Journal of Advanced Computer Science & Technology, 12 (1) (2024) 1-18

Journal of Advanced Computer Science & Technology

Website: www.sciencepubco.com/index.php/JACST

Research paper

Billing and online payment portal with multi-factor authentication using one-time password

Christle Mae Reyes Aribon-Libag *

University of Mindanao, Philippines
**Corresponding author E-mail: christlemae.libag@gmail.com*

Abstract

NCTVN Cable Network Corporation is a cable/internet distributor in Kidapawan City. Its area of operation covers Makilala, Arakan, Antipas,Matalam, Midsayap,Magpet President Roxas, Kabacan and Kidapawan City. The users of cable and internet rely to them in which they have to extend their services to the Province. By this venture, the number of subscribers of their services has grown and the area covered are widen. Given the number of subscribers there is a need to create a consistent and quick support to their customers in terms of billing presentment and payment. In the current process, Billing and delivery of the statement is one of the challenges they are facing where they usually cover cost for their workforce, paying onsite over the counter of the subscribers takes a lot of time and payment is unsafe if the collector will intend to run the money. NCTVN manual process cannot take it enough to manage their business. The aim of this project is to help the NCTVN Cable Network Corporation by developing billing and online payment portal integrated with multi-factor authentication. There are two way to access the site. First, Web Portal and Second, Mobile Application named NPAy Application (app). The system enables the customer to pay their monthly bill through the use of online payment portal using available merchants like Gcash, Maya, coin.ph and many other as payment gateway with added security features to secure the customer's information and payment online.
The best part of this app is the easiness of the users (referring to admin and customer) to access their NPay app anytime and anywhere as long as the customer is connected with internet, see their monthly bills, pay online and secure the system process and transaction from registration of customer's account down to the payment process where system will validate or authenticate using One-Time Password (OTP).
The App is design to serve one user's roles: The Subscribers of NCTVN Cable Network Corporation. For the designing and development of the project, PHP has been used for the programming language and MySQL for the integration of database, and this system was hosted in exonhost.com with the live domain name of www.nctvn2022.site as official address. Varieties of methods of testing were applied to test if the anticipated output was effectively delivered. Test results and cases were created and distributed. The outcomes show that the system satisfied the user's expectations and successfully completed the testing phase.
Furthermore, this system is optional for the users due to the following factors: First, Subscribers are from far flung barangay with no internet or cellular connection, and no mobile phones or Personal Computer. But for the customers who intend to use it. This system is beneficial to them because the process and customer will experience direct support from the company with the contact less setup, fast, easy-to-used and effective billing and payment portal with security features.

Keywords: *Multi-Factor Authentication; One-Time Password (OTP); Payment Gateway; Billing, Payment; Web Portal and Mobile Application.*

1. Introduction

Technological revolution brings us great changes to mankind and access to information become available anytime and anywhere with the use of internet connectivity as the medium of communication utilized through businesses, educational institutions, public and private entities, and other line agencies with their day to day operation. Since businesses in different categories has been evolved, it is necessary to shift to digital interactions among businesses and consumer through development of innovative information system interrelated and connected by the establishment of systematic process where the simple use of available devices has really become automated.
Before the Covid-19 epidemic, digital services were often contactless. Few people use contactless services. But The Covid-19 outbreak in early 2020 altered people's lifestyles and access to information. This has resulted in the expansion of contactless digital technologies for the benefit of customers and organizations. [4]. [1] Online payment is a second-best alternative during the COVID-19 problem, as full contactless online payment can eliminate the necessity for in-person cash exchange. Governments should therefore actively engage banks and e-money providers, encouraging them to simplify the process for businesses and households to gain access to remote electronic payment capabilities during the crisis, including by limiting physical interaction during the onboarding process. However, few researches have looked into the adoption and spread of contactless digital technology in developing countries. [5]. Somehow, these studies are similar reason and a way to engage and resolve manual business processes or services like NCTVN.

Copyright © Christle Mae Reyes Aribon-Libag. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

There are some organizations that still use the manual process and did not adapt to digital transformations/automation. Some considers the cost, effort and time are always become operational business constraint. One way to address the issue of providing business services is to adopt the second-best payment method, full contactless online payment, which offers customers of the company quality, flexibility, cost-effectiveness, and automation in exchange for a better solution to automate and secure the business process.

Based on the interview conducted, the following problem were identified: First, Outdated delivery and issuance of billing statement is one of the challenges that the customers are facing where bill distributor needs to do the house-to-house distribution of bills that will cause delays and it causes sudden payment obligation for the customers in closest due date. In addition, the corporation pays the costs associated with its employees.

