies can be tested by observing their performance against known hackers' technology |
| 21st July 2021-28th July 2021 | Testing the suitability of the technological advancements proposed. | A process for data protection impact assessment under the European general data protection regulation. | Bieker et al., 2016. | Improved technology is relevant in subduing the contemporary imminent cyber-attacks. |
| 29th July 2021-5th August 2021 | Confirming the test results of the suitability of proposed remedies through second testing. | Improving cybersecurity awareness and training programs with data analytics. | Korpela, 2015. | Improving Firewall technology and tokenization techniques will help in subduing cyber-attacks. |
| 7th August 2021-11thth August 2021 | Configuring the new technological advancements. | Privacy protection and data security in cloud computing: a survey, challenges, and solutions | Sun, 2019. | Configuring the proposed remedies eases their compatibility with the current data privacy and data protection interventions. |
| 12th August 2021-14th 2021. | Implementing the configured remedies by merging them with the existing technologies. | Deficiencies of Compliancy for Data and Storage | Goodman, and Rowland, 2020. | Configured technologies are compatible with existing technologies used in data protection. |
| 14th August 2021-15th August 2021 | Testing the performance of the new security technologies | Improving cybersecurity awareness and training programs with data analytics. | Korpela, 2015. | The new, improved techniques are effective in averting existing hackers' advancements. |

# PART-3: Project Proposal

## 3.1: Introduction

The proposed project seeks to improve the current web application security technologies which are ostensibly fueling increased cybersecurity issues. The project will ensue by scrutinizing the currently web application security technologies establish the likely loopholes that cybercriminals could be capitalizing on. The relevant literature detailing the technologies developing configurations shall be critically sought to establish the technology adopted. Besides identifying the loopholes, necessary technological improvements shall be proposed to boost these web application security technologies against imminent hackers' attacks.

The inspiration of this project is based on the prevalence of cybersecurity issues in contemporary society. According to the cyber-attack theory, at least 45% of the overall cybersecurity issues emanate from poor web application and computer system security. Current hackers have mastered the art of manipulating the existing security measures and thus exposing users to numerous cyber-attacks (Korpela, (2015). The current web security technologies are gradually getting overtaken by technological dynamicity (Sun, 2019). The technologies used in developing these cybersecurity measures do not stand a chance to the advanced hackers' pedagogy. The scenario is established after confirmations from various client side penetration tests, social engineering tests, and wireless computer system test applications conducted on the existing security technologies. This phenomenon necessitates research to establish how best these secuirity technologies could be improved to protect web applications and computer systems from imminent hackers’ attacks.

The scope of the proposed research extends from examination of the current web application security protection technologies to implementation of the new advanced security techniques noted through various penetration tests. The initial stages of the research shall critically review the technologies used in developing the existing computer system, network, and web application security measures. Various applaication penetration tests shall be perfomed on the existing security technologies to expose their vulnerabilities against hackers. The research shall then include extant study for necessary interventions that could boost the performance of these web application security technologies against any hackers' attacks. Besides literature research, the study shall also borrow from the creative innovation projects achieved in class. The last section of the study will integrate the proposed technological advancements with the current web application securitry techniques.

**The SMART objectives** **for the proposed project are expounded as follows:**

***Specific:***

The project targets improving the performance of the existing web application security technologies through penetration tests, as they contribute to the underlying issues of cyber-attacks.

***Measurable:***

The measurement technique for the project will entail testing the performance of the proposed advanced web application security technologies with some of the known 'hackers' technologies.

***Attainable:***

With the current literature provision, the course innovative projects achieved in my learning experience, and a generous schedule, it is practical to find relevant improvements to facilitate existing web application protection measures against hacking.

***Relevance:***

The research to improve the security technologies used in computer system and web application protection is in context with the contemporary cyber issues. Most cyber-related crimes capitalize on ill perfoming security technologies adopted in upholding the system protection from malicious access.

**Research Questions:**

The following research questions shall guide the proposed study:

1. What are the emerging trends in computer/cyber security theories and techniques?
2. What are some of the web application security technologies used in the contemporary society?
3. What are some of the penetration test techniques that can be used in evaluating the performance of the above security technologies?
4. What are some of the security vulnerabilities identified from the above penetration tests?
5. What improvements would you recommend on the existing web application security technologies to boost their performance against hacking?

