“DEVELOPING A SECURE CHILD ONLINE PROTECTION DATABASE ACCESS MODULE”

BY

ESTHER N SHIVUTE
215025911

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF HONOURS IN SOFTWARE DEVELOPMENT

IN THE

FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF COMPUTER SCIENCE

AT

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SUPERVISOR:

PROFESSOR FUNGAI BHUNU SHAVA

DATE OF SUBMISSION:

07/02/2022

METADATA

TITLE	**Ms**
STUDENT NAME	Esther N Shivute
SUPERVISOR	Professor Fungai Bhunu Shava
CO-SUPERVISOR	None
DEPARTMENT	Department of Computer Science
QUALIFICATION	Bachelor of Computer Science Honours
SPECIALISATION	Software Development
STUDY TITLE	Developing A Secure Child Online Protection Database Access Module
MAIN KNOWLEDGE	Software Development
TYPE OF RESEARCH	Quantitative Research
METHODOLOGY	Study
STATUS	Mini-thesis
SITE	Namibia University of Science and Technology
DOCUMENT DATE	07 February 2021
SPONSOR/CLUSTER	Digital Forensics and Information Security

DECLARATION

I Esther Niita Shivute, hereby declare that the work contained in the mini-thesis for the degree Bachelor of Computer Science Honours in Software Development, entitled: "DEVELOPING A SECURE CHILD ONLINE PROTECTION DATABASE ACCESS MODULE"**,** is my own original work and that I have not previously in its entirety or in part submitted it at any university or other higher education institution for the award of a degree. I further declare that I will fully acknowledge any sources of information I will use for the research in accordance with the Institution rules.

Signature: EShivute______________________ Date: 14 February 2022

SIGNATURE OF THE SUPERVISOR

I, ______________________________, herewith declare that I accept this mini-thesis for my supervision

Signature: ______________________________ Date: ______________________

ACKNOWLEDGEMENTS

Firstly, I would like to thank the almighty God for strengthening me on different motivations to continue with my work. He surrounded me with courage people, who assisted me and offered me with different helps and mentorships, they are as follow:

Professor Fungai Bhunu Shava, this is my supervisor and personal mentor. I had a lot of obstructions during this research but you were always there to remind me that I must learn how to work simultaneously and know my goal and how to achieve it. You ensured that I understand what I am doing, follow the correct path and give myself time to rest and do the right thing with a fresh mindset, you gave me different one on one lessons where I have learned a lot and gained confidence. I was never a fan of reading articles and books but because of you I can do this now and it have brought a good effect in my life. I really appreciate you so much for all this and very grateful to have you as my supervisor. First, I thought you were too strict but I was wrong, my colleagues can testify on this. I can't stop thanking you for everything, be blessed, you're a hero Prof.

My dear friends and colleagues, thank you for every word of encouragement and for always having that responsibility that I am working on my research, your support and understanding. Thank you very much.

TITLE

Developing A Secure Child Online Protection Database Access Module

ABSTRACT

The research tittle focused on developing a child online protection database that ensure data security within the database. The main aim or scope of the research is to gather on how to develop a database with secure access modules. Child online protection is using this data as an approach on finding ways to protect children and currently Namibia has a data storages problem in the arena. To address these problems a web-based database was designed to store data collected about different information on children online abuse and cyberbullying. The database is meant to be accessible to the COP Admins and those who are given access authorities only. This presents a security challenge of the database as the data can be accessed, modified and the research methods solutions can be used to address the challenge. In this research a quantitative method will be used to develop a secure database access module for the COP database. The module will improve in the security of databases in general and to the Namibian community. The need for a secure database access module was is in response to the findings of a workshop hosted by Namibia University of Science and Technology at then Polytechnic of Namibia in October 2014 (NUST, 2014) which established the need to have a central point where all cases can be reported and tracked and it was further supported by the findings of a study conducted by the National University of Science and Technology (NUST) in collaboration with the Centre for Justice and Crime Prevention with support from UNICEF (UNICEF, 2012). This showed that 29% of our children reported to have seen child pornography content online. This alarming finding further elaborated the need of a database system for data serves as basis to hasten collective measures to ensure the safety of our children online (UNICEF, 2012). Using the current database not all objectives and aims will be met and it is now to find out on "Developing a secure Child Online Protection Database Access Module". As this will be a benefit to both children,

parents and also organization which might get some knowledge and information to implement in their database for security purpose. The way of different work delivery including school have changed, which is caused by the COVID-19 Pandemic.

Table of Contents

TABLE OF FIGURES

TABLE OF TABLES

ACRONYMS

COP	**Child Online Protection**
DB	Database
DBMS	Database Management System
DFISRC	Digital Forensics and Information Security Research Cluster
IT	Information Technology
NUST	Namibia University of Science and Technology
UNICEF	United Nations International Children's Emergency Fund
SDLC	Software Development Life Cycle
SQL	Structured Query Language

CHAPTER 1 : INTRODUCTION AND BACKGROUND OF THE STUDY

1.1. INTRODUCTION

Technology a global computer network (Olaniran, 2013) which provide a lot of communication facilities and, which contain connected network using ordered communication procedures, which today is referred to as “the Internet” is now an elemental piece of everyday lives of utmost children. Expansion operation of ICT over past years (ECDL) is mostly in countries which are developed. Namibia as a developing country, has also witnessed the exponential growth this led to the internet becoming an extremely valuable aspect of the children’s lives, both economically and socially, and has led it to become a seemingly permanent feature of modern-day life source. Today people can connect to the global network (Olaniran, 2013) using a mobile phone, a laptop computer or other portable devices, often with video capabilities and very high-speed access to different sources online. Higher percentage of (UNICEF, 2012) kids and younger generation are mostly on high potential to access the Internet and tool used for access. Abuses of children in not limited to school homes and communities (UNICEF, 2012) with this it also takes place on the internet. Many game consoles are also Internet enabled and this has fostered a huge growth in on-line game playing among children and young people (OECD, 2012) which exposes them to internet abuse. With the increase of access to the Internet, young people and children are mostly under greater threat than ever to a range of potential harm. With this online abuse, potential harm and cyberbullying towards children is huge influence towards life of the children who are victims. It is found that collecting data and information on this will be better in getting a solution on protecting children while online. Preserve and security (Milton Keynes, 2016) is needed to prevent recollection of the same data and information frequently. The database is used in preserving, a structured set of different data kept or held in a computer it’s what we call a database, especially one that is accessible in various ways. With it being accessible in various ways access security need to be implemented in such a database to prevent disruption, unauthorized editing, deletion and insertion, and working on invalid data. Database security is the collective measures used to protect and secure (Sorkin, 2011) a database or database management software from illegitimate use and malicious threats and attacks.

1.2. BACKGROUND

The Child Protection programme in Namibia focuses on prevention and response to violence against children. UNICEF is working with partners to ensure that more vulnerable children and women benefit from integrated child protection and justice services. As internet accessibility and usage are on the rise in Namibia, the Country Office has been implementing a child online protection programme since 2016, addressing both offline and online violence against children. As a strong legal framework in the area of child protection is crucial, the country programme aims to create an enabling policy and legislative environment for children. COP is very powerful and complex requirements for multi-national efforts if it's to be successfully tackled in the near future. This is mainly due to the exponential growth in smart devices and the internet or rather "the Internet of Things". Internet penetration has increased in Namibia (Fungai, Chitauro, Mikka, Nhamu, & Gamundani ,2016). At the same time, it aims to ensure that survivors of violence, abuse and neglect receive timely and adequate support services. Additionally, UNICEF works with law enforcement and judiciary to ensure that perpetrators are prosecuted and children can grow up in a save, positive and stimulating environment. Furthermore, it is supporting knowledge generation and management around the issues of child (online) protection.

1.3. PROBLEM STATEMENT

Currently in Namibia there is no central repository of information on child online abuses. The DFISRC at NUST identified this gap and through consultative workshops, designed a database to store cases ad information on Child Online Protection. The lack of data and information security results in unauthorized access of Child Online Protection Database that cause modification of data and information in the database, resulting in delivering and acting on wrong data and information. The storage of such sensitive data needs precautions to be put in place as unauthorized access of Child Online Protection Database will cause disruptions of the data. The insecure database access module for the COP database is the one to be considered first in order to ensure that unauthorized access is prevented.

1.4. RESEARCH OBJECTIVE(S)

With the rise in terrorism threats, efforts are now focused on security issues in many organizations. One aspect of security is database security. Database security has a great impact on the design of today's information systems.

Design an authentication module to secure the Children Online Protection Database is this research main objective. The sub- objectives that will help in achieving the main objective it includes:

1. To identify current Child Online Protection Database security challenges.
2. Identify secure techniques and methods for accessing data in databases.
3. Analyse solutions that can best mitigate the security problems of Database access.
4. Design a secure database access module.

1.5. RESEARCH QUESTION(S)

The following questions have to answered in order to accomplish the main objective and sub-objectives in section 1.4. The main question is: How to design an authentication module and how will it secure the COP DB?

The sub-objectives questions:

- What are the current security challenges in Children Online Protection Database?

- What are the secure techniques and methods to access data in databases?
- How can the secure database access module reduce children online abuse and cyberbullying?
- How can one design a database with a secure access module?

1.6. RESEARCH DELINIATION

Child Online Protection capture data in a database, this database needs to be secure and this research is focusing on how to secure, by designing and prototype access module. The development of the access module will be developed by implementing different security techniques.

1.7. SIGNIFICANCE OF THE STUDY

Child online experience data collected about children online abuse and cyberbullying have to be stored in a database. Privacy and sensitivity of these data, thus must be subject to strict privacy agreements. It is of more benefit to our younger generation to secure data about children online abuse and cyberbullying, because this data will be used as a tool to lead other children on what not to do while online, take note and how to avoid them. These benefits can as well include:

- Children privacy and identity online safety.
- Teach children on different online safety guidelines.
- The strength of sector on privacies to higher ethical standards and exercises that protect and benefit children online.

1.8. THESIS BREAKDOWN/CHAPTER OUTLINE

The mini - thesis will be divided into six chapters:

Chapter 1: Introduction & Background of the study

This is where the research introduction and background are introduced and explained. Furthermore, it highlights the statement of the problem, the research objectives, research questions and the impact that this study will have towards the security of child online protection database in Namibia and for other organisations for their database security.

Chapter 2: Literature Review

Discusses the literature review and explains different studies and reports on the topic. In the literature review the author explains the risks of insecure database for COP and how this has an effect on the data to be used for the solution to secure a child online.

Chapter 3: Research Methodology

Discusses the methodology for the research, which consists of methods, design processes, design approach, data collection techniques, and questions carried out to help develop a secure database access module.

Chapter 4: Prototype and design of the secure access module

Presents the stages, flow and outcome of the design process of the access module to secure Children Online Protection Database.

Chapter 5: Conclusion and Recommendations

Provides a discussion of the outcome of the study, concludes the study, provides areas and direction for future research that the author would like to embark

CHAPTER 2 : LITERATURE REVIEW

2.1. INTRODUCTION

This chapter gives an overview about child online protection and reviews different materials published on the subject matter focusing on Child Online Protection and database access. It also elaborates more on the proposed solution to secure the child online database data, because this data will be used to identify the solutions to secure children from different attack while online. Furthermore, different workshops were also held for ensuring that most of the children if not all, that they are secure as they differently associate with the technology. The children are rightly placed as blameless victims by definition, they need an organized environment for protection which will be for their safe online interaction. Furthermore, Children Online Protection can introduce or increase the responsibility initiatives to ensure that children don't become online victims and unknowingly fall in danger.