Second, paying onsite and over the counter takes a lot of time for the customers just to secure their obligation for payment. On the other hand, paying directly to the bill distributor/collector is unsafe because they might intend to run-off with the money; and

Third, despite the fact that the consumer was given with a handwritten receipt, the payment was dubious because the customer cannot be updated if the payment made with the bill-distributor/collector was posted. The office might not get the collection in a timely manner. In addition, certain bill distributors who are no longer affiliated with the business are continuing receiving payments.

Based on the problem mentioned above, the development of this system proposal was realized in the real situation of the company in dealing and managing their business. The NCTVN Billing and Online Payment Portal with Multi-factor authentication using One-time Password is believed to achieve transformation in the business process and this system will really help the company reduce cost for man power, time and effort for reaching out their customers, and secure all the transaction and payments created using the system. The deployment was organized through strong database management and a quality resource was used for effective and efficient support of the company to their clientele.

1.1. Purpose and description

To make it easier and improve the services of NCTVN in terms of billing and online payment collection. The company needs a new strategies to their process using these proposed system as interventions to become more competitive as a cable/internet service provider. Using the billing and online payment system with the integration of multi-factor authentications through the use of OTP via SMS/Email as part of human verification to avoid uncontrollable and suspicious activities. The manual process of the delivery of the billing statements will be available online through the individual dashboard of the customers. It is more advantage and convenient to the customers instead of paying their due balance payment through visiting NCTVN office as if the system will be utilized as their solution and promotions to their clientele and also will allow user to experience error less, accurate, automated and handy.

The end user who will use the system will experience convenient and real time support beyond their control in such viewing of billing statements, notification of advisory, support to transaction concerns and ease of doing payments online. However, this technology was designed as simple to easily predict the functionalities of the system features. The online payment facility maybe used 24/7 with a single tap to a “Pay Now” button and pay to the merchant provided as option of payment gateway by the proposed system. This system will always ask for authentication for new and existing customers to keep the transaction secure and safe which the main integration for security support is enabling the system governed by an authentication and verification/validation. On the collection of data, the system observed data privacy and non-disclosure policy, so the sharing of information needs a confidential and observed acts and regulations imposed to it. To ensure that these systems are secure, reliable, and accessible to all users, various challenges need to be overcome. These security features integrated in the system are required for online transactions since the clients swiftly and conveniently paying online using the NPay Portal. In terms of development strategy and preparation. This concept will be utilized through web and mobile first availability. Every device which has an ability to connect to an internet and provide data connection can access the system using unique credentials as part of security measures. The customer will register their account through their account number received from email or SMS to gain personal access to the system. All of the features are functional and will cover and automate the entire process of NCTVN specifically observing the best layers of authentication for strong security and quality data control.

1.2. Objectives of the study

The main objective of the proposed system is to design and develop a Billing and Online Payment Portal with multi-factor authentication through the use of One-Time Password (OTP) exclusively for NCTVN Cable Network Corporation in Kidapawan City branch, specifically:

1) To develop a web-based and mobile application that can allow the user to view and update their monthly billing based on the plan they availed;
2) To develop a web-based and mobile application that can make online payment integrated with a multi-layer authentication using One-Time Password with the system-enabled processes by sending notification and verification codes through SMS or electronic email to ensure that the data collection, billing features and online payment is protected; and
3) To develop a system that enable to generate payment confirmation via SMS or Electronic Mail.

1.3. Scope and limitation

The development of this proposed project is intended to the subscribers of NCTVN Cable Network Corporation Kidapawan City Branch and the sole beneficiary of this implementation. The proposed system can be accessed also by admin through web and customer in mobile and web that will work when the respective form of device is connected to the internet. On the other hand, the customers can pay their bills through the Online Payment Portal (named to be NPay). The only pre-requisite to have a successful transaction through the payment merchant is to have sufficient balance as payment reference is presented through the billing statement automatically generated by the system.

For the limitation, the main focus of this project is for the customer’s side (Subscribers)of NCTVN only because the system main features are on billing presentment and online payment. Therefore, the system not yet connects to the existing billing and payment system of the NCTVN Company. Though there is an admin management of the proposed and developed Billing and Online Payment Portal, the admin has the full access and privilege to the use of the system. The features like managing users, managing customers, managing payments and managing system maintenance are the functionalities beyond the control of the administrator but the system cannot provide a factual report, proper formatting of document report including the signatories.

On the other hand, customers have limited engagement and use where their access is just on their respective dashboard. The common features that are allowed to be managed by the customer is to view billing statement through email, make a payment, received notifications

and OTP, and update their account details in which has driven some scope and limitation to standardized the usual usage of every role in the system.
In the payment limitation, system functions that can filter the payment once there are three (3) consecutive unpaid bills reflected in their billing statement and provide a Disconnection letter. And since the system issued some integration to third party features such for payment gateway for the online payment facility will be enabled with embedded security measures and cannot be alter by the customer in paying their personal bills payment. In such, SMS gateway also will be limited to the use of the customer where this integration purposely added to automate the messaging process. This mechanism is reliable to integrate as a function referring to the limitations and the scope of the user role.

