ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/371847809

A Web Based Employees' Cyber Security Ethical Behavior Assessment (ECEBA) Model for Ugandan Commercial Banks

Article *in* American Journal of Computing and Engineering · June 2023

DOI: 10.47672/ajce.1513

CITATIONS
0

READS
51

3 authors, including:



Geoffrey Mayoka Kituyi
Makerere University Business School
64 PUBLICATIONS **472** CITATIONS

SEE PROFILE



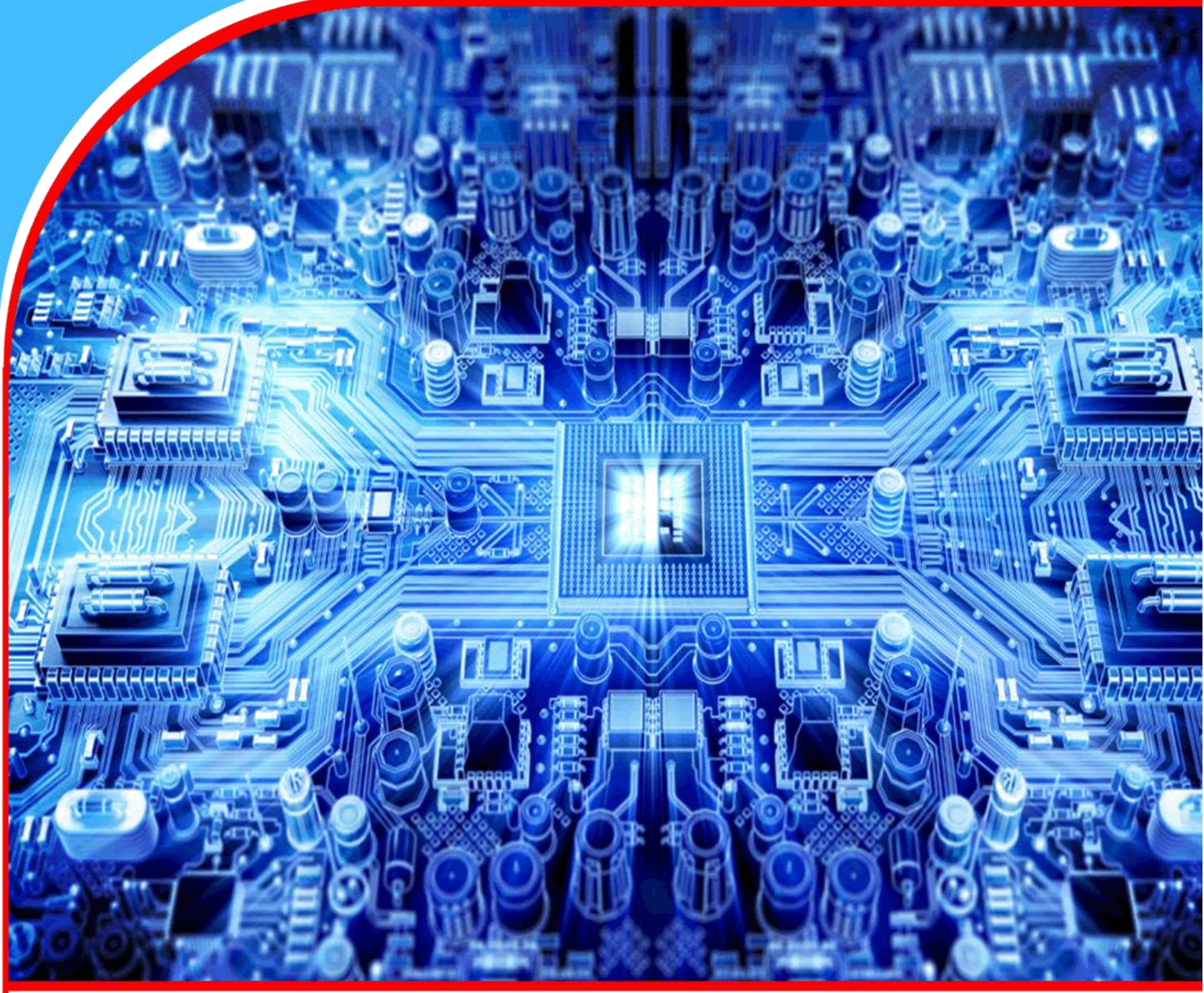
Fred Kaggwa
Mbarara University of Science & Technology (MUST)
21 PUBLICATIONS **28** CITATIONS

SEE PROFILE

All content following this page was uploaded by Geoffrey Mayoka Kituyi on 03 July 2023.

The user has requested enhancement of the downloaded file.

American Journal of
Computing and Engineering
(AJCE)



A Web Based Employees' Cyber Security Ethical Behavior Assessment (ECEBA) Model for Ugandan Commercial Banks

Nakato Ruth, Mayoka G. Kituyi & Fred Kaggwa

AJP

American Journal of Computing and Engineering
ISSN 2790-5586 (Online)
Vol.6, Issue 1, pp 46 –72, 2023

www.ajpojournals.org

A Web Based Employees' Cyber Security Ethical Behavior Assessment (ECEBA) Model for Ugandan Commercial Banks

Nakato Ruth[1*], Mayoka G. Kituyi[2] & Fred Kaggwa[3]
[1]Mbarara University of Science and Technology
*Corresponding Author's Email: rnakato@must.ac.ug
[2]Makerere University Business School
Co-Author's Email: gkituyi@mubs.ac.ug
[3]Mbarara University of science and Technology
Co-Author's Email: Kaggwa_fred@must.ac.ug

Article history

Submitted 20.03.2023 Revised Version Received 23.06.2023 Accepted 24.06.2023

Abstract

Purpose: Despite the existence of Cyber Security technical controls, checklists, and formal procedures in the banks; there exists no employees' assessment tool for Cyber Security ethical behavior. This research presents the creation of such a tool. This research aimed at enhancing Cyber Security by developing a Cyber-Security Ethical Behavior Assessment (ECEBA) model.

Methodology: ECEBA model was used as an experimentation instrument for the development of a web-based application (ETHICA) for assessing Cyber Security ethical behavior. Unified Modelling Language (UML) was used. The ECEBA model followed the reuse concept by customizing the 3-tier architecture of the web application development. The front end interface was done using HTML5 to design the web interfaces of the ETHICA Application. To style the interfaces, CSS3 was used. Then JavaScript was used as a client side script to validate the data before submitting it to the server. AJAX a JavaScript library was used to allow submission and loading of data. Bootstrap was used to achieve responsiveness of the user interfaces. XAMPP a local MySQL server was used to host the database and the system files. Object Oriented PHP was used to act as a GUI to manage data communication between the server and interfaces. PHP Data Object driver class was used to achieve this. SQL was used to write the queries purposely to perform data processing on the server.

Findings: The ECEBA model was developed. Deployed to the internet via URL http://Cybersecurity.groxels.com. It guided the design of ETHICA Application.

Recommendation: Ethical behavior questions based on virtue ethical theory, Theory of Planned Behavior (TPB) and Ethical climate theory are fed into the ETHICA Application. This provides a platform for managers in assessing those individuals who may present Cyber security unethical behavior. Banks should give employees opportunity to assess themselves. Banks to use the model in conducting Employee pre-hire screening and periodic assessments of current employees. Banks should integrate the model with other cyber security controls for better ethical decision making & planning.

Keywords: *Cyber Security, Ethical Behavior, Web Based*

1.0 INTRODUCTION

Improving computerized and online information security is one of Uganda's Vision 2040 goals for information communication technologies, as per the country' Third national development plan (NDPIII) 2020/21 - 2024/25. Goal 9: ICTs can be found explicitly as a target under SDG 9 "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation" Global efforts need to be stepped up to address an increase in cross-border cyberattacks, hate speech and security breaches.

However, Kuepper, (2019) contends that Cyber security incidents in the banking industry have increased, which has an impact on the performance of the banks. Banks have established codes of conduct and put in place a number of strong Cyber Security measures as a deterrent to unwanted behavior, (Zahoor et al., 2016). Yet, employees who act unethically ignore and bypass all of these protections (Gray, 2015). This increases Cyber insecurity in the banks which results into sensitive information falling into the hands of cybercriminals.

A Cyber security breach hurts the afflicted bank's reputation and finances, which causes bank clients to lose faith in the institution. Dupont, (2019) echoes that a bank suffers an average weekly loss of $1.8 million from a cyberattack particularly directed at their online banking services. For instance, after an increase in electronic fraud of 6.3% in 2016, the overall number of customers at Centenary Bank Uganda decreased by 11.4%, and client deposits decreased by 7%, (Matovu, 2018).

The banking sector is a crucial component of a strong economy because it plays a key role in financial mobilization, facilitates a reliable payment system, and helps implement monetary policy. Malik et al., (2018), warn that if bank workers' breaches of Cyber security are not addressed, both the micro and macro levels of the economy may suffer. This could make it harder for Uganda to realize Vision 2040. Breach of Cyber security may potentially deter international investors. They control a significant portion of the financial sector, and if their money is taken through cybercrime, the entire economy of Uganda could suffer. Standard of living, availability of jobs, National development, increased savings, and welfare may all be impacted.

Cybersecurity in Developed Countries Compared to Developing Countries

Khan et al., (2022), contend that Cybersecurity occupies a significant position in the aftermath of globalization and the intricate integration of Information Systems with Information and Communication Technologies (ICTs). The influence of ICTs on improving the quality of services in today's networked global village is unsurpassed (Murithi & Yoo); (Otieno, 2020). Developed countries are already taking strides towards sustaining multifaceted Cyber security approaches. Cyber threats however, to developing countries could impede their economic growth and destabilize the global financial system. Mars, (2021) opines that while rich nations are moving forward with diverse Cybersecurity strategies, developing nations are negotiating their own muddle of internal problems while advocating for regulations for digital infrastructures and have even failed to understand the digital transition that is taking place. Developing countries are at the forefront of the digital transition and are still having trouble understanding it. Poorer countries have insufficient institutional capacity, limited ICT skills, knowledge, and limited protection of crucial national infrastructures. They also have weak interagency coordination and emergency responses. Indeed, developing nations lag behind the developed world by a few decades.