2.2. CHILD ONLINE PROTECTION OVERVIEW

Nowadays people use mobile phones, laptop computers or other portable devices to connect to network globally (Olaniran, 2013), mostly with a very fast access speed and video abilities. Higher percentage of younger generations including children (UNICEF, 2012) progressively they can access the Internet and devices used to access it. Abuse of children is not limited to homes, school and other (UNICEF, 2012) but it also takes place on the internet which is the online environment. Children and young people are more into playing games which are mostly accessed or played online and bring them into online abuse.

Access to the internet is growing rapidly, younger generation including children (UNICEF, 2012) are mostly falling on the risk of potential harms, to add on this child online safety is now the main pillar of different strategic components around the world for ensuring children’s safety and free from harms. The focus on channeling resources to this finding in Namibia was highly informed by world trends and many other similar projects elsewhere.

A fact-finding workshop hosted by Namibia University of Science and Technology (NUST) at the then Polytechnic of Namibia in October 2014, brought to the fore the need to conduct a field of research to gather empirical data on usage by young people, and the potential risk they are being exposed to online (UNICEF, 2014). This was mainly motivated by the various contributions from stakeholders that participated in the initial workshop, where UNICEF Namibia was represented. The field research was comprised of a survey of 735 young people between the age of 13 and 17. Namibia has been celebrating Safer Internet Day (SID) since 2018. For the past two years, the day was celebrated in the capital city, Windhoek, Namibia. Parents/caregivers, teachers and social workers will join children in a panel discussion on cyberbullying moderated by the Internet Society Namibia Chapter. The celebration preceded by media engagement and talk shows which raise awareness on child online protection and cyberbullying in line with the theme "Together for a better internet". Safer Internet Day (SID) 2020 was organized by the Child Online Protection (COP) Taskforce in Namibia. The COP Taskforce was established in 2017 under the leadership of the Ministry of Gender Equality and Child Welfare. It brings together government ministries, civil society organizations, development partners and the private sector to coordinate the prevention and response to online child abuse an exploitation. NUST is part of the Taskforce which brings it to propose the database to store COP data. The security techniques explained in section 4.3 will be used to implement the access module. This will help achieve the objective in section 4.4 which is one of the requirements to solve database security problem. Furthermore based on the 2014 report by Verizon Data Breach report the highly compromised assets are the databases.

2.2. DATABASE IN GENERAL

Database is a collection of related data (Rouse, n.d.) or is a structured collection of records about children online abuse and data is gathering of figures, findings and facts that can be a be prepared for further action on information. The data or records collected about children online abuses will be stored in the database.

Database security, (Vonnegut, 2016) protection of organization's database confidentiality, integrity and availability is maintained under information. Security is an important concern as the required root in development of information security (Eduardo Fernández-Medina, 2015), and mainly in designing database. Therefore security, as an additional quality resources of software, must be included all phases of the development and design of a secure database. The fastest growth of the Internet and related technologies (Sahoo, 2013) brought a surprising ability of development of secure Database System. Secure database design is the structural outline to process and build a database for an application with different security level properties. Although there is a huge amount of papers about security (Milton Keynes, 2016) representations including aspects of security and authorization of databases, there are few procedures on how the secure DBMS is implemented. It is true that high percentage of many numerous programs for secure database multileveled it contains features (Milton Keynes, 2016) of fulfilment.

Nevertheless, the main issue is that no methodologies of database design that take security in action (and therefore models of database security) through the whole cycle, (Eduardo Fernández-Medina, 2015) exist currently at the early stage particularly. Therefore, designing a database that's secure appropriately it's not possible. There are a lot of cases reported or figured out to be specific in Namibia about data and information known by people who are not part of the company or organization. With this it must not be (Vonnegut, 2016) a surprise that the databases for companies are they main target of hackers, because most organization, companies, government and others share or try to share their main or private data and information that can cause an impact to their database, if is not well secured. For just different destruction hackers do to databases, this most measurement brings a taste amount of data stolen from databases across the breaches of security. There are some issues or effects caused by insecure database, this include business closedown, academic effect, unemployment and many others. With all these problems, to solve them is by the propose to design a secure design of the database. The three basic requirements (Cvrcek) on data protection which include security, integrity and availability must be satisfied by the secure database system:

- **Ensure security**
- **Ensure integrity**
- **Ensure system availability**

In addition to this methodology, there are some models defined that allow us to include security information in the database model (Eduardo Fernández-Medina, 2015), and a constraint language to define security constraints. These models include display of an error message to the admin, if is not him/ her accessing the database, login details, by introducing triggers. As a result, we can identify a great arrangement of information, describing with a big level of correctness which properties each user will possess for them to be enable access per portion of information.

2.3. DATABASE SECURITY SOLUTION

Most activities on research in database security focus on stored data encryption and data that come by running a query. Different techniques on encryption are (Sanjay Sareen, 2016). A lot of time, manpower and money can be spent by organizations trying to secure their assets online (Vonnegut, 2016), but still something goes wrong and cause the down of the database. According to a Dark Reading article, (Vonnegut, 2016) less than 10 seconds is the average time that takes the hacker to access the database and be out with a huge amount of data. And in Verizon’s 2009 (Vonnegut, 2016) Data Breach Investigation Report, they found that while when PoS system breaches see an average of 6% of records compromised, and 19% when the application server is compromised, database breaches (Vonnegut, 2016) see an average of 75% of the organization's records compromised in an attack. Databases are complex, and database administrators don't always know the implications of not ensuring database security and integrity. In addition, it's because huge sensitive and important information for hackers are represented by databases, because the attacks used mostly opposed to databases are not complex particularly.

2.4. DATABASE ACCESS CONTROL MECHANISM

Database access control is in control of procedures identified by policies of securities for all straight database system accesses. Operation, notions, objects and subjects are part of the control system traditional. Access control and fields of information security and physical security is part of the access restriction to different resources and places. Authorization is being permitted to access certain resources. In the Child Online Protection there will be some authorization to users of the database system, which will apply to the security of the database.

Talking about access control in the Child Online Protection Database System, administration way of access regulation (Cvrcek) must be identified:

- **Decentralized hierarchy** – Responsibilities distributions among different authorizers
- **ownership** – object owner must be determined to access the object
- **Authorizations cooperativeness** – special authorization must be defined of group of members.

2.5. PROTECTING CHILDREN WHILE ONLINE OBSERVATION

Based on most observation, reports and case studies, the Internet is marvellous to children. They can use it to research reports for school, communication to their teachers and other children, and play online games (Elana Pearl, 2018).

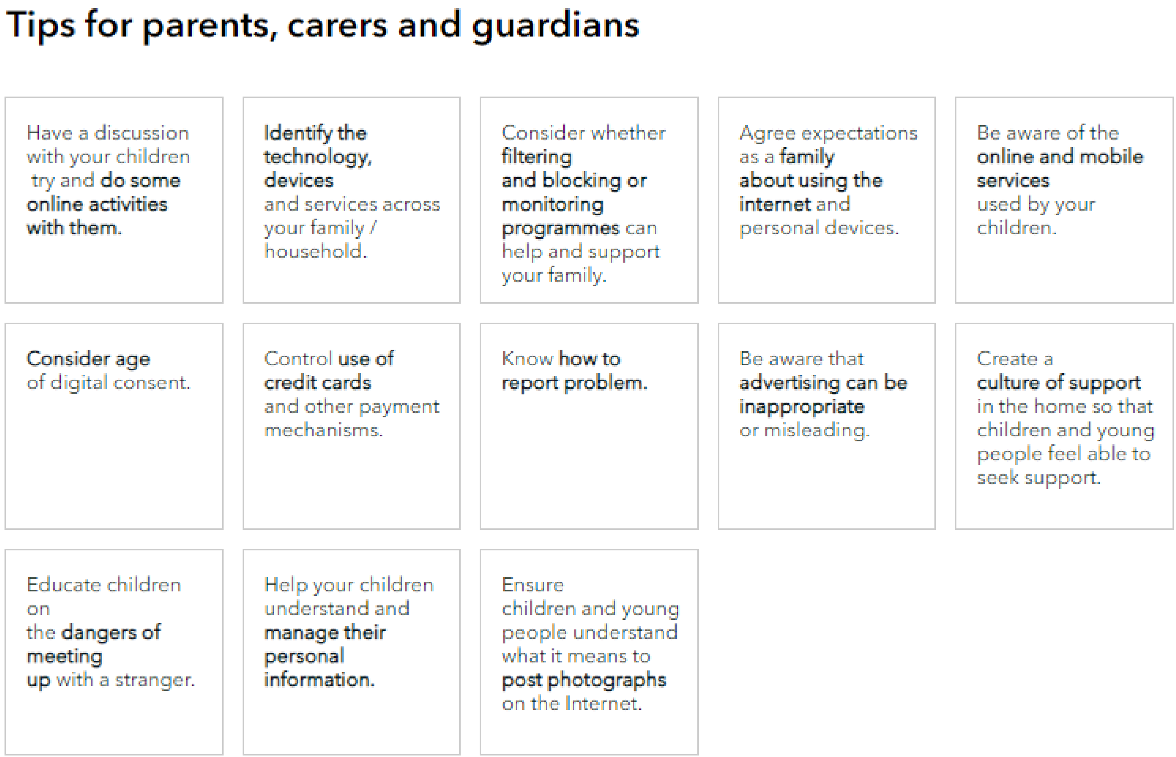
However, online access contains some risks which include contents that are inappropriate, cyberbullying and others (Elana Pearl, 2018). Children interacts with all this by the use of websites and different apps, and the predators can act as a child just to make new friends with them. According to Elana on kids' health "to keep children safer online must not end their liberty; let it be the beginning of open and continuous talk on how to be safe online and build smart online habits."

Are parent's responsibilities (Elana Pearl, 2018) to note what their children hear and see online, what details they share about themselves and what they hear. Parents are encouraged to talk with their kids including protecting them by the use of different tools, and checkout their online activities. Instead of blocking different offensive material, its more advisable to teach your children safely online behaviour responsibilities and checking them when they use the internet (Elana Pearl, 2018).

Table 2-1: Identified guidelines each parent can perform to ensure online safety for their children

Guidelines	**Processes on achieving each guideline**
Talk openly with your child about their online activity	Parents need to ensure that they question their children about what they do online. Furthermore, inform and allow their children to tell them about anything suspicious online.
Keep screens and devices where you can see them	Opening the devices being used by the children, go through their browser's history. At some points parents must try to see on the screens and identify the reactions of the children.
Know your parental controls	Act as a responsible parent
Who are your kids online friends	Identify who they chat with online

Be ‘share aware’ to protect your privacy	Teach them what not to share online
Keep control of your family’s digital footprint	Have those family discussions about online
Keep track of online time	Take note of how much time the children spend online and if it’s worth it.
Be Social Network Savvy	Be a parent who is adept full knowledge and in a simply way you can say an expert.
Lead by example	Parents must guide the children through their behaviour instead of their words as a parent. Your intention as a parent is to inspire your children to copy your behaviour.