2. Review of related literatures and system

This chapter provides a review of the research literature, empirical evidences and studies in relation to web-based invoicing, electronic billing and online payment processes integrated with multi-layer authentication using time-based OTP algorithm which supports the worked discussed in this research proposal.

2.1. Related literatures

The widespread use and commercialization of the Internet have resulted in a vibrant world of electronic commerce. The E-commerce is a boom in the modern business. The environment, organization, and performance are considered as benefits for developing countries could employ to boost e-commerce adoption. [3]. practically, e-commerce in India began to acquire popularity as the number of internet users and smart phone sales increased. However, there is no doubt that e-commerce has become popular among around 30% of the population living in cities throughout the years, but owing to a limited range of product diversity and standardization, e-commerce sales are not increasing at a quicker rate. [6].The electronic bill presentment and payment (EBPP) comprises sending bills and placing bill payment requests via the Internet or a proprietary electronic network. In a typical transaction, a consumer receives an electronic bill along with a link to payment choices. Following a perusal of the bill, the customer clicks on the link, selecting a payment option and initiating the transfer of funds. [18] Electronic bill presentment can be done independently from electronic bill payment; in fact, some companies only provide presentment or payment services. The technology can be utilized in business-to-consumer activities such as utility and credit card bill payment, as well as business-to-business transactions such as procurement bills and invoice payment. [19].

2.2. Related systems

In the Study on Impact of Online Payment Applications Among Youngsters with Reference To Google Pay. Google Pay is taking giant steps at revolutionizing the payments markets in India. Consumers or users will miss aboard of features and easy money transfer transactions if they don't use the app. The popularity of these apps for online payments has skyrocketed in recent years. The number of Google Pay users is growing at a rapid pace. More security features need to be added to increase the user base further in future. Many respondents said that cashless transactions in India were unsafe, and that the government should make electronic payment infrastructure entirely safe and secure. Government should ought to make a system infrastructure that is capable and secure so that there is as less fraud and theft. Similar services offered of the proposed system Billing and Online Payment Portal [16]. To avoid unsafe transactions and hacking of the system a multi-factor authentication and integration of md5 and sha1 combination of password encryption was applied to secure online process and to increase the system security. According to [17] Although no security measures can ensure 100% online payment security, but they can significantly minimize the number of online payment frauds.
To address the above security issues, One-time password (OTP) authentication (also known as dynamic password) is employed. The enhanced validation, often known as two-factor authentication, requires the user to supply both a static password and a dynamic OTP. [8]. The OTP is used to protect validation systems from common attacks because attackers must determine and consume each OTP before a real user can use it during each authentication session. Home credit online payments, in any other manner authorized or made by the Cardholder, whether or not a sales slip, Cash Withdrawal form, or other proof of purchase or order form is signed by the Cardholder, or confirmed by Personal Identification Number (PIN), One-Time Password (OTP), or via mobile application as applicable. The researcher came to realize that time-based one time password can be used to implement the security of client's data and information to eliminate cyber fraud with the intent to corrupt other individuals' personal and financial information to be transacted online. For data protection such as Log in accounts, codes and personal information. The cloud computing paradigm is one of the rich standards for computer environments that provide services over the Internet with numerous features such as service robustness. The expeditious growth of cloud computing demand has raised a greater concern for security threats. Nowadays, security is considered as one of the major parameters for obtaining services in any Cloud platform and The use of MD5-crypt is one of the common password hashing algorithms supported by the majority of Linux distributions and implemented in Cisco routers. [20]. SHA-1 is the most frequently used of the extant SHA hash algorithms, and it is utilized in many popular security applications and protocols. Because SHA-1 is fast and input-sensitive, it is used to improve the diffusion effect on image pixels. In the propose system through multi-layer authentication and integration of md5 and sha1 combination of password encryption the process would secure online process to increase the system security.
News published by Manila Bulletin, November 24, 2017, A Mini stop becomes the 1st convenience store to accept QR payments via GCash. The researched came out with the idea to use the digital payment in the companies mentioned like Gcash, PayMaya, Coins.ph and others to serve as payment options for the consumer's account. Security and privacy of user information are critical challenges in an online environment where authentication is essential. [10]. It checks the validity of a person attempting to access a protected system in order to prevent unlawful recovery of the user's personal information. [11]&[12]. There are several techniques employed to perform authentication (Table 1) classified as knowledge-based, token-based, and biometric-based authentication schemes.