Russu, (2022) contend that Developed nations have gathered strong Cyber security resources. Developing nations try to imitate developed countries because they are seen as major models of Cyber security tactics, policies, and technological innovation. Reluctant leaders of developing countries hurriedly pass legislation, launch extensive proposals, establish CERTs, and look for methods to raise money for national Cybersecurity infrastructures. They do so without looking at their own ICT road maps or first enhancing the very pillars of their technological state, including communications, internet services, law and order, business costs, resources, and investment security. For instance, the cybercrime in Bangladesh Heist, which cost a local bank $81 million (froman attempted $951 million), was sent to a bank in the Philippines. But lax anti-money laundering regulations and broken cybercrime laws made investigations unsuccessful. Africa's Cameroon is one of the countries where cybercrime is having the biggest impact. A few years ago, there were ideas about launching various Cyber security training programs to help address this issue. Policymakers were worried that after training, students might use their newly acquired skills to engage in cybercrime.

Nigeria has become the gold standard for phishing. Despite being simple, the phishing technique has already stolen billions from trusting people and stupid people all across the world. Nigerian fraud networks have been discovered in numerous countries, never the less the countries where they are captured determine whether they will be charged. Other socioeconomic issues are significantly impacted if the populace lacks confidence to protect them. A reliable and stable justice system, as well as competent law enforcement, are essential for sustainable growth.

While underdeveloped nations detest responsible vulnerability reports and pursue security researchers as criminals, developed nations see bug glut programs as a helpful tool in defending their national infrastructure and government systems. Although most developed countries have in place comprehensive ICTs and Cybersecurity policies and plans or are at an advanced stage of implementing them, developing countries are short of the capabilities and infrastructure when it comes to Cyber security countermeasures. Most hardware and software products used in the developing world are developed from the western world and without proper measures on how to secure these products, these countries are vulnerable to cyber exploitation due to inherent vulnerabilities on these products. Low-income states are targeted by both money-driven attacks (such as ransomware), and serve as training grounds for criminal groups in preparation for more ambitious attacks in developed countries (Owiny, 2023). Developing countries are aware of the need for Cyber security, but many would contend that they are more concerned with serious issues like HIV/AIDS or poverty. Developing countries lack well-trained cybersecurity experts. Level of understanding and education in cybersecurity issues among law enforcements agents, judiciary are not up to the standard.

Banks have established codes of conduct and put in place a number of strong Cybersecurity measures as a deterrent to unwanted behavior, (Zahoor et al., 2016). However, employees who act unethically ignore and bypass all of these protections (Gray, 2015) leading to the increase in Cyber insecurity in the banks which results into sensitive information falling into the hands of cybercriminals.

2.0 LITERATURE REVIEW

A vital component of life and the cornerstone of a cultured society is ethical behavior. Employees' ethical behavior is an important asset and source of competitive advantage in the workplace.

Unethical behavior has a negative bearing on an employee, the colleagues, and the entire business. (Andrews, 1989). In order to prevent employees 'unethical activities, banks urgently need to better comprehend the issue of Cyber Security ethical concerns (Gray, 2015; Carter & Crumpler 2019). Acting ethically means abiding by and reflecting one's personal morals and the generally accepted standards of the organization and society (Yatich & Musebe, 2017).

Running anti-virus software, installing software updates, turning on personal firewalls, avoiding adware/spyware, protecting passwords, using spam filtering techniques, are all important cyber-safety measures but they haven't been successful in addressing these human issues because their focus is placed on technological applicability. Uganda has three cyber space laws (the Eletronic transaction Act, Computer misuse Act, and the Electronic Signatures' Act), to govern fraud online, but they are difficult to implement and they are not known by the public (Lule & Buregyeya; 2023). Ethical conduct may contribute to increased Cyber Security but behavioral components of Cyber Security are still understudied, Ait Maalem et al., (2020), as a result, ethical considerations remain a challenge.

Egelman & Peer, (2015) created a scale called the Security Behavior Intentions Scale to evaluate end-users' computer security practices (SeBIS). The scale gauges' users' self-reported compliance with security recommendations for computers. The 16 items on the Security Behavior Intentions Scale (SeBIS) are specifically mapped to four factors: device security, password creation, Faklaris et al. (2019) assert that while SeBIS explains how much a user strives to follow these professional suggestions, it is unable to express people's attitudes toward security practices. Additionally, it avoided discussing the intentions behind security ethical action based on virtue ethical theories. A web-based Employees' Cyber Security Ethical Behavior assessment (ECEBA) Model for Ugandan Commercial Banks was created.

Theories Underpinning this Research

This study model is supported by the Philosophical Virtue Theory, the Theory of Planned Behavior (TPB), and the Ethical Climate Theory. An assessment model for employees' ethical behavior in relation to Cyber security was created using these theories as a foundation.

Philosophical Theories

Normative ethics examines whether a person's moral actions are right or wrong in relation to the moral laws of society (Gray and Tejay, 2014). In normative ethical theory, Cyber security ethics is a subset of applied ethics that addresses the real-world moral issues that arise from using computers and networks of computers in the information age on a daily basis. Deontological and consequentialist ethics have frequently been favored in contemporary studies as being appropriate for computer ethics, but were not considered for this research. Virtue ethical theory was instead preferred because during the past few decades, considerable efforts have been made to apply Aristotelian version of virtue ethics to computer and cyber ethics in modern research. According to MacIntrye, (1984), a virtue is a cultivated trait or personality that constitutes the fundamental components of admirable character. Virtues are advantageous for leading a contented, successful, or flourishing human existence; this good life may also entail defending particular values against opposing values. By having and using virtue, one develops self- awareness, a sense of goodness, and ultimately benefits both internally and externally (MacIntyre, 1984). The cardinal virtues of Courage, Temperance, Justice, and Prudence were included in this research model.

Employees and professionals in the field of Cyber security have ethical duties to other people, organizations, and the computing industry as a whole. Cardinal virtues should be incorporated into the information systems protection paradigm, Gray & Tejay, 2014). Theoretical work on virtue ethics in social work has grown in recent years, but little has been done to examine how the virtues are really put to use in the field of computing, and more specifically, in Cybersecurity. The current research created a web-based Cyber security ethical behavior assessment model to assist banks in analyzing the Cyber security ethical conduct of their personnel. The model also identifies employee's ethical blind spots and behavioral gaps, and this data is used to develop awareness and training programs for Cyber security ethics.

Theory of Planned Behavior (TPB)

The notion of how simple or difficult an activity would be to carry out is known as perceived behavioral control. The Theory of Planned Behavior (TPB) was proposed by Ajzen, (1991) to explain the influence of attitude, subjective norms, and perceived behavioral control upon individual behavior. The TPB has been used extensively in numerous research to forecast people's behavior. Ifinedo, (2014), contended that users' intentions to follow information security organization regulations are influenced by attitude, subjective norms, and perceived behavioral control. Intentional behavior drives behavior. The attitude toward the activity, subjective norms, and perceived behavioral control all play a role in determining behavioral intention. Tommasetti et al., (2018), opine that the TPB's primary objective is to aid researchers in making predictions about how people would act in various circumstances. TPB makes the underlying assumption that an individual's conduct is driven by a combination of intention and perceived behavioral control. Uffen and Breitner, (2013), content that earlier researchers have employed the theory of planned behavior (TPB) to explain user behavior in information systems studies.

Ethical Climate Theory

Ethical Climate is a deliberate understanding of appropriate behavior deriving from organizational architecture, which affects behavior and decision-making (Victor & Cullen, 1988). Research that includes Ethical Climate is theoretically significant because it presents insights into what ethical climate really exists and what organizations leaders essentially do to influence employees' behavioral towards Cyber security. This basically affects how firms make decisions and predict employee misconduct with regard to cyber security. Kuenzi et al. (2019), contend that a company's employees are able to uphold ethical behavior within the workplace if there is a strong ethical climate present. Employees are less likely to violate the organization's ethical standards in order to accomplish goals and objectives when the ethical climate within the workplace is robust. Hence, this study argues that EC may play a moderating role on the connection between virtue ethics and employees' ethical behavior.

3.0 METHODOLOGY

This study presents the creation of a Cyber Security ethical behavior assessment model and presents its applicability among the banking sector employees in Uganda. The model was used as an experimentation instrument for the development of a web-based application for assessing Cyber Security ethical behavior in Ugandan commercial banks. It was designed using the Unified Modelling Language (UML). UML is a standardized modeling language made up of an integrated set of diagrams for assisting software developers in specifying, visualizing, constructing, and documenting the artifacts of software systems, (Tumuhimbise et al., 2022). UML uses notations

to explicitly represent the variation points in the structure of the model thus allowing partial automation of the development and implementation. To avoid re-inventing the wheel, The ECEBA model followed the reuse concept by customizing the 3-tier architecture of the web application development. Three-tier architecture is a well-established software application architecture that organizes applications into three logical and physical computing tiers: the presentation tier, or user interface; the application tier, where data is processed; and the data tier, where the data associated with the application is stored. The web-based model focusing on specific modules tailored for assessing banks' employees' Cyber Security ethical behavior was designed and developed. The web-based customization was done by the researcher by aligning modules specific to this study.

Requirements for the ECEBA Model

The following are the model requirements.

i. Provision of data storage, access & retrieval about Cyber Security ethical situations and decisions.

ii. Map these elements to mitigate unethical behavior towards Cyber Security

iii. The ECEBA model should serve as a web-based tool that supports banks in assessing their current and potential employees' Cyber Security ethical behavior

iv. Provide a mechanism of transferring and sharing knowledge about Cyber Security ethical behavior within the bank.

The ECEBA Model Architecture

The Application Layer Module

This module offers a platform that enables Ethica web-based application to perform with ease on the web platform. This layer, also called Business Logic or Domain Logic or Application Layer, accepts user requests from the browser, processes them, and determines the routes through which the data will be accessed. The workflows by which the data and requests travel through the back end are encoded in a business layer. Using the web browser, the module enables users to view, interact with, and access web content. It sends an HTTP request to the web server and displays the results for the user. The module offers an interface where employees enter their details and access the assessment Details. It also enables the application manager to edit the assessments. This module offers a backbone for the connection of all other modules of the ECEBA model.

Network Connection Module

This module is responsible for ensuring the connectivity of the developed application to ensure that it functions. The Ethica web-based application is an internet-based application which requires the internet to function, thus the network module ensures that the application connects to the internet to run efficiently.

Storage Module

This module offers storage and access to the patients' data. The module enhances the connection of the app and is responsible for ensuring that data is accessed and retrieved. Data is stored on the

Web Server

This is a back-end component that receives requests from the client side and processes them using business logic. It retrieves data from the database and transfers it to the web browser for display.

The module is responsible for the local and cloud database management and a central repository for ensuring that all data regarding employee's assessments are stored.