Tips for parents, carers and guardians

Have a discussion with your children try and **do some online activities with them.**

Identify the technology, devices and services across your family / household.

Consider whether **filtering and blocking or monitoring programmes** can help and support your family.

Agree expectations as a **family about using the internet** and personal devices.

Be aware of the **online and mobile services** used by your children.

Consider age of digital consent.

Control **use of credit cards** and other payment mechanisms.

Know **how to report problem.**

Be aware that **advertising can be inappropriate** or misleading.

Create a **culture of support** in the home so that children and young people feel able to seek support.

Educate children on the **dangers of meeting up** with a stranger.

Help your children understand and **manage their personal information.**

Ensure children and young people understand what it means to **post photographs** on the Internet.

Figure 2-1: Tips for parents, carers and guardians

According to the Nigerian Communication Commission (NCC) the combination of the internet and children has produced new worry as identified, it has introduced the high need for caregivers and parents to be widely responsible. From the start of time worry of privacy and safety have been with us. However, what has changed is the borderless and invisible way of all these worries and the degree of consequences of bad online parenting, when they occur.

Out of the participants 50% are aware that children face several risks on the internet, which them as parents also face at some points while online. A group of four categories of risk is identified.

1. **Content Risk:** This include harmful objects and information which kids can get online.
2. **Contact Risk:** Getting in contact with wrong friends online and they mis-lead them to wrong routes.
3. **Conduct Risk:** This includes addiction to games, loss or lack of confidence, harm reputationally and the overuse of mobile phones because of wrong comments or unguided.
4. **Commercialization Risk:** Children are forced to do online payment and exposed to different online commercial decisions willingly or unwillingly.

The COP DB will be used to capture some of this information and insure that they are secured in order to be used as the evidence of how to secure children online. Furthermore, if these data are kept in the DB which is not secured it can cause the data to tempered with which will affect the solution to secure children while online.

2.6. SECURE TECHNIQUES AND METHODS FOR ACCESSING DATA IN DATABASE

Most of the misconfiguration, vulnerabilities of software, or patterns of carelessness or misuse can cause violation. According to Imperva (2021) a number of different cyber threats on database security and known causes are identified.

Figure 2 show different methods how to secure a database, based on the observation done on different database I have developed as software developer in my work place 100% of these methods are used. Different case studies indicated that these are the modern techniques to secure a database. Databases protection is essential to numerous industries and sectors, which include finance, banking, eCommerce, and IT (Thomas, 2020). Most of your transactions are depend on your secure database because it holds vital details different unique details, etc. The database administrator is responsible to setup these attributes, or use other needed measures on security, to address the consent and security requirements of their information and data (Azrieli, 2021).

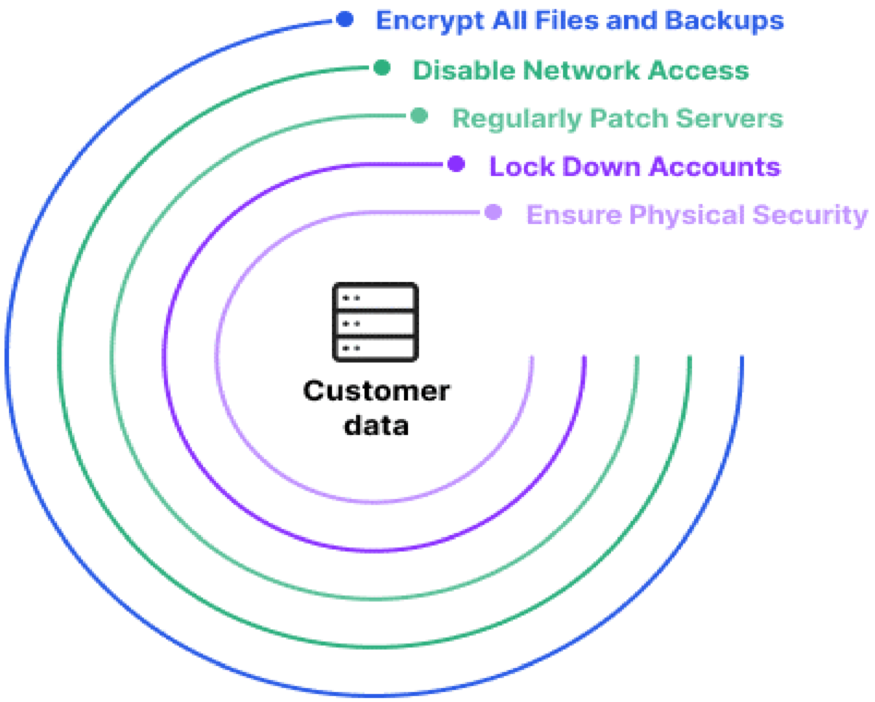


Figure 2-2: How Can You Secure Your Database Server?

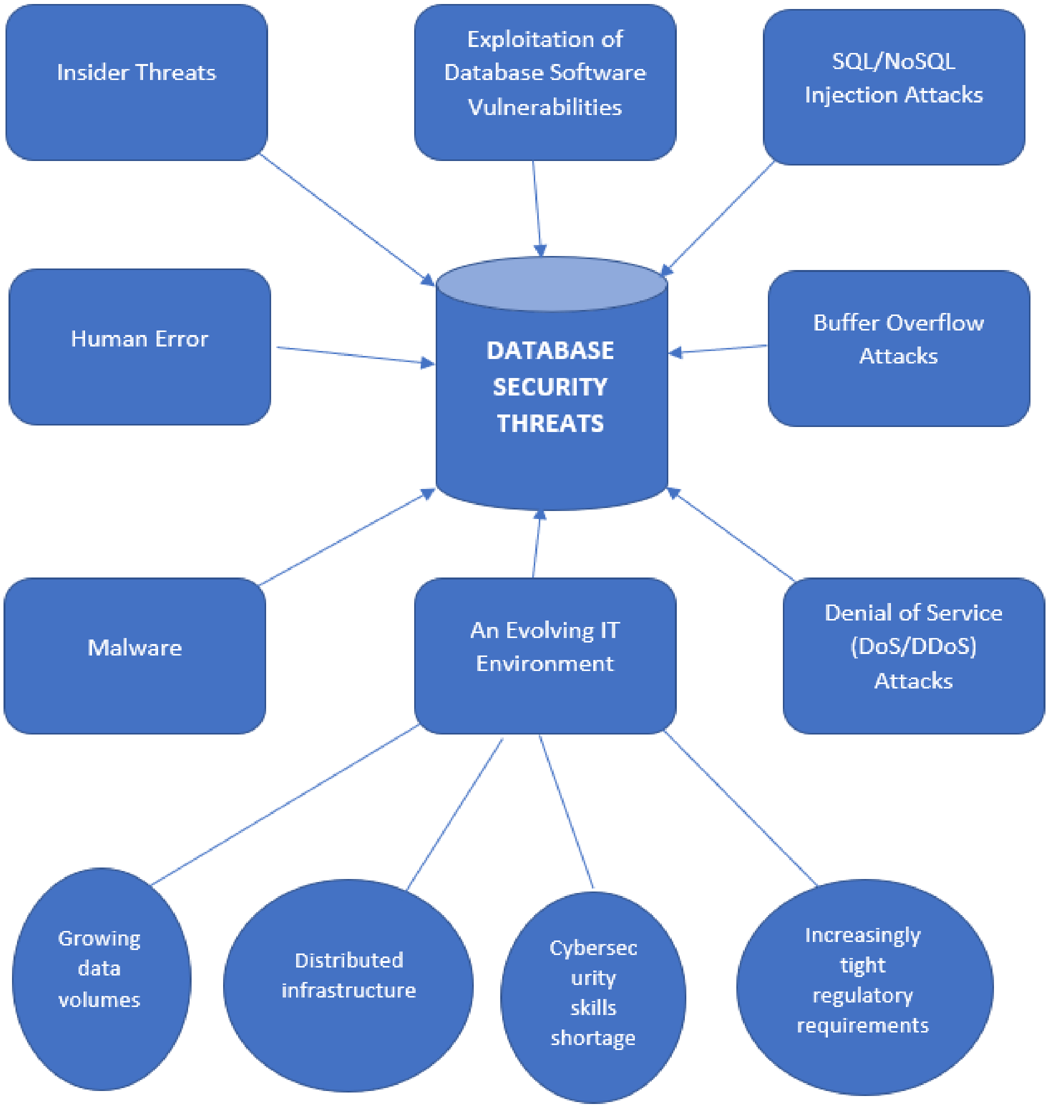

Insider Threats
Exploitation of Database Software Vulnerabilities
SQL/NoSQL Injection Attacks
Human Error
DATABASE SECURITY THREATS
Buffer Overflow Attacks
Malware
An Evolving IT Environment
Denial of Service (DoS/DDoS) Attacks
Growing data volumes
Distributed infrastructure
Cybersecurity skills shortage
Increasingly tight regulatory requirements

Figure 2-3: Database Security Threats

According to Imperva (2015) by following good practice and implementing some steps can prevent threats on database security and control it internally. Because each threat is involving many attack vectors in different ways, a complex guarding way is needed to protect the database properly. Table 2-2 shows the solutions identified for each main threats on the database (Imperva, 2015).

Table 2-2: Database Security Solutions to the identified threats

Assessment and Findings	Identify where critical and susceptible data is
Management on user rights	Introduce different user access rights to data which are more sensitive.
Blocking and Monitoring	The database must be protected from theft of data, different attacks and unauthorized access.
Auditing	Audition of the database to compile with the regulations of the industry.
Protection of Data	Requirement of security mainly includes confidentiality and integrity as explained in section 2.2.
Non-technical and physical security	Preparedness and awareness of security culture must be reinforced.

2.7. SECURITY PROBLEMS OF DATABASE ACCESS

Security on database is very challenging and difficult aspects which involves all parts of practice and information on information security (IBM Cloud Education, 2019). As the database is used and accessed mostly than the is on high risk to threats on (IBM Cloud Education, 2019).

The database network system gets more better if the applied security is powerful (Mahamod, B. 2014). Although a database is already protected by firewall or router, it as well need additional of more security techniques for it to increase and speed up the degree of protection on all important information and data (Thuraisingam, B. 2005). There are requirements operations needed on the database when the software is deployed. This include Create, Retrieve, Update and Delete (CRUD). These operations are done with no test on performance of the database on the application, reliability and security, the crash of the whole system, updates or deletions, logical structure internally (Reza, 2011). According to Sree (2016), testing of a software is the procedure of figuring out the software defects, subjecting and isolating them for correction, supplying of system quality information to collaborators with the investigation of any system on test (Berger, 2016).

In many points vulnerability of data is in most computer system. Different types of functionalities and security techniques can be implemented for protecting it. Furthermore, if there's no any privilege defined as an access permission to an identified object in an ordered way, it can result into DB access security problem. There are two distinct (ORACLE, 2002) privileges types within a database:

1. **System privileges** (ORACLE, 2002) this give permission to users to do particular actions within the system, perform certain actions on a schema. For example, insertion of a row, table creation or delete a row in a database table.
2. **Schema object privileges** (ORACLE, 2002) permit users to carry out certain actions on a specific schema object.