Table 1: Authentication Classification and Schemes

	Knowledge-based	Token-based	Biometric-based	
	Text Passwords	ID-based (Smart Cards)	Face Biometrics	Fingerprints
	Graphical Passwords	One Time Password (OTP) tokens	Keystroke Biometrics	Iris Biometrics
Scheme Examples	Cognitive Authentication	Mobile-based	Hand Gestures	Brainwaves
	Personal Identification Number (PIN)		Palmprint Biometrics	Heartbeats
	Questions		Touchstroke Biometrics	Knuckleprint Biometrics
			Gait Biometrics	Multi-modal Biometrics
			Behavioral Biometrics	

To authenticate user identification, many Android apps use password authentication techniques. However, many security breaches in recent years ACSAC '19, December 9-13, 2019, San Juan, PR, USA resulted in widespread password leaks. Moreover, users usually choose weak passwords (e.g., the infamous “123456”) because a secure password is often too complex to remember. Because of such issues, a single password authentication becomes vulnerable to attacks such as brute force or dictionary-based search, and thus is not suitable for user login protection.

Talking about the automatic reminders, on the systematic literature reviewed from the total of 1202 papers that associated to electronic invoicing, technological aspect related and notification they selected 39 papers and showed the absence of notifications into electronic invoicing system. The researcher develops a system turning the use of emails, instant messaging applications, and SMS as a regular way to be informed. These are key channels for the delivery of business information, from Business to Consumers (B2C)[7].

In the local process in the Philippines, a researcher from Sultan Kudarat State University develops a School Portal System with Notification System with SMS Notification for Sultan Kudarat State University Kalamansig Campus. “The School Portal System with SMS notification is web based that will manage all the news and events in university and notify the students and professors or faculty staffs through SMS”. With the idea of SMS notification, the researcher also added short message system for invoicing, registration and payment confirmation to provide a very convenient method of exchanging small bits of information between the system and the consumer's bills and payments. In the same survey, 54 percent claimed that utilizing an e-payment option made transactions faster. [21]. SMS Notification is adopted and embedded to the system proposed to enabled the direct reminder of billing statement, received payment confirmation and OTTP. In any role, you can be notified at your utmost convenient in the reach of the feature.

Furthermore, in all businesses and organization a website has become the most important public communication portal for most. Today, the address could indeed refer to a sophisticated (Web) application being invoked.

Advance in mobile technology have enabled a wide range of application to be developedthat can be used by people in the move. Nowadays, people are surfing the internet by using a computer or mobile phone to do their work. To surf the internet, people need to use a web system or mobile applications as their platform. A web system or website has a unique link. The mobile applications are a software application developed specifically for use on small wireless computing devices such as smartphones and tablets rather than desktop or laptop computers. Furthermore, mobile applications designed with consideration for the demands and constraints of the devices and to take advantage of any specialized capabilities they have. Both of these can use to surf . The demand for a single integrated, easy-to-use, access to information applications and people within a network of users is increasing more and more [13] . The study tends to give an idea on how usefully and effective to develop a web and mobile application where the NCTVN web portal and Npay app can be access

Through this review of related literature to the research and study conducted in relation to the institutionalization of billing system and online payment portal with the multi layered authentication using proven OTP algorithm exclusively to the proponent of this study the NCTVN Cable Corporation which operates in lined business integrated with the various literature provided above as reference that the development will make use of this resources to collaboratively be completed with the projected scope and limitations and the main objectives of this study.

3. Technical background

This chapter discusses the technicality of the project, by which describes the type of the project to be developed and its functionality including its underlying frameworks and models.

3.1. Conceptual framework

Conceptual Framework shows the description of the desired application, criteria for completion and provides an overall guidance to ensure that everyone is on the same page in understanding and conceptualizing of the proposed project. The proponent presents the proposed Input-Process-Output (IPO) for the client who is the beneficiary of this system and the end users which are the consumers of the beneficiary of the said system which will show in the figure below.

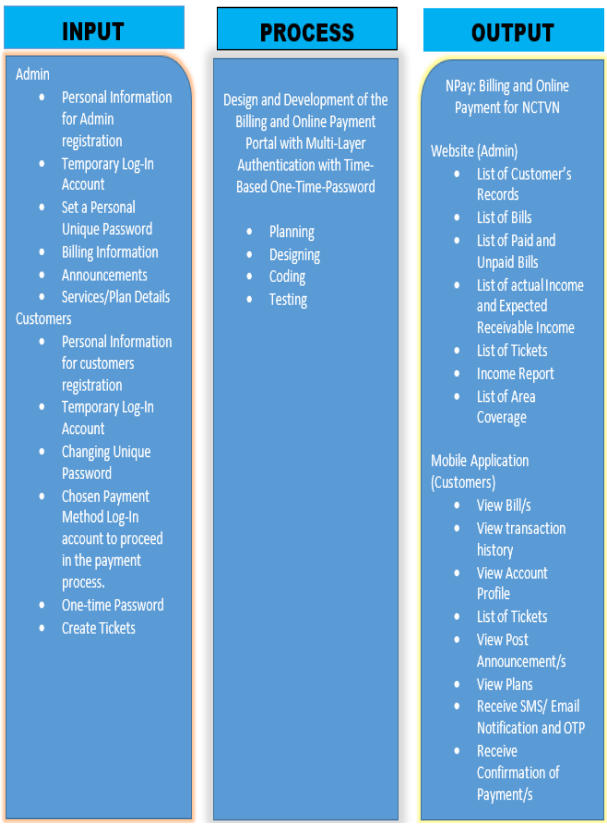


Fig. 1: Input-Process-Output.