ECEBA Analytics Back-End

Question engine, Scoring Engine, and Data analytic module are in the application back end. **Question engine:** Questions are generated from normal text data input into an html form in the application. When employees are logged in, they can only view their respective profiles and attempt the assessments available. There are three sections of assessments; **Section 1;** Background Information that includes Demographic data and professional characteristics of employees. Section Two: Cardinal Virtue Constructs that assesses list of items related to Cyber Security i. Virtue of courage, which is defined as; Personal honesty and determination to make ethically correct or unpopular decisions regarding Cyber Security that affect decisions concerning adherence ii. List of items associated to the virtue of **temperance** that is explained as; individual modesty, self-control, and the ability to regulate sentiments and actions that affect decisions regarding Cybersecurity. iii. Items connected to **justice** which is defined as; Being sensitive to the rights of others and acting fairly and responsibly towards individuals, organizations, and communities. Behavioral intentions towards Cyber Security; (defined as the desire and likelihood of the individual to perform Cyber Security ethical behavior), Ethical Behavior towards Cybersecurity and Ethical Climate Questionnaire.

Scoring Engine does the marking and computing of scores. When an employee logs into the App. She/he can continue to answer the questions by selecting and responding to the answer options and ticking the most appropriate option. The system analyses the answer provided by the user and marks them depending on whether they tally with preset options stored in the database. Scores are calculated by a script in the 'Assessments Controller'. This script computes all total questions attempted, and answered in a Likert scale, correctly answered questions, missed questions, time taken to complete assessment.

Marking and Tot Up

Depending on the department of the specific employee, questions are pulled from the database and supplied to his User Interface (UI). The employee is given the opportunity to respond to each question by choosing what he believes to be the appropriate response. Depending on whether the user's response is correct or incorrect after analysis by the system they add up to a specified, database-stored accurate response. A script in the "Assessments Checker" determines the user's scores. Script calculates the total number of questions attempted, the proportion of questions that were answered correctly, incorrectly, and in the allotted time for the assessment.

Reporting

For reporting and analytical visualizations, the generated data is then attached to JavaScript charts and graphs. These are then read by the different policy makers for further recommendations including Cyber Security ethical trainings.

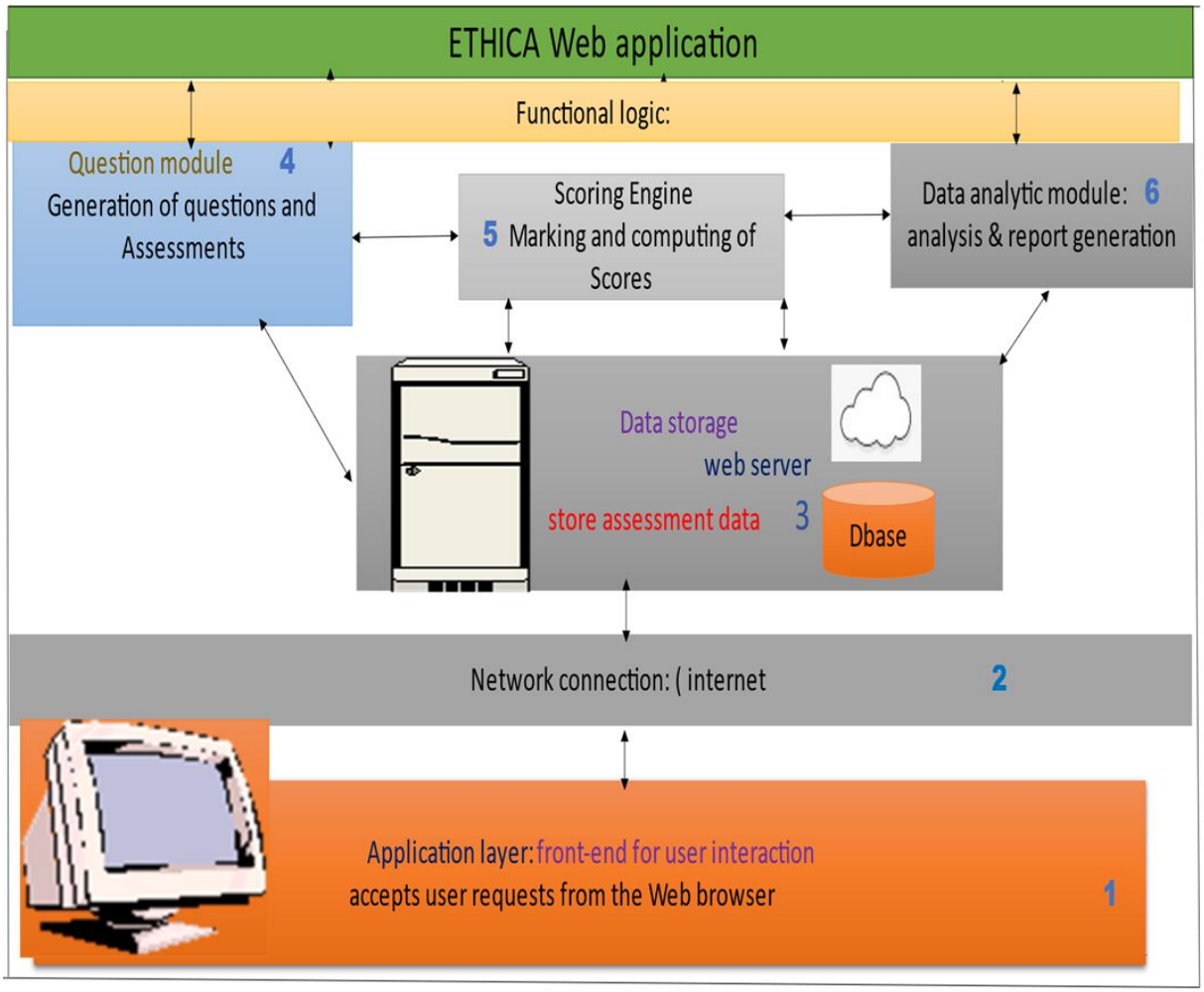


Figure 1: The ECEBA Model Architecture

ECEBA Model Design Tools

ECEBA Use Case

The Use Case diagram illustrates the major interactions that take place between the various subsystems and actors in the developed ECEBA model. ECEBA model is built on a 3 tier web architecture to provide an ethical behavior assessment ground that brings together technical employees in the bank to effectively manage Cyber Security ethical behavior in Ugandan commercial banks. Existing and potential new employees are continuously assessed to identify any misconduct in decision making especially when they are presented with Cyber Security ethical dilemmas.

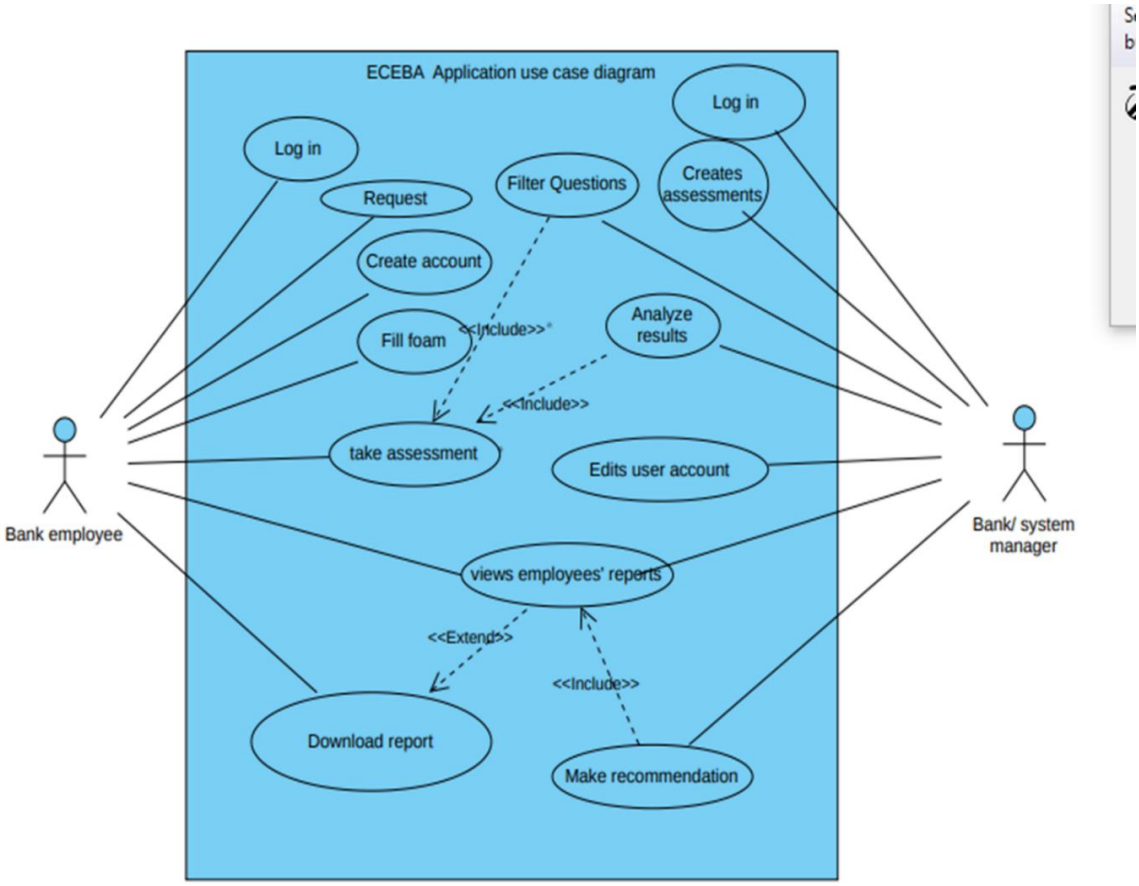


Figure 2: The ECEBA Use Case Diagram

Sequence Diagram

This diagram shows the interactions and communications between the Model actors. It helps in logical understandings of the model development. The purpose of a sequence diagram is to illustrate the sequential flow of information passing through the key entities of the system. The ECEBA sequence diagram illustrates how a user is authenticated into the system to allow access to the assessment.