The destruction and violation of your brand can be caused by failing to protect a database that contain sensitive data for your major operations (Imperva, 2015). Mastering the main database threats as shown in figure 4-4 and implementing the solutions outlined in table 4-2 will allow to realize when you're being attacked or vulnerable, ensure best security practices, and guarantee the protection of your high valuable assets (Imperva, 2015).

According to the Verizon Data Breach Report of 2014, database is one of the high advantageous assets. The fact that mostly databases are the main target is very simple: they are used for records and other confidential data, and they are at the heart of most organizations (Imperva, 2015). But why are databases so vulnerable to breaches? Protection of most crucial assets in many organizations is not well maintain and implemented. According to IDC, less than 5% of the $27 billion put on products for security straight addressed the data centre security. Furthermore, the great outcome is the hugest of incidents– more than 97% according to the Online Trust Alliance (OTA) in 2013 – might be prevented by the implementation of easy procedures and following the great exercise and internal controls.

2.8. CHAPTER SUMMARY

This chapter focused on demonstration of the literature of each sub-objective of this research and different components which indicated the importance of Children Online Protection data security. Developing a secure Child Online Protection Database System will be ensured by secure data access and data integrity for the data and information collected about children online abuse. This data will provide information which will be used to find ways or solution of ensuring children online protection.

CHAPTER 3 : RESEARCH METHODOLOGY

3.1. INTRODUCTION

Methodology defines the procedure applied for data and information collection as the reason for business decision making (Bryman, 2007). Research methodology is the specific technique or procedure used to select, identify, process and analyse information on a certain topic. The section of methodology in research it allows the examiner or reader to evaluate all importance of the study for reliability and validity.

Table 3-1: Research objectives and tools used to achieve them

Objective	**Research approach/strategy/technique and tools**	**Why are they appropriate supported by literature**
Design a prototype of a secure database access module.	SDLC Waterfall model	Providing what you are proposing and get a feedback before actual design it helps in getting more knowledge and improve on the solution.
Designing an authentication module in context for the development of a secure COP Database and to the NUST network.	phpMyAdmin, MySQL, SDLC, Waterfall model	The authentication module can as well apply to other databases.
Identify techniques and methods to access the database data.	Quantitative research using a derived method to find out from previous reports, articles and books on database authentication and COP DB.	Most research related to database and security have introduced different way of accessing a database.
Propose solutions to best mitigate the security problems at the COP Database and NUST network.	Derived Method	It's not always possible to provide a solution without knowing the problem.
To identify current COP Database security challenges.	Derived Method	Technology keeps on changing or upgrading.

3.2. THE RESEARCH DESIGN

The design of a research helps to identify the clear structure of a study. A good research design decision process is a decision applied based on the research address because it decides how to get specific information for a study; however, it also includes different linked decisions (Kassu, 2019).

This study is focused on a quantitative method. Quantitative research, according to Van der Merwe (1996), is an approach for research aimed at facts determination, theories testing, predicting out comes and relationship between variables demonstration. It uses procedures from the natural science which are designed guarantee reliability, generalizability and objectivity (Weinreich, 2009). Quantitative research uses different techniques which includes accidental choice of participant, intervention they receive or questionnaire which are standardized and statistical methods used for testing identified hypotheses based on certain variable relationship.

3.3 RESEARCH METHODS

Descriptive research uniqueness partly lies in its ability to explore both quantitative and qualitative research methods. Therefore, researchers have the opportunity to use a wide variety of techniques that aids the research process, when conducting descriptive research.
Descriptive research explores research problems in-depth, beyond the surface level thereby giving a detailed description of the research subject. That way, it can aid further research in the field, including other research methods.

The method used for the research is to ensure that the information helps the researcher to reach the main goal of the study. For this study, the method was based on experiment and evaluation of the literature review findings. It will be ensured that it follows the Software Development Life Cycle using a waterfall model and it have effects on the research goal. The SDLC Waterfall Model is a software development life cycle model that was originally defined by Royce around 1970 Sherrell L. (2013). The process consists of the following phases:

1. Requirements (the needs of the study are collected which is the main objective as described in section 1.4).
2. Specification (a formal explanation containing the requirements is constructed).
3. Design
    - Architectural – the modules for the program are specified.
    - Detailed Design – the algorithms and the data structures are defined.
4. Implementation (coding of the COP DB is completed).
5. Unit Testing (the COP DB components are tested individually).
6. Integration Testing (the components are combined and tested).
7. Post-delivery Maintenance (corrections or enhancements are made to the code).
8. Retirement (the code can no longer be maintained or is obsolete so it is removed from service)

3.4. DATA COLLECTION INSTRUMENTS

Quantitative data from the literature review of different findings, researches and reports in the past as explained in chapter 2 assisted in ensuring a valid method in conducting this research. Many literature reviews of past research and different views indicated different security challenges and solutions on how to secure a database.

3.3.1. DESIGN AND PROTOTYPE AND A SECURE DATABASE ACCESS MODULE

The Software Development Life Cycle (SDLC) Waterfall model is the method which will be used to design. The secure database access module was designed and developed based on the methods shown in figure 2 on how to secure a database. Studies and literature review were conducted on what to be implemented to ensure that those methods are valuable and will help in future on securing a database. The design and development of the access module is explained and shown in chapter 4 based on the experiment done. The module is tested and the results was analysed.

3.5. DATA ANALYSIS

The summary of data collected is done in analysis of data. This includes the explanation of the gathered data between trends or relationships, logical line of thoughts and analytical to identify patterns. With the quantintative type of research that is being conducted in this research data will be more analyzed in a mathematical manner (Galetto, 2018).This are the steps (Galetto, 2018) to follow in analyzing the data:

- **Objectives decision** – Decide on objectives for information to develop a quantifiable method to decide wether the research is go forward to its goal;
- **Business levers identification** – Identify metrics, levers, and goals on projects for analysing data give the main focus and scope (Molly, 2016)..
- **Cleaning of data** – Aspect of data improvement to produce correct results and prevent making wrong reasoning(Molly, 2016).
- **Grow a data science team** – Provide the team with the big amount of platforms for data analysis they have to automate the collection and analysis of data (Molly, 2016)..
- **Repeat and optimize** – Ensure best data analysis representation so that the procedure can be done continuously to produce clear predictions, goal reaching, and report and monitor always (Molly, 2016)..

Testing of data plays a huge role in software development. The access module is tested and data is needed. This data needs to meet certain requirements in order to ensure that the tests are successful and reliable and that the developed access module is secure and all techniques are implemented. The results obtained from testing the module as shown in chapter 4 was used to identify that this study have a good role on COP DB security and also to other organizations, because a database is a heart of most organization where sensitive and important data are kept.

3.6. LIMITATIONS

Due to time and other responsibilities the research was only done on previous research under results on literature review. According to Saunders et al. (2009), the main backbone of research study research methodology. Quantification of data is the main purpose of quantitative research. It permits conclusion of the findings by sample population responses and views measurements. Each research methodology contains two major stages namely planning and execution (Younus 2014). For this, it's obvious that with these two stages, there are limitations involved which we can't control (Simon 2011). Qualitative research method could be used for this research but because of time, cost, the inability to control the environment and many other reasons limited this research to focus on the Quantitative research methods. The main limitations included:

1. Time
2. Access to reliable information sources
3. Who to approach for the study findings
4. Accuracy of the findings
5. How the research study must be done

3.7. ETHICAL CONSIDERATIONS

There are several responsibilities for research conductor which include identifying the research problem statement that have to be focused on during the research. The responsibility of a researcher includes:

- Recognize that self-development is your responsibility
- Embrace training and development opportunities
- Seek advice and mentoring on career development from the supervisor
- Engage positively with the Performance and Development Review
- Actively develop the ability to transfer and exploit knowledge
- Conduct and disseminate research in an honest and ethical manner
- Have honest, critical and independent thought

Ensuring or approving that the research processes, documentation and conducting is on point is the responsibility of the research supervisor. Selecting a research tittle is limited to the field of study and area to focus on based on the supervisors and they are the one to accept the research tittle. If it was not because of time, finance and other limitation the research tittle could be submitted to different organizations and professors for comments and approving its relevant.

Ethical considerations (Quadri) in research are critical. Ethics are standards or norms to differentiate between right and wrong. They assist on identifying between behaviors which are acceptable and unacceptable. According to Bryman and Bell (Bryman, 2007) there are ten points which represent the most important approach relatedd to ethical consideration. This study ethical consideration included:

1. All type of communication in relation to the research was done with honesty and transparency.
2. Primary data findings in a biased way is avoided.
3. Confidentiality and reference of all findings

3.8. CHAPTER SUMMARY

This chapter has outlined the aim of the study and how it was conducted using the quantitative method. The data collected was outlined from the literature review in chapter 2. All data collected for this research were explained and analysed in this chapter. This result will be used to answer and solve the research questions. Furthermore, this will help to secure children while online and improve on different weaknesses which are currently causing children online cyberbullying and different attacks. The different security challenges within databases, threats, solutions to threats and solution on how to secure a database it was all outlined in this chapter.

CHAPTER 4 THE DESIGN AND DEVELOPMENT OF A SECURE ACCESS MODULE

4.1. INTRODUCTION

The previous chapter it explains about the research methodology, tools used for data collection and the limitation on this. This chapter will narrate the findings by developing a secure access module. The results are reported and reveals the analysis.

According to Northeastern University (2014) the purpose of SDLC is to create good software that has visibility with minimum risks, reduce costs and to develop the software in the shortest time possible. The SDLC aims to produce a high-quality software that meets or exceeds customer expectations, reaches completion within times and cost estimates (TutoriasPoint). The primary objectives of SDLC are to ensure the delivery of high-quality systems using strong management controls to maximize productivity (Monika, 2013). The main widely used and well known SDLC includes: V-shaped, waterfall and evolutionary rapid.

This chapter presents how the authentication module was designed using the waterfall model in fulfilment of the main objective of the study. Waterfall model is a sequential model that divides software development into five (5) as shown in Figure 4-1. Each phase must be completed before the next phase can begin with no overlap between the phases. Each phase is designed for performing specific activity during the access module design and development (Mathew, 2021). Figure 4-1 shows the model different phases which will be followed to design the authentication module to secure COP DB based on the literature review presented in chapter 2.

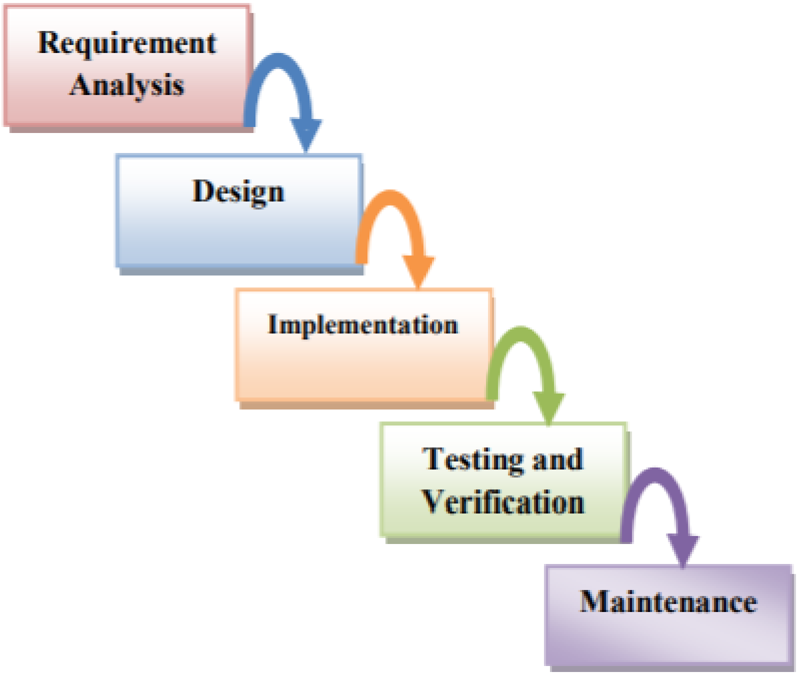


Figure 4-1: Waterfall model phases

Table 4-1 presents the different phases of the Waterfall model, how each phase is performed and the delivery or results of each face. Furthermore, each phase will be explained in detail on what was done to reach the study requirement and achieve the main objective of the study.