- Input/Process/Output - Admin

The Figure 1. above presents the INPUT process of the system, as shown the billing and online payment portal with Multi-Factor Authentication Using OTP system developed for NCTVN is compatible to desktop/laptop and mobile device as means of input device to interact with the system. In this input procedure, the users as admin which is referred as the beneficiary of the project is expected to input their credentials for login features, update their account, and overdo in all of the privileges in the whole functionality of the system.

The PROCESS inside the system from the execution of procedure from the users (admin) the system will process through series of functionalities like managing all customer records, managing bill and dispositions, create announcements, managing all tickets, manage site basic settings like adding of plan, advisory type and area coverage. While as process in the integration of authentication, the system integrates One-Time Password (OTP) as verification method, validation codes will also process and capture credentials eligibility in gaining login access, and forgot password recovery method that allow users to change their password. The system also integrates reCAPTCHA which uses Google Authorization to verify an expected user.

The system OUTPUT can now provide all consolidated data in a table form which has an action buttons that will perform delete, update/view and add function. As overall output, all the output data can be seen in the Admin Dashboard.

- Input/Process/Output – Customer

The Figure 1 presents the INPUT process of the system from customer, as shown the billing and online payment portal system developed for NCTVN System is available for mobile as means of input device to interact with the system. In this input procedure, the user as customers which is the main user that will make use and interact with the system is expected to input their credentials for login features, update their account, view billing and transaction history, change password and create tickets for issues/concerns.

The PROCESS inside the system from the execution of procedure from the user (customers) the system will process through a functional requirement where login process needs a valid credential using Account No., Password, Forgot Password Recovery feature, and Account Inquiry using Account No. In customer login, the customer has provided with the Account No. In a unique format with the combination of current year and six (6) digits random numbers (example: 2023123456) which will process and triggered by multi-layer authentication. Before the customer can process the log-in process there is a prompt message asking to enter the OTP code. The system will automatically generate an One-Time Password (OTP) code from SMS API and the customer must enter the OTP code receive via SMS. OTP Code can be used only once.

The system OUTPUT can provide customer the copy of their bill, the status of their payment provided with the billing details which is indicated in the dashboard with the current bill and unpaid bill, also provide ticket status through the Help desk and account profile which will display all the individual customer information. They can also receive SMS Notification for the bill, payment confirmation and OTP.

3.2. System architecture

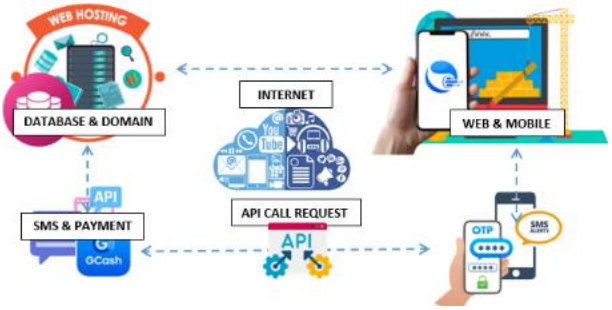


Fig. 2: System Architecture Design.