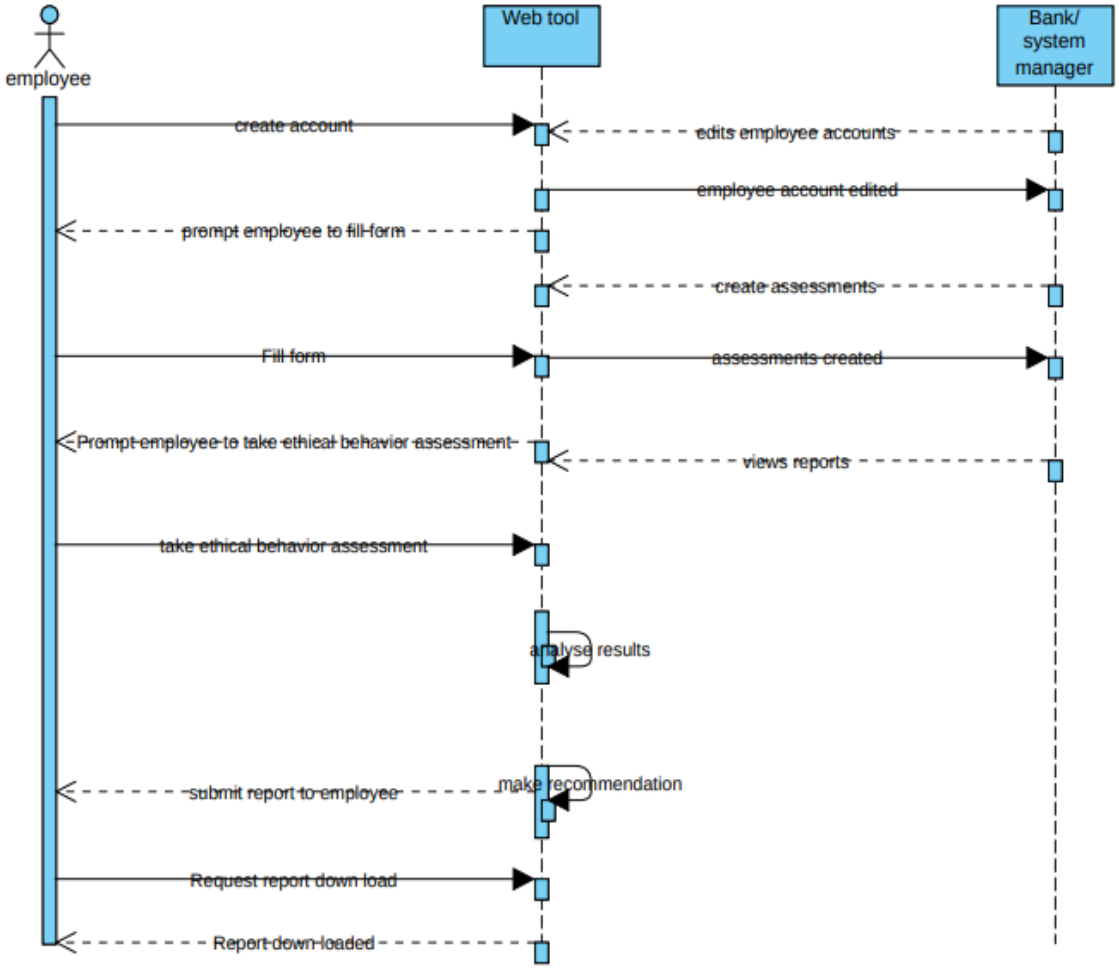


Figure 3: The ECEBA Sequence Diagram

American Journal of Computing and Engineering
ISSN 2790-5586 (Online)
Vol.6, Issue 1, pp 46 –72, 2023
www.ajpojournals.org

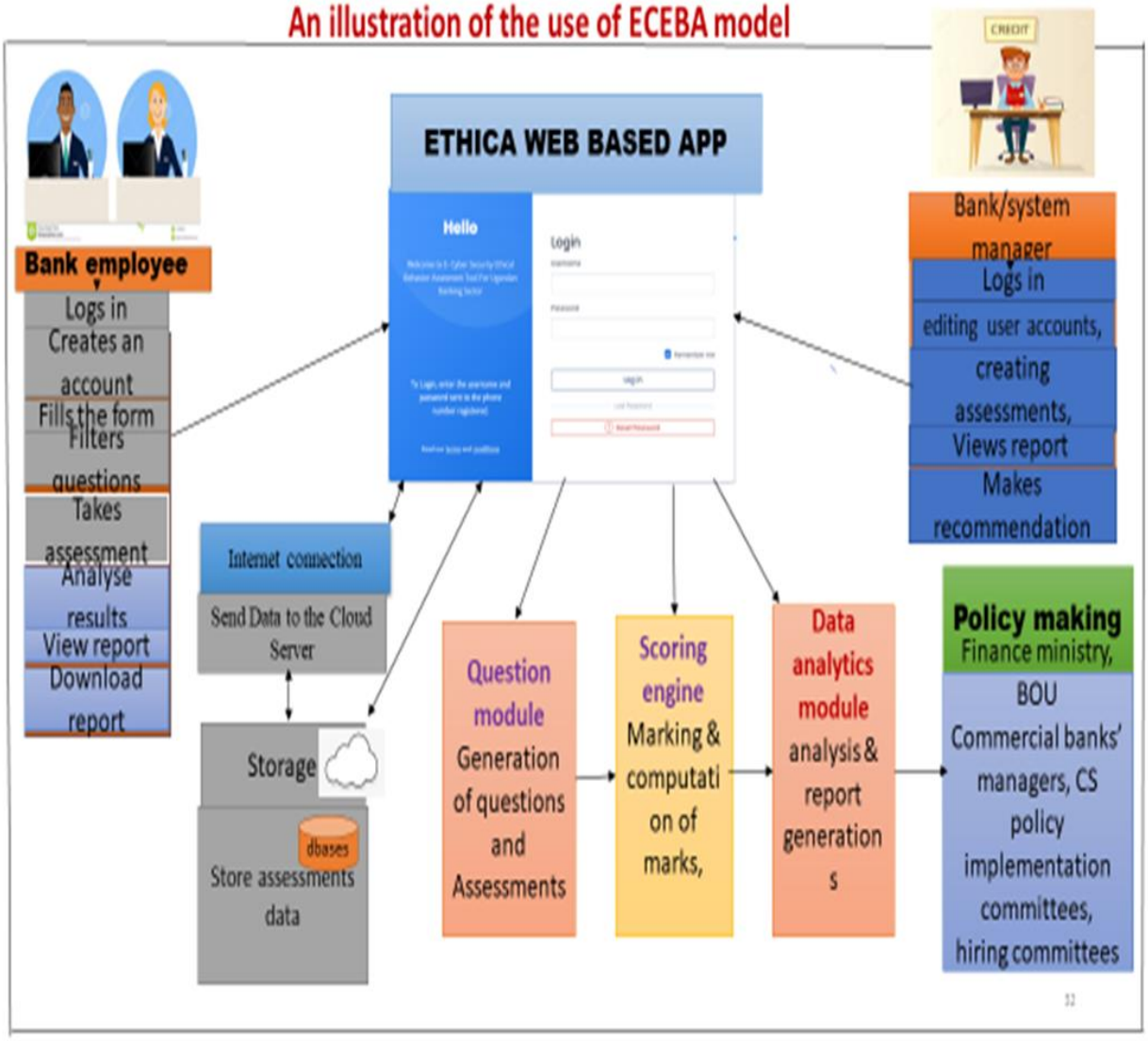


Figure 4: An Illustration of the Use of the ECEBA Model

The ETHICA web based Application Development to Test ECEBA Model

ETHICA app was developed to illustrate the potential of the ECEBA model, to prove its reliability (internal consistency and stability), validity (construct and concurrency), and accuracy in improving Cyber Security ethical behavior. The key features of the ECEBA model have been employed in the implementation of the ETHICA web based App. The word ETHICA was derived from ethical implying employees should possess good morals. The app was implemented among commercial banks employees and Absa bank Mbarara consented to test our App. The app enables bank employees to log in at their convenient time and take assessment and the banks can also carry out their employees' ethical behavior assessment.

The ECEBA Model Actors

a. The ETHICA App has an administrator, who is responsible for configuring and managing the developed Web based Application. He/she is answerable for administration, management, and support activities associated with the system.
b. The APP administrator further drafts and issues system terms and conditions, views registered users in the system, notices registered banks in the system,
c. Observes and updates the assessment questions.
d. Information managed and administered by the App administrator include assessment model sections, subsections, questions, assessment results, and bank staff information. They register their respective bank employees in the system, create and manage their accounts. an App administrator is privileged to register bank departments in the system which are used to group users under their designated departments. This helps in data visualization where it's easy to know how many staff belong to a certain department. He describes the role of the App to users. She/he is also responsible for creating and adding questions to the assessment model. These questions are placed under subsections of the ETHICA App. Creating a question involves selecting its level of evaluation. Manages the visibility status of the assessment model after adding questions. After staff performing assessment on the model, it cannot be accessed or edited.
e. The administrator views assessment results Note: the system calculates the assessment results basing on the staff response and given a recommendation based on the staff score. Then the administrator after accessing the results can provide their responses basing on the degree of assessment on a given question.
f. Generate reports; the administrator is also able to generate reports from the system. These include staff who have passed or failed the assessment, those who have partially or fully completed the assessment. They are also entitled to viewing statistics generated from the system.

A bank staff registered in the system is able to perform assessment simply by selecting any open model and answer the questions. An employee can view the certificate after assessment. Once the staff has completed assessment under a given model, the system automatically generates a certificate for the user showing assessment completion.

The ETHICA Web Based System's Requirements

Software Requirements

Table 1: Software Requirements of the Developed ETHICA Application

Requirement	Description	Usage
A source code editor	A text editor program designed specifically for editing source code of computer programs by system developers.	In this case Sublime text editor 3 was used to write codes during the process of system development.
Data Store	A repository for persistently storing and managing collections of data.	MySQL database management system was used to store and manage the system data.
Database Server	A software application typically for hosting application databases.	XAMP a local MySQL server was used to locally host the database that stores the system database and host the system files so that it was able to be accessed in a client server environment using a web browser.
Database Modelling Model	A software application for creating and manipulating database models and physical databases.	MYSQL Workbench was used to design the logical database model so as to graphically represent the different database entities and their relationship and also show how data flows in the system.
Operating System	A system software that manages computer hardware and hardware resources and support basic computer functions	Only Windows 10 was used to provide a platform for installing other software in order to design and develop the system.

Software Specifications

XAMPP version 7.2.32 was used to act as the local database server to locally host the MYSQL database where the system data is stored. The server also hosted the web application files which were accessed in a client server environment using a web browser (Google Chrome). MYSQL Workbench 8.0 CE was used to design the database model purposely to illustrate the flow of data between entities. This helped in designing the logical database model which was later converted into a physical database after forward engineering. Sublime Text Editor Version 3 32bit was also used as the source code editor for editing the developed web system source code.