Table 4-1: The activities involved in different phases

PHASE	**Activities Performed**	**Deliverable**
Phase 1 Requirement Analysis	What is main use of the COP DB? What are the current security challenges of the COP DB?	Requirement understanding is needed in this phase. During my internship in 2017, I was managing the COP DB, where I identified

	How will a secure COP DB help with securing children while online? What are the solutions to secure a COP DB or DB in general?	the need of a secure COP DB. The data kept in the COP DB, it's the one used to find a solution on how to secure children online for example based on different risk the children can face while online. COVID-19 pandemic impact has created a new normal and a shift in the traditional ways of doing many things. This change has also moved education from the classroom to mobile phones, tablets, laptops, and desktops or a blend of both. • Secure and accessible by authorized users. • Understandable and with all the techniques explained in chapter 4 are implemented. • Free from errors. • Usable for the future
Phase 2 System Design	1. As per the requirements, create the design	Design the secure access module for which will be

	2. Capture the software requirements. 3. Document the designs	implemented in the COP DB based on the findings in chapter 4.
Phase 3 Implementation	1. As per the design in phase 2 create the programs / code 2. Integrate the codes for the next phase. 3. Unit testing of the code	Actual development of the COP DB using phpMyAdmin takes place in this phase to implement the secure access module designed in phase 2.
Phase 4 System Testing	Did we meet the requirements? Is the COP DB Secure? Is there any anomaly? Are the results from the testing meeting the main objective?	1. Integrate the unit tested code and test it to make sure the access module works as expected. 2. Perform all the testing activities (Functional and non-functional) to make sure that the COP DB meets the requirements.
Phase 5 System Deployment and Maintenance	Ensure the COP DB is up 2. The system is running. 4. Deploy the application in the respective environment. 5. Perform a sanity check in the environment after the application is deployed to ensure the application does not break. Ensure sure that the application is up and running in the respective	User Manual which explain how the system works. Environment definition / specification where the COP DB will run from. List of new features implemented.

	environment. 2. Incase user encounters and defect, ensure to note and fix the issues faced. 3. In case any change in the system; the updated code is deployed in the environment.	

4.2. PHASE 1 REQUIREMENT ANALYSIS

In this phase, detailed requirements of the software system to be developed are gathered, this includes the introduction and background of the study as explained in chapter 1. The access module should meet the following requirements:

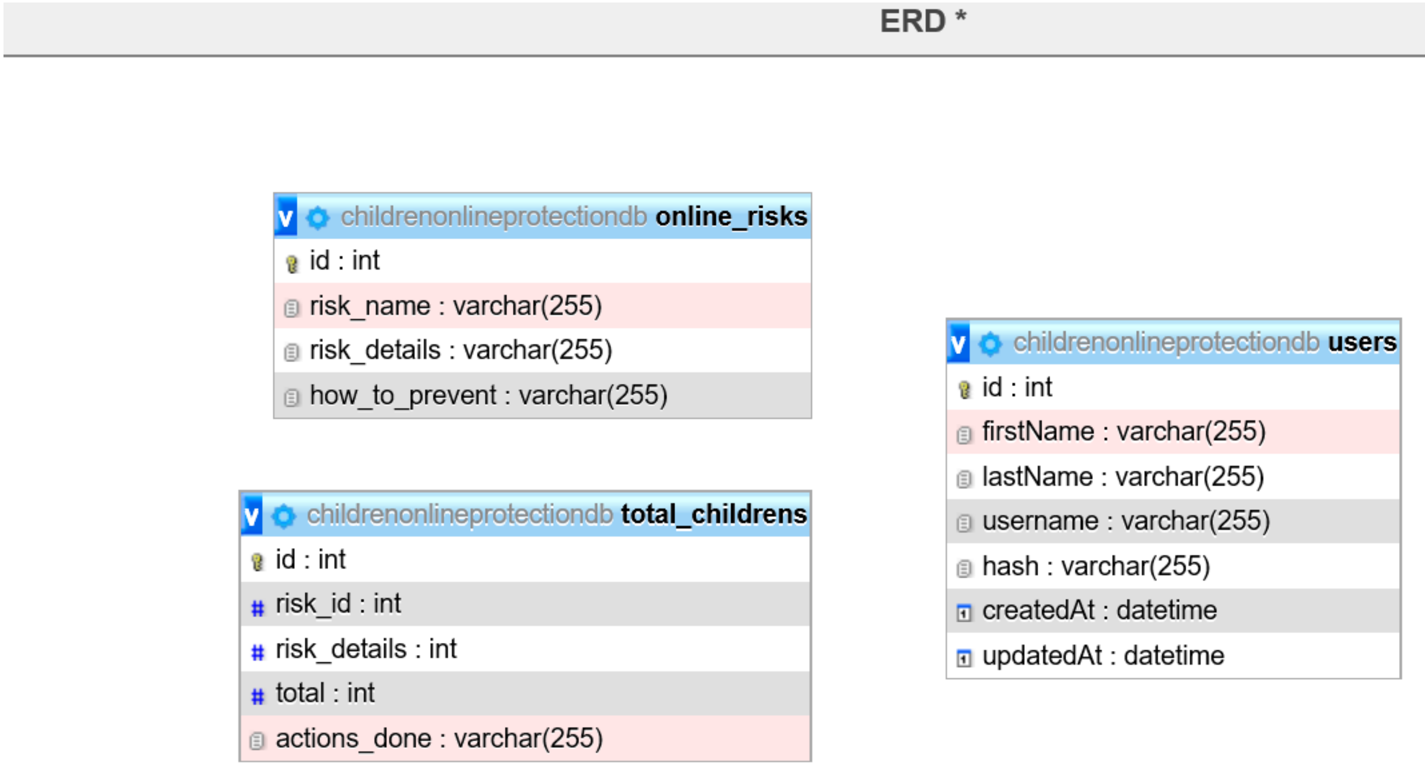
1. Secure and accessible by authorized users
2. Understandable and with all the techniques explained in chapter 4 are implemented
3. Free from errors
4. Usable for the future

4.3. PHASE 2 SYSTEM DESIGN

Phase 2 of the SDCL focuses on planning the programming language for development of the access module for the COP database and other high-level technical details of the study. The design will be implemented based on the literature in chapter 2 section 2.7, section 2.6 and the Database Security Solutions to the identified threats as described in table 2-2. Oracle Corporation suggested that where there is a chance, , you build applications in which the users of the application are the database user. In this way you can leverage the intrinsic security mechanisms of the database (ORACLE, 2016). Figure 4-3 contains the different users and the different security features of the access module. All users to access the DB, they have to go through the access module as the main entrances to access the DB. These users will be implemented and validated in the COP DB, in order for them to access the DB. The users will be granted different permissions as follow:

1. **Root and Admin user:** This is the main user who has all permissions to the COP database, which include create:
    - ALL – Permits the full access to the database
    - CREATE – Users can create the tables and other database dependencies
    - DELETE – Deletion of table rows.
    - DROP – The user can drop the tables and entire database.
    - EXECUTE - The user can perform execution on different routines. GRANT OPTION – This permits the user to give or remove privileges of other users. .
    - INSERT - Allow a user to insert rows from a table.
    - SELECT - Allow a user to select data from a database.
    - SHOW DATABASES- Allow a user to view a list of all databases.
    - UPDATE - Allow a user to update rows in a table.
2. **Superuser:** This can now be defined as user that can only**:**
    - EXECUTE - Allow a user to execute stored routines.
    - INSERT - Allow a user to insert rows from a table.
    - SELECT - Allow a user to select data from a database.
3. **Users:** This user can only view the data:
    - SELECT - Allow a user to select data from a database.

Figure 4-2 shows the main database Entity Relationship Diagram. The DB will have different tables were the data will be stored and secured by the access module being developed. database techniques and methods which will be implemented based on the literature review findings as explained in chapter 2 section 2.6. These techniques will help in achieving the security solutions explained in chapter 2 section 2-6 table 2-2. Furthermore figure 4-4 shows the access module with different features which will make it secure and indicate how the COP DB will be accessed, the features which will secure the DB before any access and it will be the main entrance or gate to access the COP DB will be through the access module.



ERD *

childrenonlineprotectiondb **online_risks**
id : int
risk_name : varchar(255)
risk_details : varchar(255)
how_to_prevent : varchar(255)

childrenonlineprotectiondb **total_childrens**
id : int
risk_id : int
risk_details : int
total : int
actions_done : varchar(255)

childrenonlineprotectiondb **users**
id : int
firstName : varchar(255)
lastName : varchar(255)
username : varchar(255)
hash : varchar(255)
createdAt : datetime
updatedAt : datetime