## 3.2: Literature Review

A previous course assignment study that my group and I performed, intending to establish the prevalence of malware in the contemporary world. In our research, we consulted Albakri et al. (2019), Lloyd (2020), Steinke et al. (2015), Feng and Zhang (2020). They guided us to conclude that the new malware used by hackers adopt more advanced technology than the techniques used in web application security mechanism. The study revealed that the development of modern malware such as Ransomware, Mobile Malware, Remote Accessed Trojans (RAT), and Adware adopt highly advanced technology (Korpela, (2015). This scenario exposes the current web and application security measures of combating hackers to advanced attacks than they can handle.

Bieker et al. (2016) performed a study to investigate the causes of numerous cybersecurity issues. The study concluded that the current web and application security technologies are not sufficient to avert imminent cyber-attacks. The study, which based on a survey conducted using the administration of questionnaires to various software developers, concluded that the technology adopted by hackers is gradually surpassing the technologies used in developing web and application security measures (Sun, 2019). This study postulates of a malicious speeding of technological advancement by hackers to face out the existing anti-cyber-crime technologies.

A penetration test study performed by Lloyd (2020) to investigate the effectiveness security technologies adopted against hackers that the technologies are insufficient in averting contemporary cyber-attack advancements. The research designed as a cohort study sampled numerous anti-hackers technologies through penetration tests. The study points out that a common causative of the current cybersecurity issues is the ill development of web and application security technologies. The author noticed that the hacking technologies used in cracking the protected web applications and computer systems assume more advanced configurations than the current generation of technology. This scenario ostensibly accounts for the contribution of technological insufficiencies in security intervenetions and the prevalence of hackers’ attacks in the current generation.

Raul (2018) also performed a study through penetration tests to investigate the suitability of the existing web protection mechanisms against hackers. The study involved sampling security technologies such as Firewall technology and gathering observing their perfomances against known hackers’ technology. The study concluded that though Firewall is relevant in protecting external attacks, they are vulnerable to internal attacks. Raul (2018) argues that 85% of the Firewall applications are insufficient in averting hacker's activities emanating from within the computer system. This scenario exposes users to Trojan attacks that mainly originate from the computer system. The scenario depicts that the Firewall technology used in data protection and data privacy is not sufficient to repel imminent cyber-attacks.

Besides, Steinke et al. (2015) performed penetration tests to analyze the effectiveness of Pseudonymisation as a protective technology used in web applicatrions to combat hacking. The study concluded that though the technique effectively strips identifying information that hackers capitalize on in specifying their attacks, the technology still faces tough competition from hackers' advancements. Steinke et al. (2015) lament that contemporary hackers have mastered and can reverse the (General Data Protection Regulation) technology GDPR deployed in effecting Pseudonymisation as a protective measure for web applications, networks, and computer system. Similar to Hu et al.'s (2011) conclusions, the current defense mechanisms are developed on outdated expertise due to the dynamicity of the present technology. This scenario reaffirms a technological insufficiency in the performance of the various security technologies adopted against hackers.

A follow-up study was performed by Hu et al. (2011) to establish the possible improvements that can be reflected in the contemporary technologies used in protecting web apllications, networks, and computer systems. The study concluded that improving the technologies used in web application protection would help to match the dynamicity of technology exhibited by contemporary cyber attackers. A similar recommendation was drawn by Feng and Zhang (2020) in a study to investigate the causatives of rampant cybersecurity issues in the modern world. Feng and Zhang (2020) quote, 'the good guys should scale up their technology to catch up with the bad guys' technology. There is an existing race of technological advancement between hackers and ordinary computer users, and the latter is widely losing.

Lloyd (2020) advanced his study on the reasons for the failure of the Pseudonymisation technique in ensuring cybersecurity. The research concluded that hackers discovered the concept of revealing user identities concealed through Pseudonymisation. Lloyd (2020) accounts that contemporary hackers have staged advanced techniques of reverting almost all the data privacy and data security interventions. A delay in advancing protective technologies causes this phenomenon. The study also concludes that contemporary cybersecurity issues can only be solved through scaling up the security technologies to match the hackers' technology.

**An illustration of the body of knowledge**

Cyber Security

Compromising

Web application insecurity

Out date

Cloud data protection

Out dated

Encryptions

Out dated

Tokenization

Advanced

Out dated

Firewall

Advanced

Advanced Advanced

RAT Trojan

Mobile malware

Adware

Ransomware

## 3.3: Research Methodology and Planning

**The study design**

The proposed research will adopt two research designs in different stages of the study. In the preliminary stage, the research shall deploy a descriptive study design. At this stage, the research will scrutinize the recommendation of various scholars and researchers to improve web application security. The advanced stage of the research study will deploy an experimental study design. The study will involve penetration testing on various recommended technologies used against the current hackers' technology. The recommended improvements will be experimented with to verify their suitability in protecting applications, networks, and web against contemporary hackers.