Non-Functional Requirements for ETHICA Application

Non-Functional requirements explain the operation state and attributes of ETHICA Application. They include: (i) Security, this is enforced in the way that only authorized users with correct login credentials are allowed to access the system. ii) Access control only authorized users' access what they are supposed to access. For example, a bank staff cannot perform what is privately delegated

to administrators. (iii) Lean-ability, the developed web system provides clear and user friendly interfaces which can be easily remembered by the users. For instance, when a user is attempting the questionnaire, only one question displays at a time to keep user focused. (iv) Usability, the developed system provides properly labelled modules which are easy for a user.

ETHICA Architectural Design

The ETHICA Web based App provides a platform for assessing the staff Cybersecurity ethical behavior in commercial banks in Uganda. In developing the system, a number of programming languages and platforms were used. The front end interface was done using HTML5 to design the web interfaces of the system. To style the interfaces, CSS3 was used since it provides styling attributes for the HTML5 Components like headings, Paragraphs, Forms and Others. Then JavaScript was used as a client side script to validate the data before submitting it to the server. To achieve submission of data asynchronously, AJAX a JavaScript library was used to allow submission and loading of data without loading the 7 entire pages. This was done to limit the amount of data bundles required by the users while using the system. In order to achieve responsiveness of the user interfaces Bootstrap was used. Bootstrap is a free and open-source CSS framework directed at responsive, MobileFirst front-end web development. It contains CSS- and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components. When it comes to processing system data to and from the database, XAMPP a local MySQL server was used to host the database and also the system files and Object Oriented PHP was used to act as a GUI to manage data communication between the server and interfaces (connecting front end to back end). PDO (PHP Data Object) driver class was used to achieve this simply because PDO involves use of prepared statements which makes execution faster than running direct queries. In order to interact with the MySQL server using PHP, SQL was used to write the queries purposely to perform data processing on the server.

ETHICA Application Flow Chart

The system flow chart below shows how the different system users access the system and what they are entitled to execute in the system.

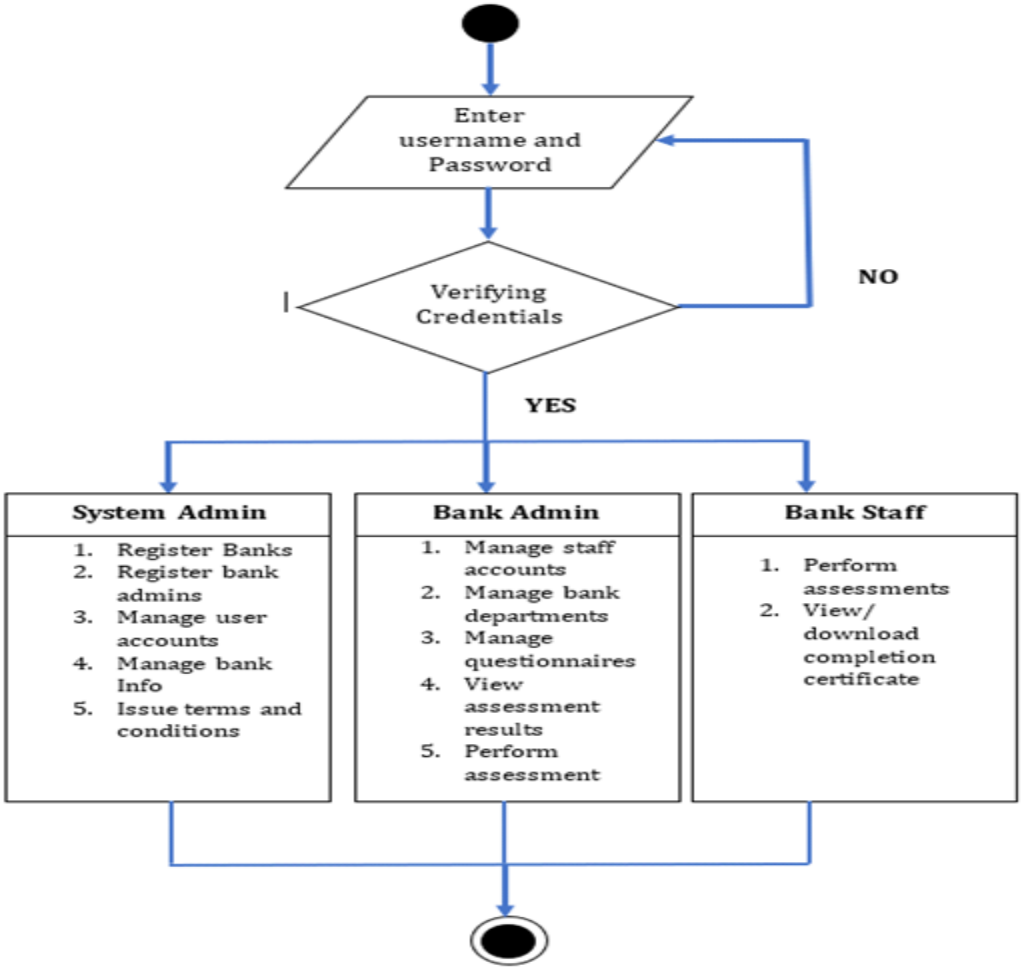


Figure 5: Showing the Flow of the System, System Users and Their Designated Tasks

Database Design

Entity Relationship Diagram (EERD)

Enhanced entity-relationship diagrams, or EERDs, are specialized Entity Relationship Diagrams that can be extremely useful for modeling the databases. EERDs use several concepts that are closely related to object-oriented design and programming. The EERD below shows the logical database design of the ETHICA application. It portrays different entities/ tables and the relationships among them. It shows how data flows in the system database. The database uses a number of entities to collect, save and retrieve data. These entities are represented in Figure 7.1. An Entity Relationship Diagram is a type of flowchart that shows how "entities" such as people, objects or concepts communicate with each other within a system. In this system, a basic user can only take the assessment appropriate for his department. A user can attempt only one assessment at a time. A basic user can edit his own profile, change his password, view his own assessment report, and print his own certificate of completion. The system administrator can create user accounts, create new categories of assessment, and populate an assessment with questions, view individual users' reports, and view aggregate reports.

American Journal of Computing and Engineering
ISSN 2790-5586 (Online)
Vol.6, Issue 1, pp 46 –72, 2023
www.ajpojournals.org

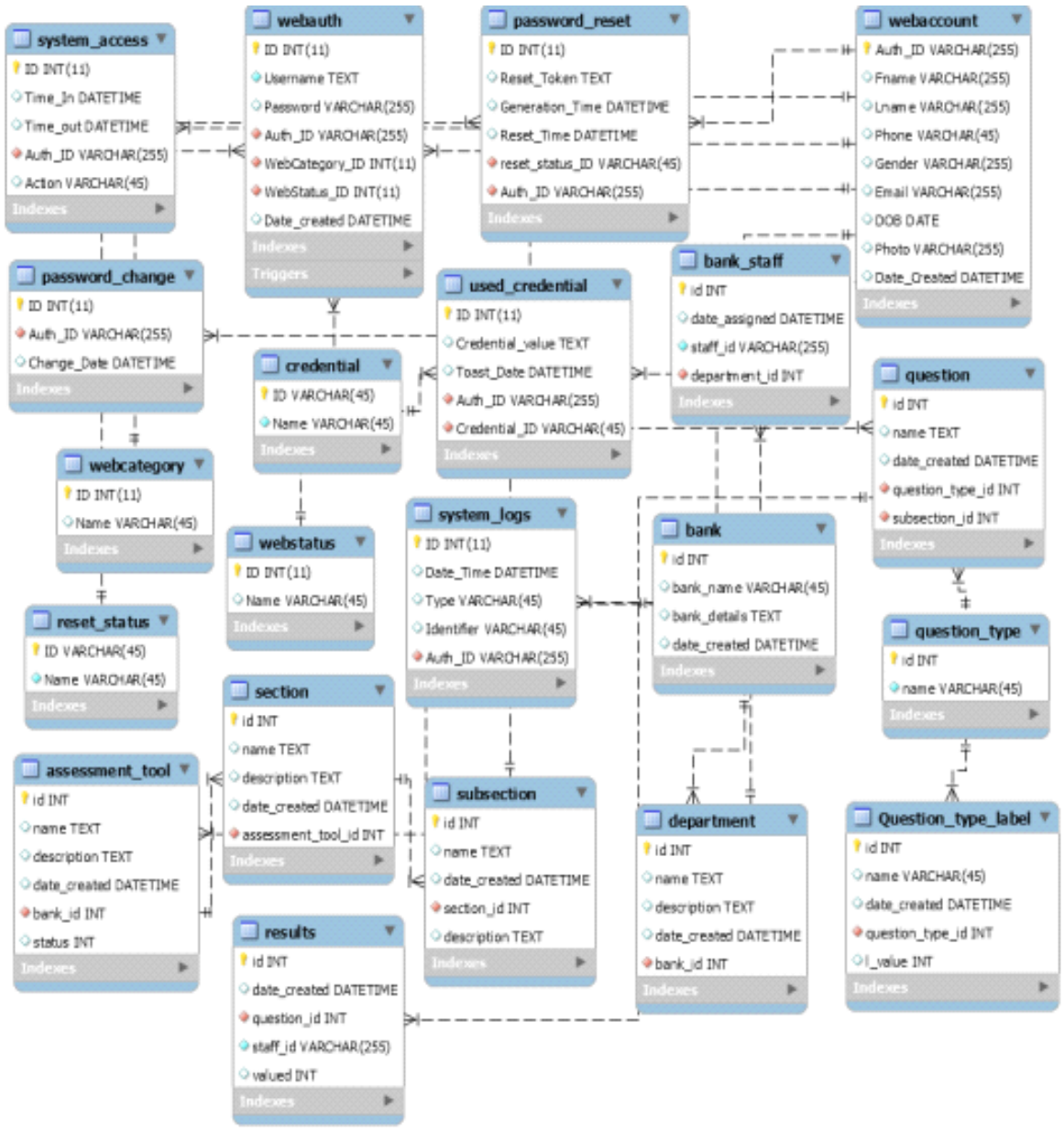


Figure 6: An Enhanced Entity-Relationship Diagram Showing Database Entities and Their Relationships