Figure 2. Shows the proposed system architecture design. In this setup, the main programming platform used to develop is on PHP with version compatibility from 7.4 to latest release to 8.2. For mobile instance, the researcher uses GoNative UI, one of the best system development kit (SDK) that builds and compile mobile application. While using the PHP development a Bootstrap framework and structure has been used to give a stunning user interface that comes with a clean and cool design that is predictive to the eyes of the system users. The approach of development uses object-oriented programming where it will help the developer integrate a well unified codification. In the part of data collection and restoration, this system used MySQL for the database management system where data collected is stored electronically. However, the use of mobile application that runs in the GoNative tool can communicate directly to the database as source of information in creating secure and well-built solution for NCTVN. The user interface comes in two (2)
dashboard, one is the admin where it can perform all privileges and actions throughout the system using web application that runs on a live domain and hosting service and the customer dashboard using the GoNative build mobile application. The web where manages by Administrator can perform the following privileges, as follows: 1.) Can create customer by filling out the form, can delete and update the records in customers table, 2.) Can create bill, process the bill and can check transaction history according to the disposition of admin, 3.) Can create advisory and send advisory through SMS API integration, 4.) Can manage ticket and process, 5.) Can Add an Area, Plan and Advisory Category and can update and delete records all through its corresponding table.
In GoNative build mobile application where it will be handled by customers. The customers can view bill with status, can view account profile and update, can create ticket of their concern and issues and can check if tickets are already processed or closed. This mobile application has integrated specifically and intended for Online Payment Portal facility, in one glance, the customers will be updated anytime, anywhere at one touch over handy integration. The payment process is made easy through the integration of Paymongo as online payment gateway. This concept will help the beneficiary of the system to support the customer and help them experience the convenience while the manual process has to be replaced with this kind of organized process.
Since this system has to collect data and payment from customers, in terms of security vulnerability and quality assurance as part of data privacy and data control. The session of every user has a correspondence where the use of mobile and web become easy. In the login process, the customer will provide their unique Account Number which is automatically generated in the back-end system upon the creation of the account of the individual customer. Hence, there is an SMS Notification that will be sent directly to the registered mobile number with the temporary password. The integration multi-layer authentication using time-based OTP algorithm to provide unique codes to be sent via SMS. This time-based one-time password is uniquely generated through the SMS API that will validate the transaction of the customer or admin. This SMS API also will be used in the advisory and notification for bills, account is created and others. Furthermore, online payment gateway is a tool that transmits payments processes payments in online transactions. The payment method integrated for this system is the use of e-wallets, like available in all of the transactions like Gcash, Maya and Grab as third-party payment solutions provider (merchant).
In this structure, we can guarantee that the workflow process has an organized flow. Referring to the figure above, the system was up to the live server in the use of domain and hosting. This service will hold the system and will communicate to other components like the GoNative UI build for mobile version has limited only for tickets and online payment, where the web itself manages all transactions in the whole system features. While customer will perform payment, the system will trigger the API and the specific codification that will validate and redirect the specific users to the result of their transaction using the system. In overall aspect, with the use of the internet as medium of communication service has the critical role in integration of such mechanisms to make this system functional as to the features and correlation to third party solutions.

3.3. Technicality of the project

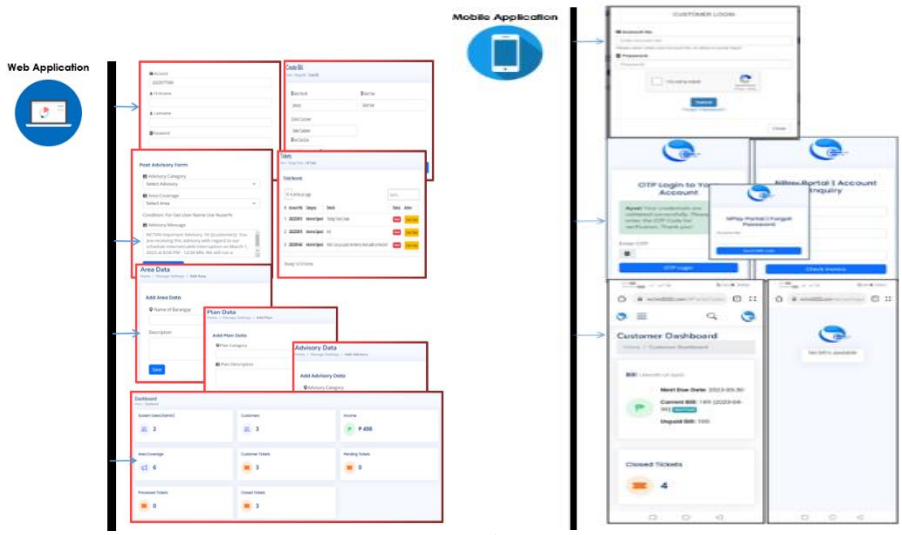


Fig. 3: Technicality of the System.

- Web Application

The web application of this system was designed for the back end components where all of the functions are managed by the system administrator. Like the creation of customer account from there within after availment of the services, manage all customer accounts that will make updating and deleting of the account, manage bill by creating bill for customer's, manage unpaid and paid bills, can post advisory or announcement per area, manage ticker where customer issues and concerns are processed accordingly, and manage back end setting like adding advisory category, plan (subscription) and area coverage details that can be used in the features.

- Mobile Application

The web application of this system was designed for the customer's dashboard that can be manageable through installation of mobile app. This is a simplified GoNative UI that the user can check their account profile and update, can easily view the bill for the current month, create ticket of the issues and concerns and can track it if it is already resolved or not and can inquire individual account through the online portal for the status of the account.