Figure 4-2: COP database Entity Relation Diagram

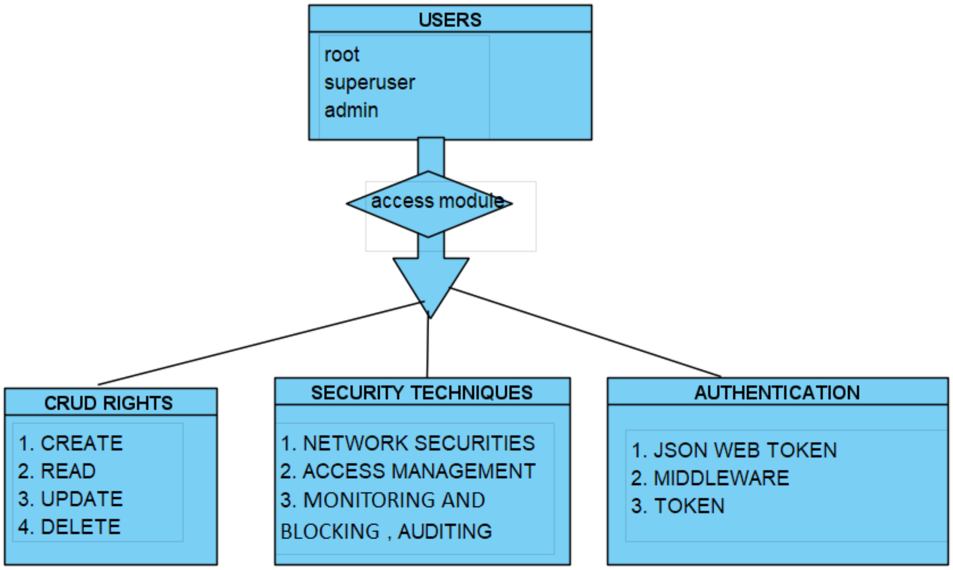


Figure 4-3: Access Module Class Diagram

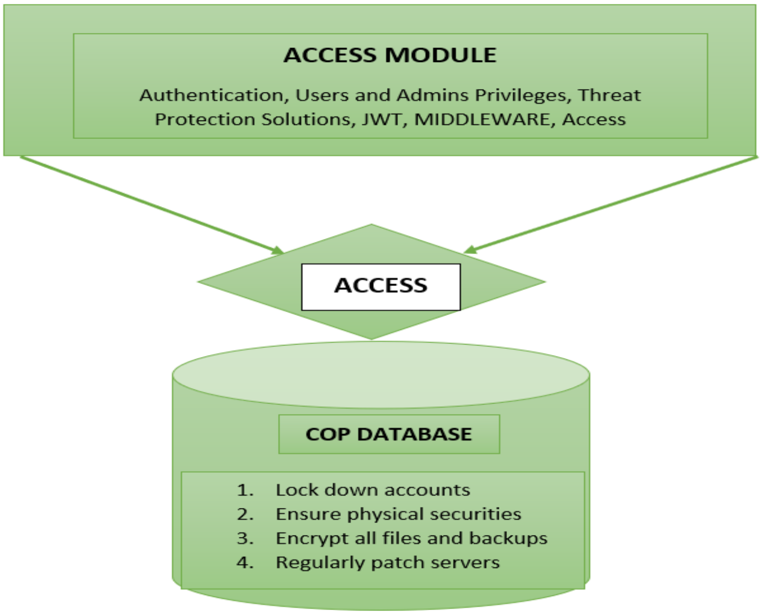
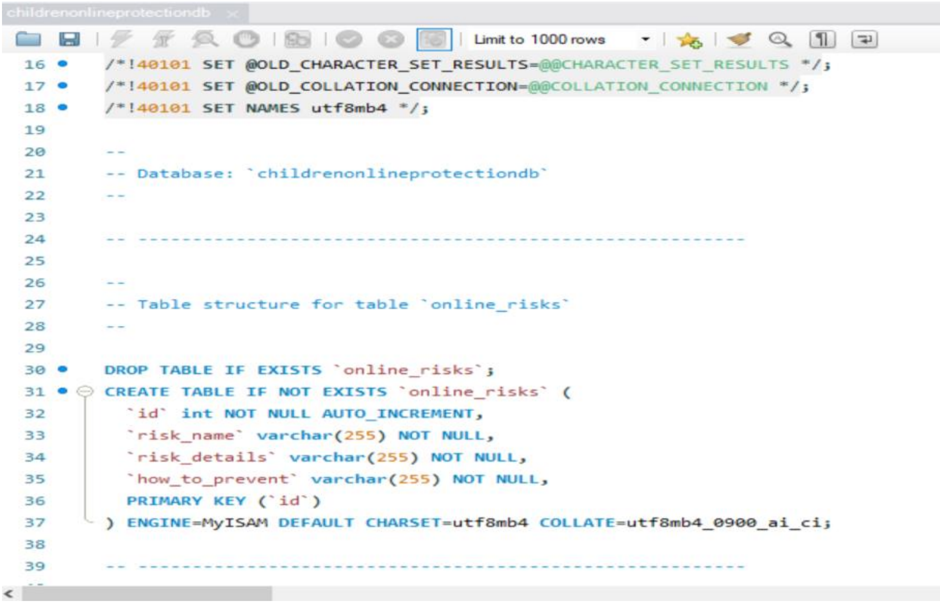

ACCESS MODULE
Authentication, Users and Admins Privileges, Threat
Protection Solutions, JWT, MIDDLEWARE, Access
ACCESS
COP DATABASE
1. Lock down accounts
2. Ensure physical securities
3. Encrypt all files and backups
4. Regularly patch servers

Figure 4-4: COP DB Secure Access Module design

4.4. PHASE 3 IMPLEMENTATION

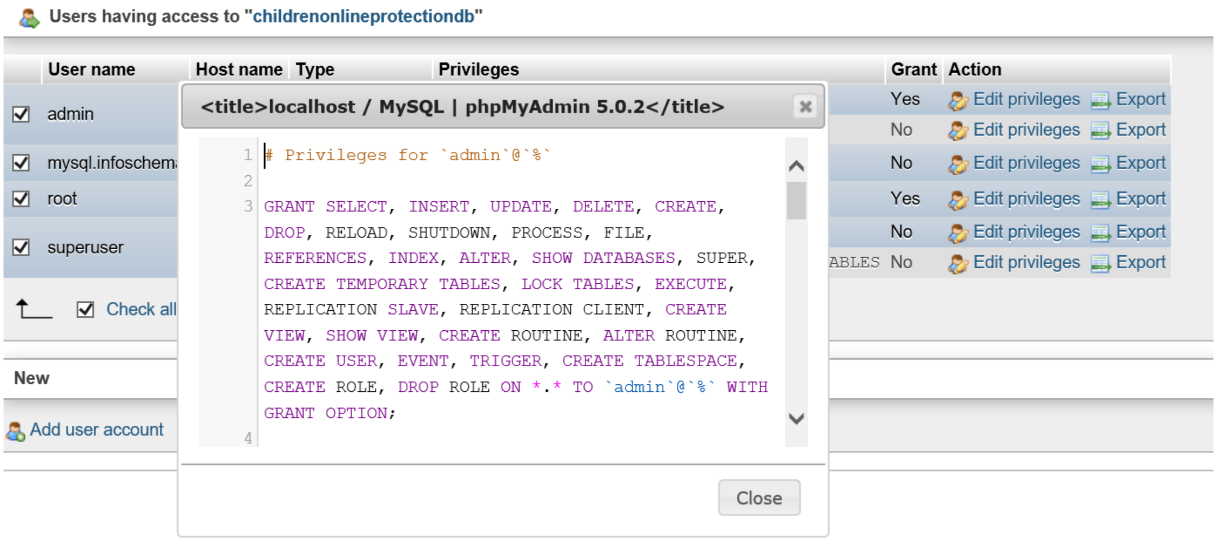
After design phase, it is the implementation phase. This is where coding the software takes place. The development section contains the front-end, back-end and the database development, but for this study it will only focus on the database development. Figure 4-5 shows the database SQL query code which developed the database, the tables and different security features. The database was developed on the localhost server and it can only be accessed through the local machine using the following link: http://localhost/phpmyadmin/server_privileges.php?db=childrenonlineprotectiondb&checkprivsdb=childrenonlineprotectiondb&viewing_mode=db

The access module is implemented with users' privileges, network security and access management. Figure 4-6 indicates the code which was compiled to create the access module and users' privileges. This can only be accessed and changed by the root user.



```
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;

--
-- Database: `childrenonlineprotectiondb`
--

-- --------------------------------------------------------

--
-- Table structure for table `online_risks`
--

DROP TABLE IF EXISTS `online_risks`;
CREATE TABLE IF NOT EXISTS `online_risks` (
  `id` int NOT NULL AUTO_INCREMENT,
  `risk_name` varchar(255) NOT NULL,
  `risk_details` varchar(255) NOT NULL,
  `how_to_prevent` varchar(255) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;

-- --------------------------------------------------------
```

Figure 4-5: Database SQL query



Users having access to "childrenonlineprotectiondb"

	User name	Host name	Type	Privileges	Grant	Action
☑	admin				Yes	Edit privileges Export
					No	Edit privileges Export
☑	mysql.infoschem				No	Edit privileges Export
☑	root				Yes	Edit privileges Export
☑	superuser				No	Edit privileges Export
				ABLES	No	Edit privileges Export

☑ Check all

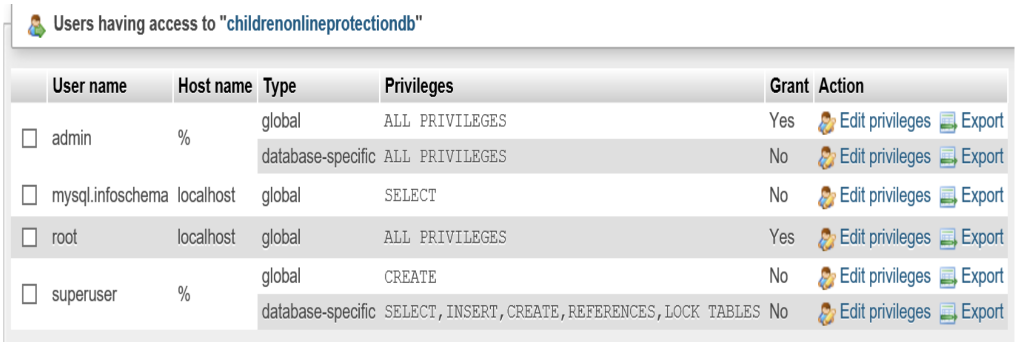
New

Add user account

<title>localhost / MySQL | phpMyAdmin 5.0.2</title>

```
# Privileges for `admin`@`%`

GRANT SELECT, INSERT, UPDATE, DELETE, CREATE,
DROP, RELOAD, SHUTDOWN, PROCESS, FILE,
REFERENCES, INDEX, ALTER, SHOW DATABASES, SUPER,
CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE,
REPLICATION SLAVE, REPLICATION CLIENT, CREATE
VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE,
CREATE USER, EVENT, TRIGGER, CREATE TABLESPACE,
CREATE ROLE, DROP ROLE ON *.* TO `admin`@`%` WITH
GRANT OPTION;
```

Figure 4-6: Access module and users privilege code implementations



Users having access to "childrenonlineprotectiondb"

	User name	Host name	Type	Privileges	Grant	Action
□	admin	%	global	ALL PRIVILEGES	Yes	Edit privileges Export
			database-specific	ALL PRIVILEGES	No	Edit privileges Export
□	mysql.infoschema	localhost	global	SELECT	No	Edit privileges Export
□	root	localhost	global	ALL PRIVILEGES	Yes	Edit privileges Export
□	superuser	%	global	CREATE	No	Edit privileges Export
			database-specific	SELECT,INSERT,CREATE,REFERENCES,LOCK TABLES	No	Edit privileges Export

Figure 4-7: Different users and their privileges

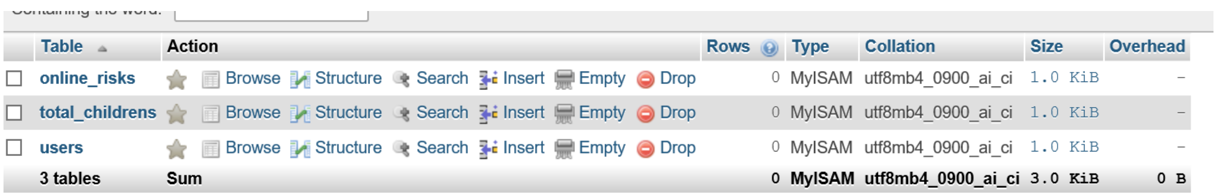


	Table	Action	Rows	Type	Collation	Size	Overhead
□	online_risks	Browse Structure Search Insert Empty Drop	0	MyISAM	utf8mb4_0900_ai_ci	1.0 KiB	-
□	total_childrens	Browse Structure Search Insert Empty Drop	0	MyISAM	utf8mb4_0900_ai_ci	1.0 KiB	-
□	users	Browse Structure Search Insert Empty Drop	0	MyISAM	utf8mb4_0900_ai_ci	1.0 KiB	-
	3 tables	Sum	0	MyISAM	utf8mb4_0900_ai_ci	3.0 KiB	0 B