Graphical User Interface

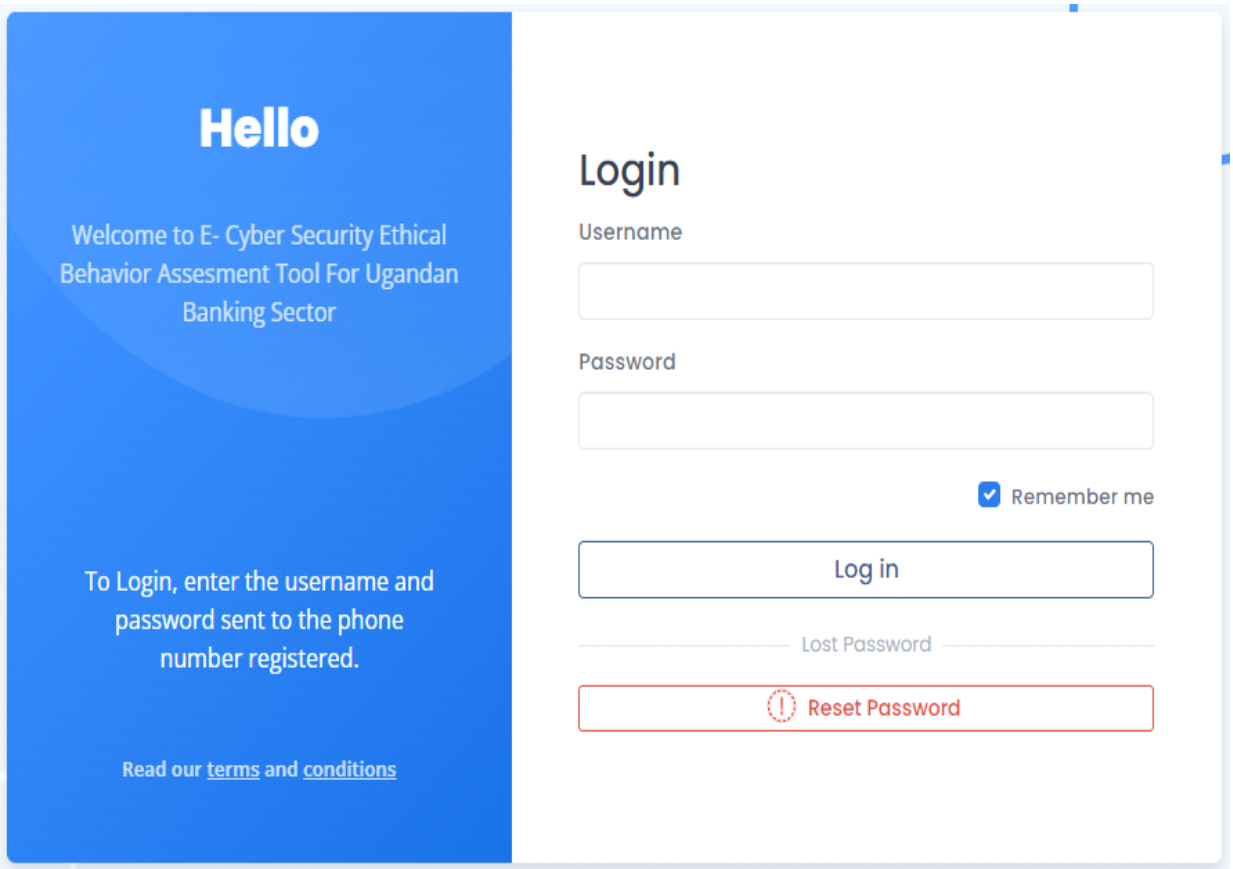


Figure 7: ETHICA Login Interface

The figure above portrays the login interface used to authenticate users at different levels into the ETHICA APP. On login, a user is required to provide a pair of matching credentials i.e., user name and password which are used to prove the user's identity. Once the user has provided the correct and valid credentials, authorization to the system is granted and a new session is started holding the ID of the user which is used to determine the level at which the user has accessed the system in order to prepare the right modules corresponding to the level of access. The system uses the same session ID to determine the bank where the user is registered so that all actions executed are tracked and stored under that bank.

When the users forget their password, the login interface provides a reset password button where user can click and get directed to the reset password interface. On this interface, a user is requested to enter their phone number or email address registered during account creation. If the phone number or email address exists, a six-digit OTP (One Time Passcode) is sent to the phone number or email address provided and thereafter a user is given an input field to confirm the sent code. The OTP is given a lifetime of 60 minutes valid. True confirmation of the OTP directs a user to where they can enter a new password and also confirm.

New Staff/Employee Registration Form

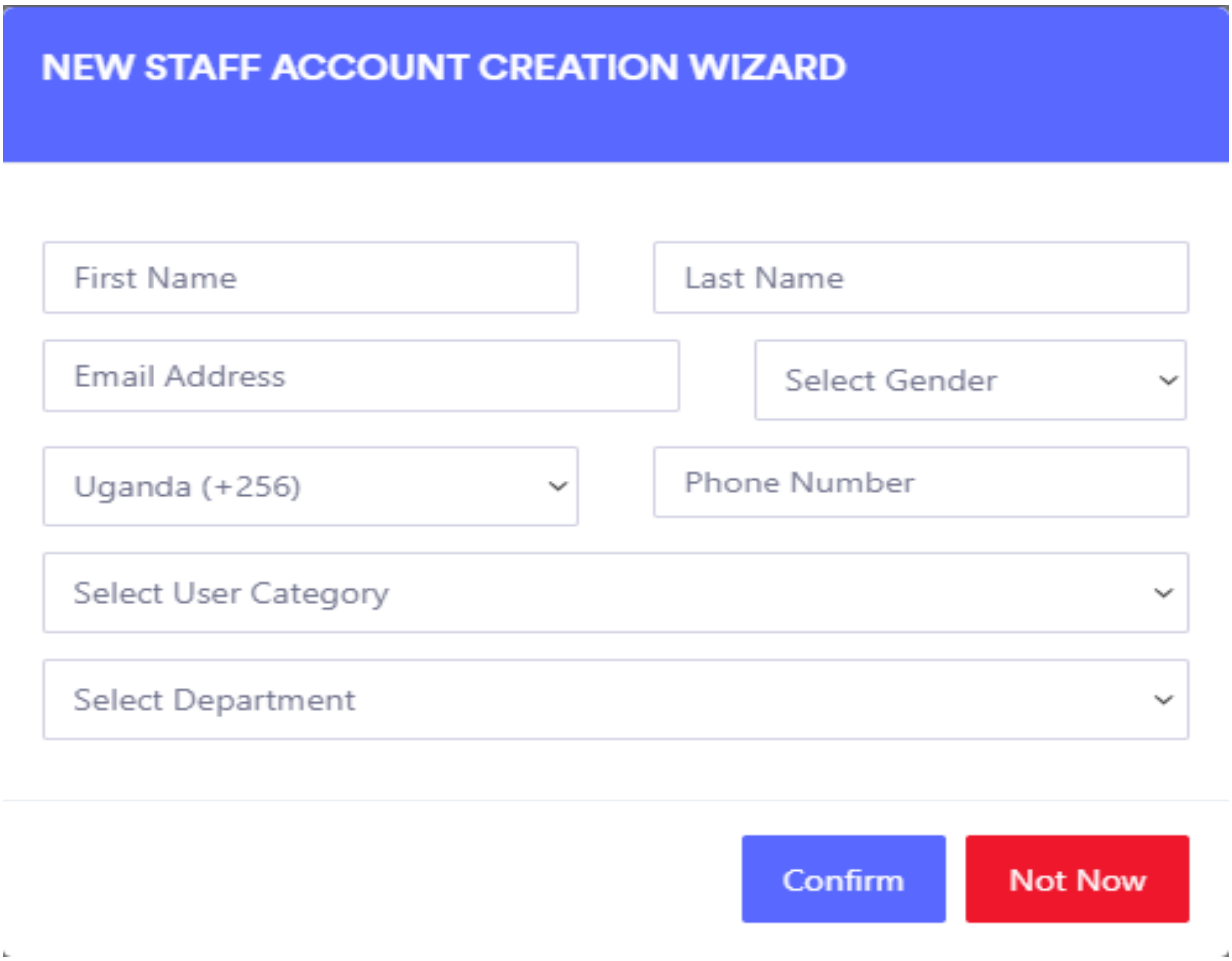


Figure 2: New User Account Creation Interface

The figure above shows new user account creation interface. On this interface, a bank administrator is able to provide basic information about a user which is used to set up an account for them as well labelled in the form placeholders above. After validating that the email or phone number is not already in use, the system concatenates the selected country code and the provided phone number to generate a full number with a plus which together with the email address acts as the address to which the system generated authentication credentials for that account are sent i.e., username and password. After sending a copy, the system goes ahead and encrypts them before being inserted in the authentication table. Encryption is done using a PHP encryption method which takes in two argument i.e., the encryption algorithm **sha256** and the string to be encrypted i.e., username or password to form a ciphertext (encrypted). Formula below clearly explains the process of encryption in the developed model.

Where ***x*** represents the encrypted string to be obtained(ciphertext), ***hash*** is the predefined PHP function used to encrypt, ***y*** is passed as ***sha256*** which is the encryption alogorithm and ***z*** is the text to be encrypted in plain text i.e., username or password in plain text. Once this step is completed, the system sends a POST request to the MySQL in order to store the user information in the

database. The posted information includes an ID which is automatically generated. The ID is used as a primary attribute to uniquely represent and track user actions in the system.