- Algorithm Integration: Multi-layer Authentication

In the setup of the web and mobile system as an application really secured the spaces of the system through integration of system security and data control. This system also has equipped with authentication through the use of SMS API for the notification and OTP and Payment Gateway that will govern to all captured payments and transactions. Through the integration of md5 and sha1 combination of password encryption will increase the security of the system. Ideally, it is being tested before making the development on live server. The server itself has the auto SSL that encrypt the connection between the server and the client. It is a standard security solution that replaces the Secure Socket Layer (SSL) with Transport Layer Security (TLS). SSL enables the safe transmission of sensitive information such as credit card details, social security numbers, and login credentials. Data exchanged between browsers and web servers is typically transferred in plain text, making you open to eavesdropping. An attacker can see and utilize information if they are able to intercept all data transmitted between a browser and a web server.

All means of authentication comes from the complexity of the code use and the verification features of the third party as API that connects directly to this system can be triggered and can capture illegal and fraud intentions using the service particularly in the payment service. The two-factor authentication is just an extra layer of security for a user's account. That means that after enabling two factor authentications, the user has to go through one more step to log in successfully. The usual steps for logging in to an account are:

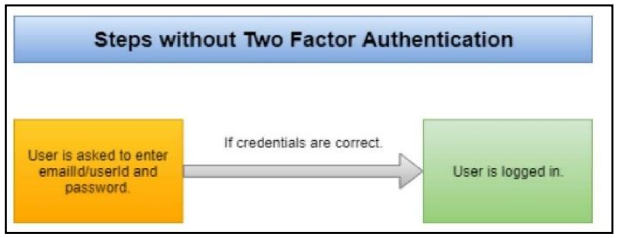


Fig. 4: Usual Steps for Logging in to an Account.

In this method, it shows the process if the system will integrate the multi-layer authentication.

- Login Process

In the login process, the customer and the admin has to bypass the login system. The two users has different style of authentication where Customer has to deal with their personal information and confirmation via OTP using SMS API while Admin has to use email and password with the OTP verification to successfully gain access to the system. The passwords are encrypted by sha1 and md5 so decryption if possible through any form of illegal activities of the system is not possible.

To farther understand the OTP integrated on this system especially in Log-in process. An OTP Authentication API is used. A simplifying User Verification API's are a valuable tool that simplifies the user verification process for developers. These APIs seamlessly integrate one time password (OTP) Verification directly into application or system. With the help of the OTP authentication API, the developers can enhance the security of the application by implementing an additional layer of user authentication.

When a user wants to authenticate or login the application, the application calls the OTP authentication API. This call triggers the generation of a unique OTP or one-time password. The OTP is a temporary code valid for a short period, typically a few minutes.

Once the OTP is generated, the OTP authentication API initiates the delivery process. It sends the OTP to the user's registered mobile number through SMS. This delivery method ensures that the OTP reaches the user quickly and securely. SMS delivery is a widely adopted approach due to its accessibility and familiarity to users.
Developers integrate the OTP authentication API provided by MSG91 into the applications or systems. This involves incorporating API endpoints and implementing the required code to trigger OTP generation and delivery.
User Request: When a user initiates the authentication process, the application sends a request to the OTP authentication API, passing the user's mobile number as a parameter.
OTP Generation: The OTP authentication API generates a random, unique code. This code is typically time-limited to ensure security and expires after a predefined period.
SMS Delivery: The OTP API initiates the delivery of the generated OTP to the user's registered mobile number via SMS. MSG91, as a leading OTP service provider, ensures fast and reliable SMS delivery across various mobile networks.
User Verification: The user receives the OTP on their mobile device and enters it into the application or system. The application then verifies the entered OTP against the one generated by the OTP authentication API.
Authentication: If the entered OTP matches the generated OTP, the user is successfully authenticated, granting them access to the application or system. In a mismatch, the user is denied access, indicating a failed verification attempt.

- CUSTOMER (Login Process)

When the customer login to the system, the Account No. and Password sent to SMS is needed as notification to gain access to their dashboard but before proceeding the customer will undergo a challenge. The customer will login using the credentials and if validated successfully by the system, the SMS API will be triggered and send an One-Time Password (OTP) to the registered mobile number which is one layer of authentication to verify the individual customer with their unique Account No. With the format of (current year + random 6 digits number). When the customer input has missing or invalid the system will capture the error and display it that the password is wrong/incorrect or the account has not found which is the second layer authentication. This method can capture and hold the access of a certain customer and who also play as dummy that has intention to go in without the knowledge of the real customer. By this multi-layer authentication, the process of mere investigation will go series of challenge while the transaction will not be made successful due to the insufficiency of information provided with the system. The following are detailed steps on the customer login process:
Step 1: The customer requires to secure Account No. and Password sent over their mobile phone to gain access.
Step 2: By clicking the 'Account Login' button in the NPay Portal (referring to the mobile application), the system will automatically prompt a modal asking for the credentials.
Step 3: In the event that the customer has provided the needed credentials, by clicking 'Submit' button the system will analyze and validate the input and the authentication will determine if the credentials will pass to gain access.
Step 4: When the credentials are successfully validated and found correct. The system will be triggered to send an One-Time Password (OTP) to the customer.
Step 5: If the customer did not provide the correct credentials he/she will be stocked and expected not to enter their respective dashboard.
Step 6: If the OTP received to the customer's mobile phone, he/she will input it to the OTP verification screen provided by the system. If the customer input correct OTP same with the OTP sent to mobile. The system will redirect the customer to their dashboard. However, if contrary the system will redirect back the customer to repeat login process.
Step 7: Customer has login successfully.