Figure 4-8: COP Database Structure

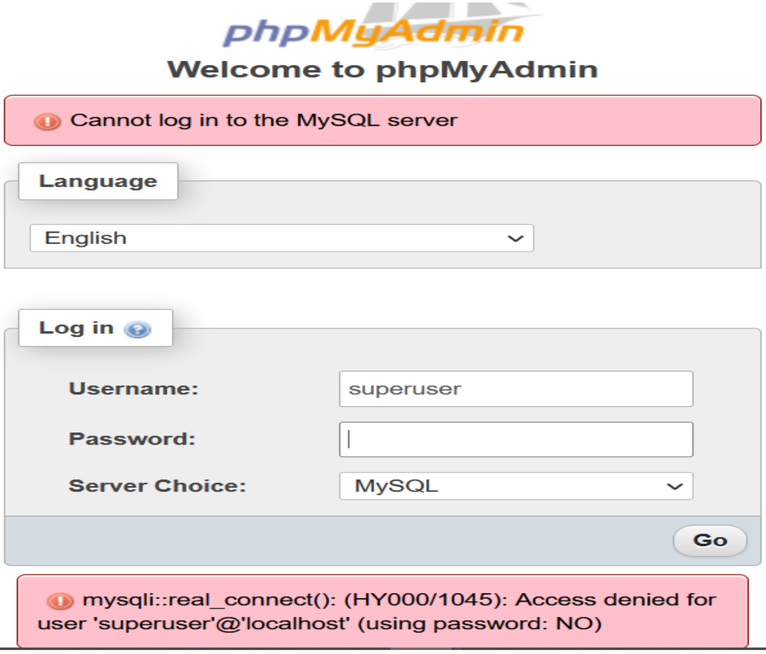
4.5 PHASE 4 TESTING SYSTEM

Phase 4 is where testing of the COP DB is deployed to ensure that the database is secure and the access module was implemented and the requirements was met. Usually, the security of network database system relies on network database management systems top a great degree.

The tests conducted were:

1. Accessing the COP DB with different user details
2. Use different privileges on user which is not assigned to that specific user
3. The validity of the Access module
4. Registration of user with unauthorised details
5. Accessing with correct details

Figure 4-9 show the error which display if one tries to access the COP DB with invalid user login details, monitoring and blocking as one of the database security solution as explained in chapter 2 section 2.6 and 2.7 table 2-2 is achieved here. Figure 4-10 indicates the error after a superuser tries to create a table in the COP DB, which is not part of its privilege permissions performs a privilege which is not assigned to the user, based on the explanation of user permissions in section 4.3. If the user has the specific privilege that’s when they can access it and perform it within the COP DB.



Welcome to phpMyAdmin

Cannot log in to the MySQL server

Language: English

Log in

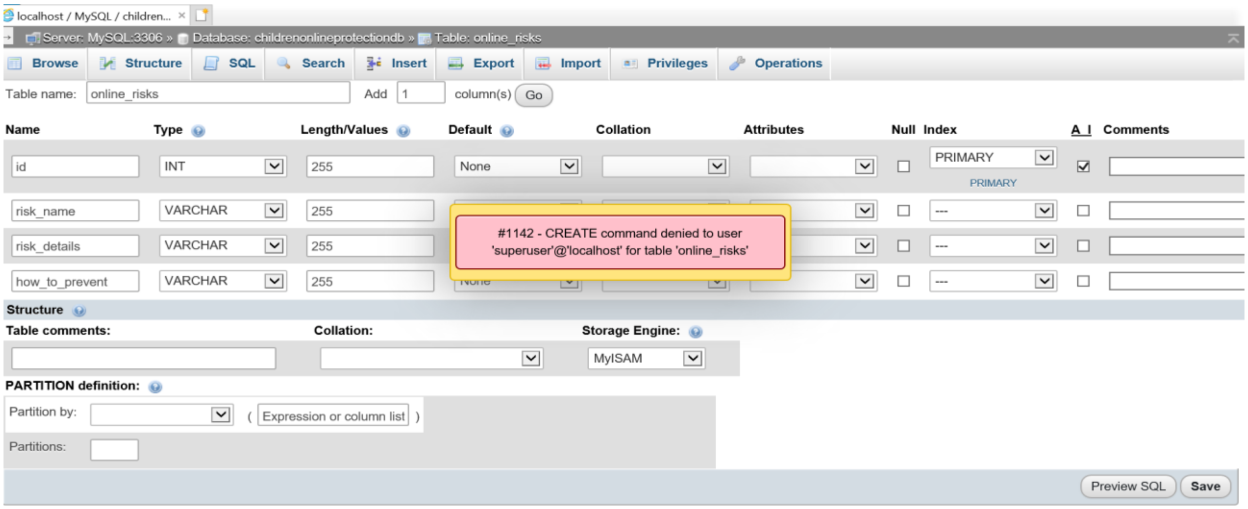
Username: superuser

Password:

Server Choice: MySQL

mysqli::real_connect(): (HY000/1045): Access denied for user 'superuser'@'localhost' (using password: NO)

Figure 4-9: Accessing the COP DB Denied



localhost / MySQL / children...

Server: MySQL:3306 » Database: childrenonlineprotectiondb » Table: online_risks

Table name: online_risks   Add 1 column(s)

Name	Type	Length/Values	Default	Collation	Attributes	Null	Index	A_I	Comments
id	INT	255	None			□	PRIMARY PRIMARY	☑	
risk_name	VARCHAR	255				□	---	□	
risk_details	VARCHAR	255				□	---	□	
how_to_prevent	VARCHAR	255	None			□	---	□	

#1142 - CREATE command denied to user 'superuser'@'localhost' for table 'online_risks'

Structure

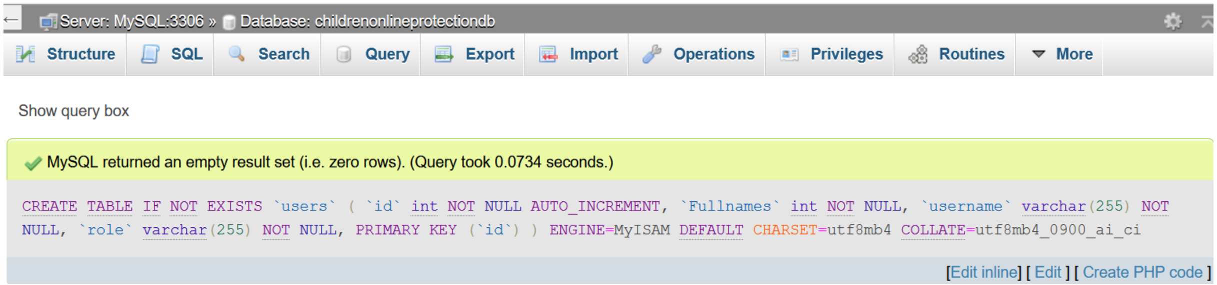
Table comments: Collation: Storage Engine: MyISAM

PARTITION definition:

Partition by: (Expression or column list)

Partitions:

Figure 4-10: Privilege access


Server: MySQL:3306 » Database: childrenonlineprotectiondb
Structure
SQL
Search
Query
Export
Import
Operations
Privileges
Routines
More
Show query box
[Edit inline] [Edit] [Create PHP code]

MySQL returned an empty result set (i.e. zero rows). (Query took 0.0734 seconds.)

```
CREATE TABLE IF NOT EXISTS `users` ( `id` int NOT NULL AUTO_INCREMENT, `Fullnames` int NOT NULL, `username` varchar(255) NOT
NULL, `role` varchar(255) NOT NULL, PRIMARY KEY (`id`) ) ENGINE=MyISAM DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci
```

Figure 4-11: Access to the database

4.6. PHASE 5 SYSTEM DEPLOYMENT AND MAINTENANCE

The deployment and maintenance phase will be the final phase of the software development life cycle (SDLC) and puts the product in use. The user manual will be compiled which will guide the user on how to use the COP DB. Once the system is ready to use, it may later require change the code as per requirements if any. This stage can be continuous based on how the database is upgrading, new users and new security techniques to be implemented.

4.7. CHAPTER SUMMARY

This chapter focused on the design of an authentication module to secure the COP DB and outlines the SDLC Waterfall model processes in order to achieve the main objective of the study in development of the access module. The researcher also outlined the design and development using phpMyAdmin and MySQL as shown in section 4.4 which explain the implementations and this is based on the literature reviews of each sub-objective explained in chapter 2.

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS

5.1. INTRODUCTION

The last chapter provides further explanations for the results from the study. This section also usually future work and conclusions that focuses on the current status and future of the Child Online Protection Database Security. The study and speculates on what the results say about the problem(s) identified in the research question(s).   This study focused on securing the COP DB by developing a secure access module.

Figure 5-1 shows the three pillars of information security which was used to achieve the sub-objective as found in chapter 2 section 2.5 to section 2.7, the solutions and results are explained in table 2-2. Confidentiality, Integrity and Availability, often referred to as the CIA triad (has nothing to do with the Central Intelligence Agency!), are basic but foundational principles to maintaining robust security in a given environment (Cranford, 2021). The CIA triad is useful for creating security-positive outcomes.

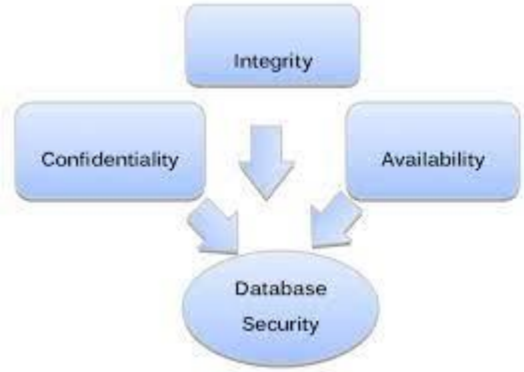


Figure 5-1: Three main pillars of Information Security

Figure 5-2 outlines the secure techniques and methods for accessing data in databases. These techniques are outlined in chapter 4 section 4.3 to achieve the sub-objective of Secure

“Techniques and Methods for Accessing Data in Databases”, which are used to design the secure access module in chapter 4 section 4.3.

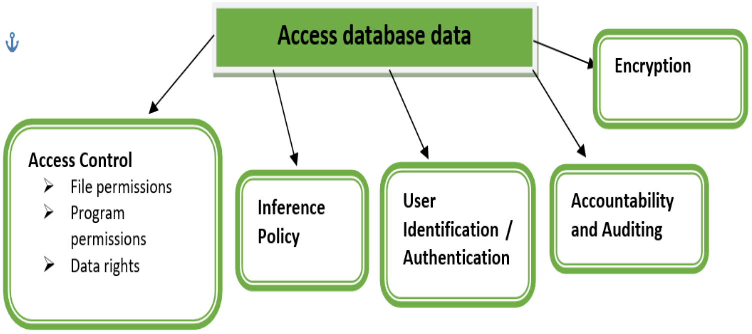


Figure 5-2: Accessing data in a Database

5.2. SUMMARY

This research focused on developing a secure COP DB data access module and it introduced different security measures and approaches to secure children while online. A database holds confidential, sensitive, or protected information, making it a prime target for cyberattacks (Global Asset Systems, 2021). If your intellectual property is stolen or leaked, you might struggle to maintain or recover your competitive advantage in your niche.