Attempting a Questionnaire

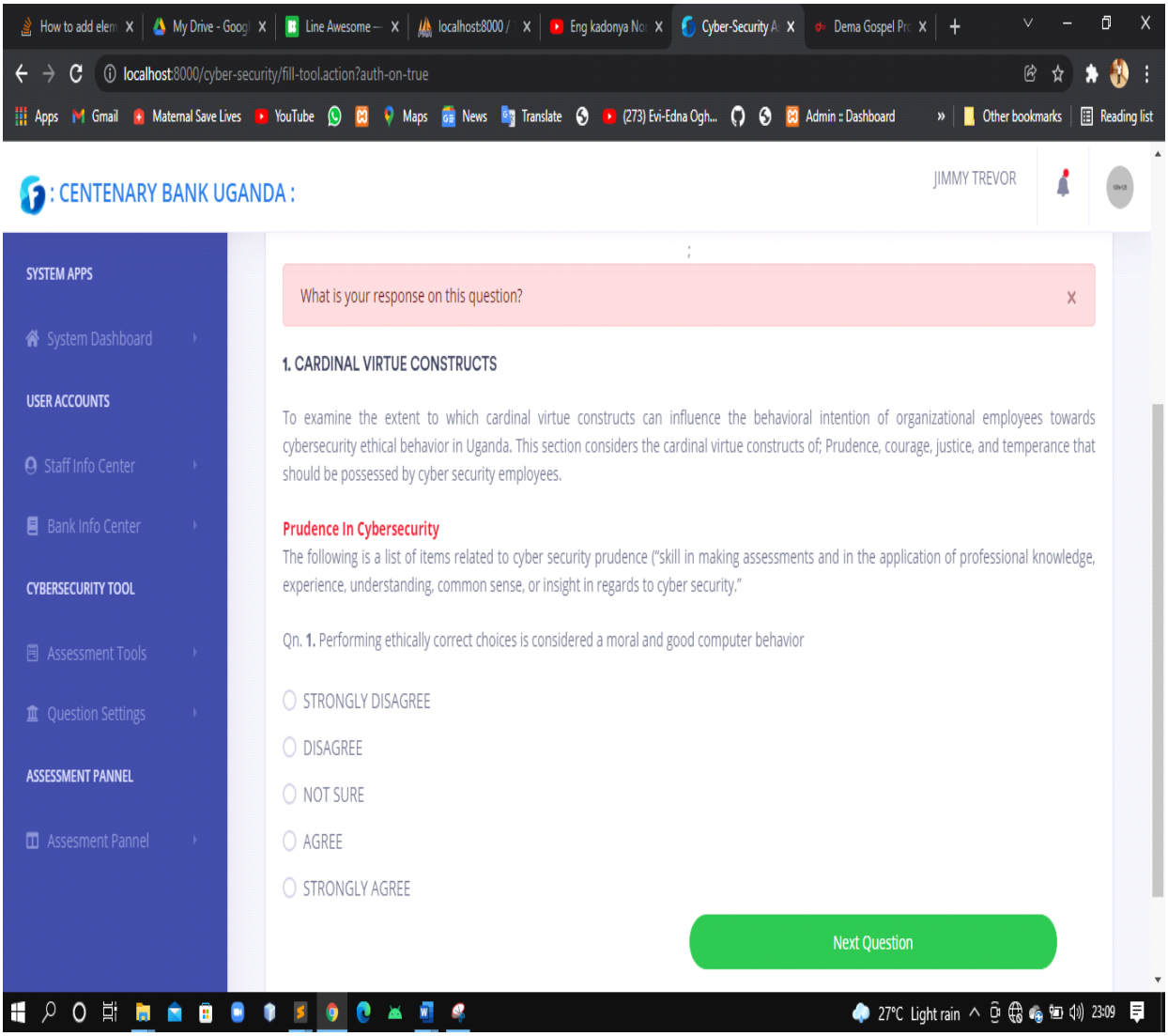


Figure 9: Attempting the Questionnaire

The figure above provides a clear view of how the assessment is conducted in the system. On this interface, a user is able to interact with the system by providing their view or level of satistication based on the question displayed. During the question setting, each question is given a response type which is used to determine the degree of user's satisfaction towards that question. Each response type is allocated different levels where a user selects basing on their satisfaction toward the question. Majorly, two response types are used in the model.

These include **True/False Type** with level of ***mostly false, somewhat false, somewhat true, mostly true, completely true and agree/disagree type with levels of strongly disagree, disagree, not sure, agree, and strongly agree. Each response type level is assigned a mark/ numeric value which is***

based on to assess user's performance. 1- Mostly false, 2- somewhat false, 3- somewhat true, 4- mostly true, 5-completely true.

After a user providing their response, the system sends a POST request to the server containing the reponse Value/Mark, Question ID, User ID and store the information in the result entity in the database which waits for at least 85% of the attempt to mathematically compute the results.

Marking and Tot Up

To the employees assessed, the system bases on the number of questions a model contains to determine the response progress as given in the formula below;

To the employees assessed, the system bases on the number of questions a model contains to determine the response progress as given in the formula below;

$$\boldsymbol{Res} = (\boldsymbol{NoQ}/\boldsymbol{TnQ}) * \mathbf{100}$$

Where $\boldsymbol{Res}$ respresent the Assessment progress result in percentages, $\boldsymbol{NoQ}$ represents the Number of Question Attempted and $\boldsymbol{TnQ}$ is the Total number of questions in a given cybersecurity ethical behavior assessment model. ***Note***: For an employee to be assessed, the $\boldsymbol{Res}$ must be above $\mathbf{85\%}$**.**

Computing the Employee Assessment Score (EAS)

The computation is based on the Employee response on a given Question. The system adds the response values/marks of all questions divides it with the maximum score possible and multiplies the result by 100 to convert it to percentage.

Computing the Maximum Score Possible ($\boldsymbol{MsP}$)

The MsP is given by the fomular below;

$$\boldsymbol{MsP} = (\boldsymbol{TnP} * \mathbf{5})$$

Where the TnP is the Total number of Questions in the given assessment model. The value Five (5) is considered to be the maximum response type value based on the range. This means response values ranges from $1 - 5$.

Computing the Total Response Score ($\boldsymbol{TrS}$)

The TrS is given by the fomular below;

$$\boldsymbol{TrS} += \boldsymbol{SqV} \quad \textbf{OR} \quad \boldsymbol{TrS} = \boldsymbol{TrS} + \boldsymbol{SqV}$$

Where the $\boldsymbol{TrS}$ is given an initial numeric value Zero (0) and then subjected to the loop counted basing on all the questions attempted. As loop counter traversers through the attempts, it add the $\boldsymbol{SqV}$ which is the Single Question value to the $\boldsymbol{TrS}$ basing on the given criteria/ condition which looks at traversing through all the question attempts of a given user. When the loop counter terminates, the last incremented $\boldsymbol{TrS}$ value is recorded.

Computing the Final Assessment Results ($\boldsymbol{FaR}$)

The $\boldsymbol{FaR}$ is given by the formula below;

$$\boldsymbol{FaS} = (\boldsymbol{TrS}/\boldsymbol{MsP}) * \mathbf{100}$$

Where the $\boldsymbol{Trs}$ is the Total response score and $\boldsymbol{MsP}$ is the Maximum Score Possible.

Determining the Employee Recommendation

The employee recommendation is determine by the Final Assessment Results **(FaR).** The FaR is subjected to a condition statement i.e. , **IF Statement** to make decision regarding employee performance. This determination was done using the formula below;

$$if\,(\boldsymbol{intval}(FaR) \geq 50):$$

$$Cybersecurity\ ethical\ behavior\ Assessment\ Passed$$

$$else:$$

$$\boldsymbol{Cybersecurity\ ethical\ behavior\ Training\ Needed}$$

Where $intval()$ is the function used to convert the result of FaR to an integer value.

Assessment Results

Assessment Results

Show 10 entries Search:

ID	Staff Name	Phone	Attempts	Tool Qns	Score	% Score	Recomendation
1	Jimmy Ssegujja	+256774165087	60 (100%)	60	183	39%	CyberSec Ethics Training Needed
2	Emma Muheerza	+256756254760	60 (100%)	60	221	27%	CyberSec Ethics Training Needed
3	Chris Trevor	+256752453485	59 (98%)	60	129	57%	CyberSec Ethics Assessment Passed
4	Tonny Engwau	+256751636282	51 (85%)	60	128	58%	CyberSec Ethics Assessment Passed
5	Ruth Nakato	+256701501880	10 (16%)	60	32	85% of Tool Attempt not reached	85% of Tool Attempt not reached

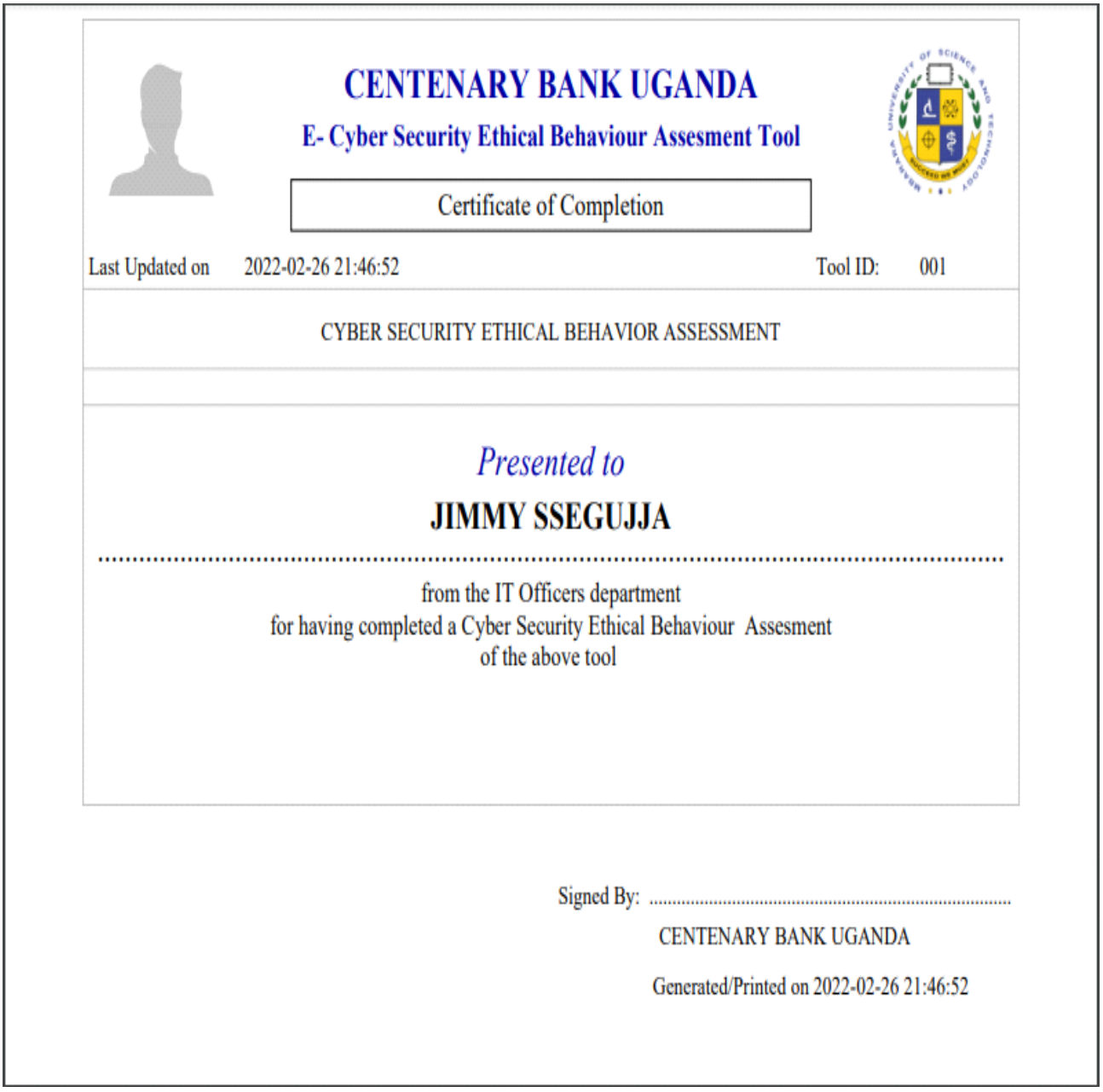
Showing 1 to 5 of 5 entries Previous 1 Next

Figure 10: Assessment Results

The figure below shows a report generated by the system displaying the assessment progress of each staff on a given cybersecurity ethical behavior assessment model. The report only shows those employees who have made any progress towards attempting the assessment model. The

reversed result set of this report is a list of employees who are registered in the system but have not attempted any assessment question under the selected model.