**Research Approach and Data collection**

Based on the nature of the study as guided by the research questions, the study will consider previous classwork and group projects as the primary source of information. The various course projects' conclusions will be regarded as the introductory guide to the study. Besides, peer-reviewed scholarly articles and Books shall be considered secondary sources of information. Secondary data shall be sourced from relevant databases such as google scholar. The guiding search terms for the secondary search will be; penetration testing, web application, web application security, and cybersecurity vulnerabilities. The obtained results will be vetted based on the author's credibility, year of publication, and their precisions in responding to the research questions.

**The Project Plans**

The proposed research is scheduled to be covered in 10 weeks. The study will involve tracking the potential technological deficiencies in web application security measures. Both the course group projects and secondary sources identified will be sought to investigate the outstanding technological limitations existing in cyber security technologies.The following week will then be spent locating the identified technical limitations in the web application security interventions currently used. This stage uses the secondary electronic database such as Google scholar as the primary resource.

Nevertheless, two more weeks will then be spent locating possible remedies to the identified technological limitations. The primary resources to be used during this stage are the recommendations from the previous group projects. Also, scholarly suggestions from existing literature will be sought to gather relevant solutions to the identified technological deficiencies. The research will then cover additional three weeks to experiment with the suitability of the remedies proposed towards improving the performance of web application security measures. The leading resource for this stage of the plan will be the secondary sources drawn from reliable electronic databases. The last step of the research will involve incorporating the identified and experimented technological advancements (Herrmann et al. (, 2018). This stage will include configuring the recognized technological advancements to match the hackers' technology.

**Gant Chart illustrating the project plan throughout the ten weeks:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Week 1** | **Week 2** | **Week 3** | **Week 4** | **Week 5** | **Week 6** | **Week 7** | **Week 8** | **Week 9** | **Week 10** |
|  |  |  |  |  |  |  |  |  |  |

Critical Tracking potential technological deficiencies.

Locating the identified technological limitations.

Locating possible remedies to the identified technological limitations.

Experimenting with the suitability of the proposed remedies.

Implementing the proposed and experimented remedies.

**Risk Assessment and Management**

The proposed research shall be exposed to the risk of biases. Since secondary sources of information are vital resources in the project, there is a risk of potential bias from scholars' perceptions. However, this risk shall be screened by vetting the credibility of authors. Besides, the study is at risk of gathering irrelevant and outdated recommendations to improve the current data privacy and data protection technologies (Herrmann et al. (, 2018). However, the risk shall be screened by vetting the year of publication for various articles and books. Moreover, a specialist in cybersecurity issues will be considered the ideal authors of the secondary sources sought.

Moreover, the proposed research is vulnerable to the risk of misleading information. The secondary information gathered in developing the research study could be tricky. Authors who produce various publications could be interested parties in the dynamics of cybersecurity. This phenomenon can result in the production of misleading information that could limit the practicality of the proposed research project. However, the risk of misleading response will be assessed and averted by examining the various authors' credibility and achievements consulted.

The research project could face the risk of timeframe constraints. According to the breadth of cybersecurity topics and the extensive experimentation required in the field, the plan is likely to exhaust the scheduled time before it is completed. This risk will be assessed and managed by ensuring that only the essential facets of the study were preferred. In the event of time laps in any research stage, an extra day has been scheduled before the next step ensues to clear up the unfinished tasks.

Moreover, the proposed research faces a legal risk as most of the technology versions in the market assume copyright measures. Software information stored in secondary sources of information is under copyright protection. This means that it is illegal to borrow someone's technological ideas without due consent. However, this risk will be managed by seeking permission from the identified scholars to develop more advanced technologies. Besides, consent shall be sought from the (General Data Protection Regulation) GDPR to explore their protected information regarding the potential improvements that could affect the current data protection and data privacy techniques.

## 3.4: Conclusions

The prevalence of cybersecurity issues in contemporary society is fueled by outdated technologies in web and application security. The technology used by hackers has surpassed the configurations used in developing the existing cyber security techniques. The dynamicity of technology postulates a technological deficiency in the data privacy and data protection measures adopted in contemporary society. Scaling up the web application security technologies is a relevant initiative in addressing cybersecurity issues. The development of this research attached to consideration of various facets as follows:

***Ethics:***

The subject of cybersecurity commands gross ethical consideration as it touches on privacy and user protection. Therefore, the proposed research is planned concerning the ethical obligation to seek consent from authors before using their literature in advancing publications. Besides, the research is conscious of the moral responsibility to raise socially accepted solutions in solving the cybersecurity issue as a contemporary social issue. The study also majors on upholding modesty to produce accurate and unbiased conclusions that can offer reasonable solutions to the underlying problem without misleading the target audience.