5.3. RECOMMENDATION

Base on the research carried out, findings, observation and reports and literature review done as presented in chapter 4, this concluded that Child Online Protection is very important and all stakeholders involved are recommended to contribute on gathering all information about COP and capture this in a secure database. As this will be used as the key or way to act on how to secure children while online. Parents need to be educated on how to communicate with their children, take note of anything suspicious their children discover while online and take up this to the COP organization and stored in the DB to be used in the future. The data must be kept on the DB safe to avoid any interruption or edition on this, because if an online cyberbully sees that information they can destroy them and there will be no data to be used for finding solutions and what to be careful with for children online safety.

All organization involved in child-care, need to invest in research about Child Online Protection and suggest on different online safety for children either at home or school. Furthermore, is recommended that the institution offers the students with sponsorship letters, because there are some researches which require some materials and money to complete the work.

5.4. FUTURE WORK

For future works this research is to invite different organizations which are part of and not part of the COP for them to engage in organizing campaigns and meetings where both parents and children are invited to say their experience on children online safety, what they see as the main issues and provide solutions. In the current world were COVID-19 is changing a lot of things including the mode of education for children, it will be an advantage to this study for children to be taking note of anything suspicious online as this data will be shared to other children but only if the data is kept safe in a secure database. The secure access module can be presented to different organization with databases to give suggestion, there might be more techniques missed or new ones, because technology keeps on upgrading and changing everyday with new features.

5.5. CONCLUSION

This research focused on the development of a secure access module to secure a Child Online Protection Database, securing database in general and the importance of securing a database. The literature review of different current and past research contributed on achieving each sub-objective, the main objective and answering the research questions. Parents need education on what to do with information they get about their children online safety. information that has been translated into a form that is efficient for movement or processing. Child Online Protection is something that requires different participants, lessons for online safety starts with parents by addressing the different online safety tips and guidelines presented in chapter 4.

REFERENCES

Berger, D., Fröhlich, P. (2016). Software testing techniques. Power Point Lecture, 20 pages (2016)
https://whatworks.org.nz/observation/
https://doi.org/10.1007/978-1-4020-8265-8_200285

Bryman, A. &. (2007). Business Research methods. Oxford University Press.
Child Online Protection, an ITU initiative (2020). Guidelines on Child Online Protection Children's Health Queensland (2022). Children's Health Queensland Hospital and Health Service.

https://www.childrens.health.qld.gov.au/blog-10-things-keep-kids-safe-online/

Bhunu Shava, F., Chitauro, M., Mikka-Muntuumo, J., Nhamu, I., &, & Gamundani, A. (2016). Exploratory research study on knowledge, attitudes and practices of ICT use and online safety risks by children in Namibia. Windhoek: UNICEF Namibia.
Course Hero. (2015). Top 10 Database Security Threats.pdf - Top Ten..
https://www.coursehero.com/file/27317213/2015-Top-10-Database-Security-Threatspdf/
Cvrcek, D. (n.d.). www.fit.vutbr.cz. Access Control in Database Management System.
http://www.fit.vutbr.cz/~cvrcek/confers98/datasem/datasem.html.cz
DeFranzo, S. E. (2011, September 16). qualitative-vs-quantitative-research. https://www.snapsurveys.com/blog/qualitative-vs-quantitative-research/ECDL. (n.d.). COMPUTER ESSENTIAL. ECDL NOTES.
Eduardo Fernández-Medina, M. P. (2015). Designing_secure_databases . Information and Software Technology.
Elana P. Ben-Joseph, MD. (April 2018). Internet Safety.
https://kidshealth.org/en/parents/net-safety.html
Formplus B. (2021). 7 Data Collection Methods & Tools for Research.

https://www.formpl.us/blog/data-collection-method#:~:text=Case%20Studies%2C%20Checklists%2C%20Interviews%2C,tools%20used%20to%20collect%20data.&text=You%20can%20easily%20get%20data,%2C%20Focus%20Groups%2C%20and%20Reporting.

Galetto, M. (2018, May 2). what-is-data-analysis.
www.ngdata.com: https://www.ngdata.com/what-is-data-analysis/
Global Asset Systems (01 September 2021). Why Good Database Security is Important in 2021. https://www.okta.com: https://www.okta.com/identity-101/authentication-vs-authorization/

IBM Cloud Education (27 August 2019). Database Security.

https://www.ibm.com/cloud/learn/database-security.Imperva (2021). Database Security.

https://www.imperva.com/learn/data-security/database-security/.

ITU (7-8 April 2012). ITU Global Cybersecurity Agenda and Child Online Protection (COP).

https://www.unodc.org/documents/southeastasiaandpacific/2012/05/cyber-crime/ITU_Cybersecurity_COP_UNODC_Workshop.pdf

Keeping children safe online.

https://www.itu-cop-guidelines.com/parentsandeducators

Mubina M. (2016). Database Security - Attacks and Control Methods

Michigan, T. R. (2018). Survey Research and Questionnaires. Child Care and Early Education RESEARCH CONNECTIONS.

Microsoft (2021). An overview of Azure SQL Database and SQL Managed Instance security capabilities.

https://docs.microsoft.com/en-us/azure/azure- sql/database/security-overview

Milton Keynes, B. R. (2016). Secure Database Development. Secure DBMS development, secure database design.

Molly Galetto. (January 20, 2016). What Is Data Analysis?
https://www.ngdata.com/what-is-data-analysis/

Nigerian Communications Commission. KEEPING CHILDREN SAFE ONLINE: Advice to parents and caregivers

Northeastern University. (2014). Software Development Life Cycle (SDLC). Software Development Life Cycle (SDLC), 1(1), 9–12.
http://www.tutorialspoint.com/sdlc/sdlc_tutorial.pdf

OECD (2021). Children in the digital environment.

https://www.oecd.org/sti/ieconomy/protecting-children-online.htm#:~:text=The%20OECD%20Recommendation%20on%20Children,that%20the%20digital%20world%20provides

OECD. (2012). THE PROTECTION OF CHILDREN ONLINE : RECOMMENDATION OF THE OECD COUNCIL: REPORT ON RISKS FACED BY CHILDREN ONLINE and POLICIES TO PROTECT THEM . THE PROTECTION OF CHILDREN ONLINE .

Okta. (2022). Authentication vs. Authorization.

https://www.gasystems.com.au/blog/database-security/

Olaniran, B. A. (2013). ICTs and Management Systems for Improving Efficiency in Healthcare and Social Care. (Texas Tech University, USA) and Natasha Rodriguez (Communication Professional, USA).

ORACLE (2016). About Oracle Database Security.
https://docs.oracle.com/database/121/DBSEG/intro.htm#DBSEG99774

QuestionPro (2022). Survey Software.
https://www.questionpro.com/blog/descriptive-research/

RESPONSIBILITIES OF RESEARCHERS. (2013).

https://www.ncl.ac.uk/hr/assets/documents/research-responsibilities-researcher-postcard_hc.pdf

Rouse, M. (n.d.). What is database (DB)? - Definition from WhatIs.com - SearchSQLServer. https://searchsqlserver.techtarget.com/definition/database

Reza, H., Zarns, K. (2011).: Testing relational database using SQLLint. In: Proceedings - 2011 8th International Conference on Information Technology: New Generations, ITNG 2011,pp.2011, pp. 608–613 (2010)4.

Sahoo, R. K. (2013). A Novel Watermarking Scheme for Secure Relational Databases. Information Security Journal: A Global Perspective.

Sanjay Sareen, S. K. (2016). Towards the design of a secure data outsourcing using fragmentation and secret sharing scheme. Information Security Journal: A Global Perspective.

Saunders, M. L. (2012). Research methods for business students, 6th Edition. Pearson Education Limited.

Schach, S. R. (2007). Object-oriented and classical software engineering (7th ed.). New York: McGraw-Hill.

Sherrell L. (2013) Waterfall Model. In: Runehov A.L.C., Oviedo L. (eds) Encyclopedia of Sciences and Religions. Springer, Dordrecht.

Shona McCombes . (May 15, 2019). Revised on September 3, 2020. Descriptive Research Design | Definition, Methods and Example. https://www.scribbr.com/methodology/descriptive-research/

Sorkin, D. E. (2011). Why Data Security is of Paramount Importance. The Importance Of Data Security.

www.spamlaws.com: https://www.spamlaws.com/data-security-importance.html

Sree, U. (2016).: Software Testing Life Cycle: Defects and Bugs (2016). https://olaiainforarch.wordpress.com/. Accessed 11 July 20165.

Stefan Rommer, Catherine Mulligan (2020). Network Access Security.

https://www.sciencedirect.com/topics/computer-science/network-access-security

Sudeshna. (2016, September 7). Limitations and weakness of quantitative research methods. https://www.projectguru.in/publications/limitations-quantitative-research/

Thuraisingam, B. (2005). Database and Application Security (Integrating Information Security and Data Management). Broken Sound Parkway NW: Auerbach Publications.

UNICEF. (2012). Child Safety Online: Global Challenges and strategies. United Nations Children’s Fund (UNICEF).

Vonnegut, S. (2016). The Importance of Database Security and Integrity. Database and information security.

WESTERN Illinois University. (2019). Research Paper Writing: 6. Results / Analysis. https://wiu.libguides.com/researchpaperwriting.

Yi, W. (2005). Database Security – Threats and Countermeasures. http://www.ils.unc.edu/~wenyang/inls258/wenyang.htm.

Vantsevich, V., Howell, S., Vysotski, M. and Kharytonchyk, S., 2003. An integrated approach to autonomous vehicle systems: theory and implementation. International Journal of Vehicle Autonomous Systems, 1(3/4), p.271.

Chan, C., 2017. Advancements, prospects, and impacts of automated driving systems. International Journal of Transportation Science and Technology, 6(3), pp.208-216.

Yazdizadeh, A., Patterson, Z. and Farooq, B., 2019. An automated approach from GPS traces to complete trip information. International Journal of Transportation Science and Technology, 8(1), pp.82-100.

Komzalov, A. and Shilov, N., 2017. Application of modern technologies in car driver assistance systems, pp.1077-1082.

Cheah, M. and Shaikh, S., 2015. Autonomous Vehicle Security. Engineering & Technology Reference,.

Gruel, W. and Stanford, J., 2016. Assessing the Long-term Effects of Autonomous Vehicles: A Speculative Approach. Transportation Research Procedia, 13, pp.18-29.

Katrakazas, C., Quddus, M., Chen, W. and Deka, L., 2015. Real-time motion planning methods for autonomous on-road driving: State-of-the-art and future research directions. Transportation Research Part C: Emerging Technologies, 60, pp.416-442.

Cesari, G., Schildbach, G., Carvalho, A. and Borrelli, F., 2017. Scenario Model Predictive Control for Lane Change Assistance and Autonomous Driving on Highways. IEEE Intelligent Transportation Systems Magazine, 9(3), pp.23-35.