Complete assessment Certificate



CENTENARY BANK UGANDA

E- Cyber Security Ethical Behaviour Assesment Tool

Certificate of Completion

Last Updated on 2022-02-26 21:46:52 Tool ID: 001

CYBER SECURITY ETHICAL BEHAVIOR ASSESSMENT

Presented to

JIMMY SSEGUJJA

from the IT Officers department
for having completed a Cyber Security Ethical Behaviour Assesment
of the above tool

Signed By: .....

CENTENARY BANK UGANDA

Generated/Printed on 2022-02-26 21:46:52

Figure 11: Complete Assessment Certificate.

Figure above a sample certificate generated by the system when an employee completes the assessment exercise for a given cybersecurity assessment model. An employee who has completed the assessment can download the certificate and take it to the bank administrators to attach a signature and a bank stamp in order to brand its authenticity.

4.0 CONCLUSION AND RECOMMENDATIONS

Conclusion

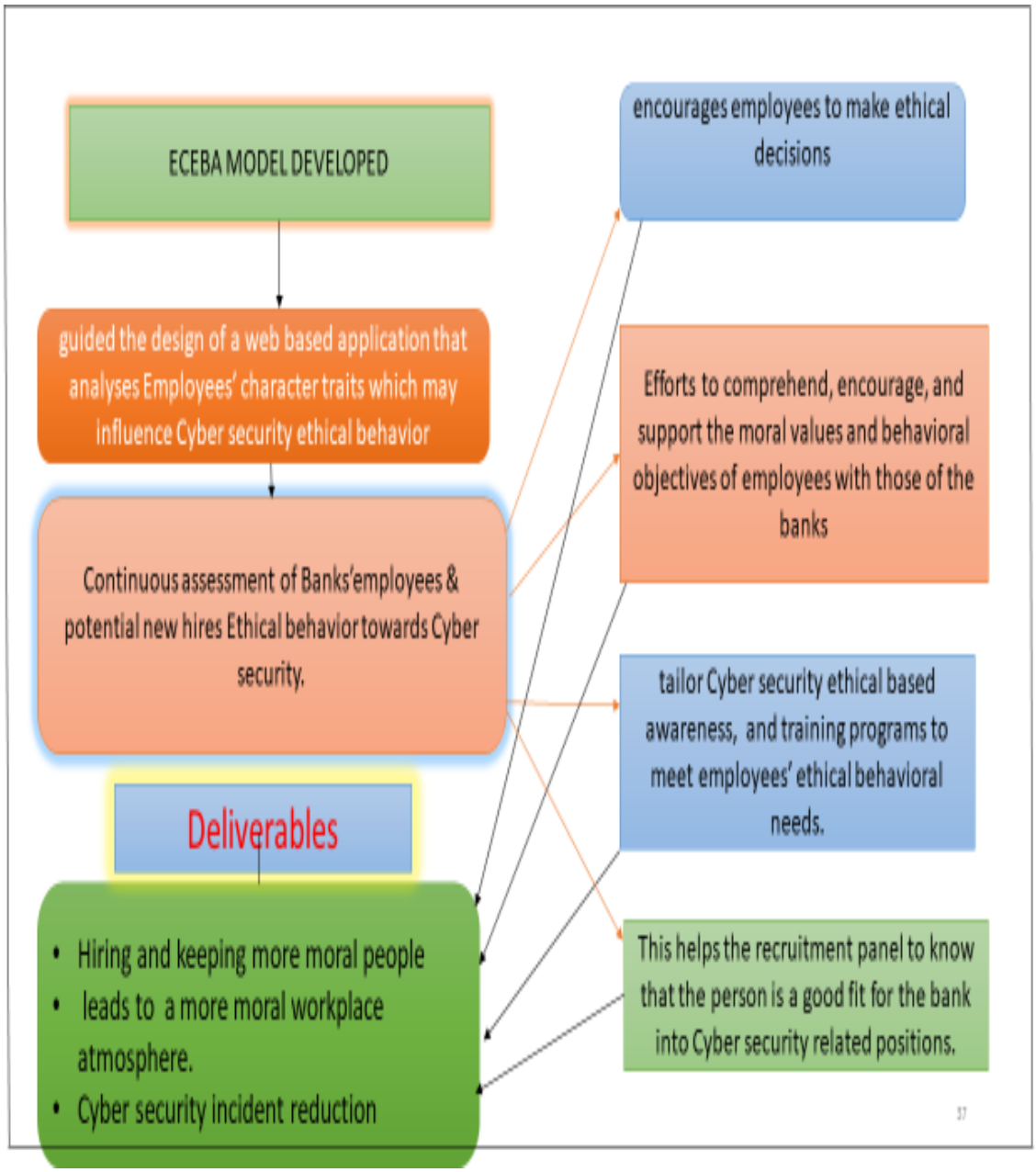


Figure 12: Conclusion of the Study

Recommendations and Future Research

This study is a stepping stone for further research into virtue ethics for addressing behavioral issues linked to upholding Cyber security. It offers the interfaces of the components and indicators of an employee ethical behavior assessment model and provides a structure for future research.

A web based Cyber security ethical behavior assessment model is of great prominence to banks' employees. However, the banks' employees' awareness of the existence of the system is required

to help increase acceptance and execution of this model. ETHICA can progressively be made known to the entire bank by the systems' administrator cooperating with all bank branch managers and heads of departments so as to create more awareness about its existence. In so doing Cyber security ethical behavior assessments could be a continuous process and be used to identify and address employees' unethical behavior and reduce Cyber insecurity caused by insiders.

The developed model might be of help in identifying ethical virtue traits of a prospective new employee's background. This can provide insight as to whether the individual is ethically and morally well-grounded. This helps the recruitment panel to know that the person is a good fit for the bank into Cyber security related situations.

The banks are encouraged to implement this model and use it as a methodology to identify an employee's style of ethical decision making towards Cyber security.

REFERENCES

Ait Maalem . R. L., et al. (2020), Review and insight on the behavioral aspects of Cybersecurity

Carter, A. and Crumpler, W D. (2019). Financial Sector Cyber Security Requirements in the Asia-Pacific Region; A Report of the CSIS Technology Policy Program

Cybersecurity (2020) 3:10

Dupont, B. (2019). The Cyber-resilience of financial institutions significance and applicability Journal of Cyber security, 2019, Vol. 5, No. 1

Gray, J. .M (2015). Virtue Ethics: Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (364)

Kuepper, (2019) Bank Fraud effects on the banking industry, customers and the economy Cyberattacks and Bank Failures

Lule & Buregyeya, (2023) reporting for New vision newspaper of Tuesday February, 14, 2023 page 7.

Malik, S., Shazia, N., Awan, A. G. (2018), The Impact of Cybercrimes on the Efficiency of Banking Sector of Pakistan Global journal of management, social sciences and humanities Vol 4 (4), pp. 821-842.

Matovu, A. (2018). Electronic Fraud and performance of Retail Banking in Uganda: A Case Study of Centenary Bank limited Mapeera House. Masters level. Nkumba University

Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 2873–2882.

THIRD NATIONAL DEVELOPMENT PLAN (NDPIII) 2020/21 – 2024/25; July 2020 NATIONAL PLANNING AUTHORITY

Tumuhimbise, W., Atwine, D., Kaggwa, F. et al. (2022). Enhancing Tuberculosis Care in Southwestern Uganda: Facilitators and Barriers to Utilizing Mobile Health Technologies. Glob Implement Res Appl https://doi.org/10.1007/s43477-022-00056-1.

Yatich, H. K., & **Musebe**, R. (**2017**). Assessment of ethical behaviour on organizational performance. African Journal of Business Management, 11(1), 12-16.

Zahoor, Z., Ud-din, Moin., Sunami, K. (2016). Challenges in Privacy and Security in Banking Sector and Related Countermeasures. International Journal of Computer Applications (0975 – 8887) Volume 144 – No.3.

Khan, N.F., Ikram, N., Saleem, S. et al. Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. Secur J (2022). https://doi.org/10.1057/s41284-022-00343-4

Murithi, J., Yoo, J.E. Teachers' use of ICT in implementing the competency-based curriculum in Kenyan public primary schools. Innov Educ 3, 5 (2021). https://doi.org/10.1186/s42862-021-00012-0

C. Russu. (2022) The impact of low cyber security on the development of poor nations | Experts' Opinions

ADDRESS OF HON. JUSTICE ALFONSE CHIGAMOY OWINY – DOLLO CHIEF JUSTICE OF UGANDA; DELIVERED AT THE NEW LAW YEAR, 2023 AT HIGH COURT GROUNDS, KAMPALA ON 3rd FEBRUARY 2023

Zahoor, Z., Ud-din, Moin., Sunami, K. (2016). Challenges in Privacy and Security in Banking Sector and Related Countermeasures. International Journal of Computer Applications (0975 – 8887) Volume 144 – No.3.

MacIntyre, A. C. (1984). After virtue. A study in moral theory. Notre Dame, IN: University of Notre Dame Press.

Ajzen, I. (1991). The theory of planned behavior, Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179-211.

Ifinedo, I. (2012). Effects of organization insiders' self-control and relevant knowledge on participation in information systems security deviant behavior.

Tommasetti, P. Singer, Orlando T. et al., (2018). Extended Theory of Planned Behavior (ETPB): Investigating Customers' Perception of Restaurants Sustainability by Testing a Structural Equation Model Sustainability, 10, 2580;

Uffen. J. and Breitner M.H (2013). Management of technical security measures: an empirical examination of personality traits and behavioral intentions. System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE

Kuenzi, et al., (2019) Creating an ethical organizational environment: The relationship between ethical leadership, ethical organizational climate, and unethical behavior; Personnel Psychology. 1–29. Wiley Periodicals, Inc.

©2023 by the Authors. This Article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/

View publication stats