***Legal:***

Also, the proposed research is considered to a legal obligation to seek permission to use materials under copyright protection. The investigation believes that the secondary sources recommended are works of authors that the lawful copyright provision has protected. Besides, the study is also conscious that a wrongful branding of someone's genuine work as malware amounts to gross defamation, which is a crime. Considering all these legal issues, the research shall seek copyright consent before using protected secondary sources of information. In addition, the study intends to confirm the relevance, authenticity, and use of various software before terming them as malware.

***Social:***

The study is conscious of the social consideration and obligation to provide solutions to the problems affecting humanity in society. Researchers' social responsibility is to identify societal problems and devise necessary interventions to address the underlying issues. The proposed research considers cybersecurity as a societal problem. In this context, the study's social responsibility is to find necessary solutions to cure the cybersecurity menace.

***Security:***

The proposed research credibly appreciates that cyber-attack issues as vital security issues in contemporary society. For instance, many recent bank robberies have been perpetrated using hacking technologies, and most of the cases are still undecided in the court of law. Some of the hacking technologies used in recent bank robbery crimes could be available in the public domain. Therefore, the research is careful not to explore security-related issues before the court.

***Professional considerations:***

The nature of the research proposal assumes a professional approach as it involves exploring the proficient and skilled field. The proposed research intends to establish factual findings with relevant evidence in the area regarding this consideration. Besides, the information sourcing technique deployed in the study consults professional perceptions from the various secondary sources of information deployed.

# Appendix

**ETHIC CLEARANCE REFERENCE:** Cyber Security Project

**FORMAL DETAILS**

**Name and student number:**

**Supervisor:**

**Title of the research project:**

Cyber Security Project

**Purpose of the research:**

The proposed project seeks to improve the current data privacy and data protection technologies that are fuelling increased cybersecurity issues. The project will ensure by scrutinizing the currently existing cyber security technologies to establish the likely loopholes that cybercriminals could be capitalizing on.

**Research methodology:**

The proposed research will adopt two research designs in different stages of the study. In the preliminary stage, the research shall deploy a descriptive study design. At this stage, the research will scrutinize the recommendation of various scholars and researchers to improve data privacy and data protection techniques and a more significant extent, cybersecurity. The advanced stage of the research study will deploy an experimental study design. The study will involve testing various recommended technologies against the current hackers' technology. The recommended improvements will be experimented with to verify their suitability in protecting data against contemporary hackers.

**Funding source (or anticipated funding source)**

Personal

**Duration of the research project:**

Ten weeks

**Contact details for the applicant:**

# 

# References

Albakri, A., Boiten, E. and De Lemos, R., 2019, June. Sharing cyber threat intelligence under the general data protection regulation. In Annual Privacy Forum (pp. 28-41). Springer, Cham.

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H. and Rost, M., 2016, September. A process for data protection impact assessment under the European general data protection regulation. In Annual Privacy Forum (pp. 21-37). Springer, Cham.

Feng, X. and Zhang, X., 2020. Personally identifiable information security in cloud computing.

Goodman, H.B. and Rowland, P., 2020, June. Deficiencies of Compliancy for Data and Storage. In National Cyber Summit (pp. 170-192). Springer, Cham.

Korpela, K., 2015. Improving cybersecurity awareness and training programs with data analytics. Information Security Journal: A Global Perspective, 24(1-3), pp.72-77.

Lloyd, I., 2020. Information technology law. Oxford University Press.

Herrmann, A., Brenner, W. and Stadler, R., 2018. Cybersecurity and data privacy. In Autonomous Driving. Emerald Publishing Limited.

Hu, P., Li, Z. and Peng, J.K., 2011. Application research of distributed Firewall based on intrusion detection. Microelectron Comput, 28(6), pp.126-130.

Raul, A.C. ed., 2018. The privacy, data protection and cyber security law review. Law Business Research Limited.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A.J., Repchick, K.M., Zaccaro, S.J., Dalal, R.S. and Tetrick, L.E., 2015. Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Security & Privacy, 13(4), pp.20-29.

Sun, P.J., 2019. Privacy protection and data security in cloud computing: a survey, challenges, and solutions. IEEE Access, 7, pp.147420-147452.