- ADMIN (Login Process)

When the admin login to the system, the Email and Password is needed to gain access to their dashboard but before proceeding the admin will undergo a challenge. The admin will login using the credentials and if validated successfully by the system, the SMS API will be triggered and send an One-Time Password (OTP) to the registered mobile number which is one layer of authentication to verify the individual admin access with their unique Email and Password converted to md5 and sha1 hash. When the admin input has missing or invalid the system will capture the error and display it that the password is wrong/incorrect or the email is invalid which is the second layer authentication. This method can capture and hold the access of a certain admin and who also play as dummy that has intention to go in without the knowledge of the real admin. By this multi-layer authentication, the process of mere investigation will go series of challenge while the transaction will not be made successful due to the insufficiency of information provided with the system. The following are detailed steps on the customer login process:
Step 1: The admin requires to secure Email and Password over the login system on the back end of the system. Admin address is hidden and only admin know how to access it.
Step 2: By clicking accessing the hidden web address by admin, the system will automatically redirect the admin to login system of the system.
Step 3: In the event that the admin has provided the needed credentials, by clicking 'Submit' button the system will analyze and validate the input and the authentication will determine if the credentials will pass to gain access.
Step 4: When the credentials are successfully validated and found correct. The system will be triggered to send an One-Time Password (OTP) to the admin.
Step 5: If the admin did not provide the correct credentials he/she will be stocked and expected not to enter their respective dashboard.
Step 6: If the OTP received to the admin's mobile phone, he/she will input it to the OTP verification screen provided by the system. If the customer input correct OTP same with the OTP sent to mobile. The system will redirect the admin to their dashboard. However, if contrary the system will redirect back the admin to repeat login process.

Table 2: Technical Description of Attributes

Notation	Description
accountno	Customer Account Number
OTP	Time based One-Time Password
	password
Md5 and sha1	Encryption string for password
Email	Admin credential for login process
Password	String that converted into hash that will be used for login

Step 7: Admin has login successfully.

- Authentication Process

The authentication process has to capture the users activity to the system. The authorization service initiate validation and verification method from server data. The credentials submitted by both users are being analyzed through the multi-layer authentication as means of security and data control. When the information is valid, the system will grant access to information and users can manipulate their role over the system. Otherwise, when the authentication is invalid, access to the system will not be possible.
Step 1: The user input his credential information on the given logon screen
Step 2: The system will capture the submitted credentials and compare the information from the server.
Step 3: If the credentials is validated successfully. The system will automatically generate an One-Time Password (OTP) code from SMS API during the creation of account by admin, login of both admin/customers, forgot password recovery and bills payment.
Step 4: If the credentials in invalid. The system will be triggered off to different layer where if the user as admin which is expected to provide email and password, if the email is provided correctly but the password is incorrect. The system will display error informing the user "Password is Wrong/Incorrect". If the email is invalid, "Your Account Not Found". The user as customer is expected to provide Account No and Password. If Account No is invalid, the system will display error, "Your Account Not Found". If the password is invalid, the system will display error, "Your Password is Wrong/Incorrect".
Step 5: If the credentials are provided correctly with admin and customer, the authentication process will grant permission to access the respective dashboards.
Step 6: Authentication successful.

- Payment Process

The payment service will access the third party API using Paymongo. This third party platform will serve as payment gateway that will be triggered if bills payment has been processed. For this project, the integration of e-wallet is preferred to use for the method of payment. In such, the system will communicate via API and when customer details and bill information are validate through the API, the payment will be deducted from the e-wallet of the individual customer and the response will be retrieved in admin dashboard.
Step 1: The customer will access their personal dashboard using Account No and Password.
Step 2: The customer will view bill details by clicking Bill tab in the sidebar panel of the dashboard.
Step 3: When the customer accessed the bill tab, the bill details can be viewed in a table form and will notice bills payment status. If "Pay Now" button is visible in the action column, the customer must click the button to process the payment.
Step 4: After clicking the "Pay Now" button, the customer will be asked of the billing information as the Paymongo payment gateway will verify customer billing information.
Step 5: After completed to fill out the billing information form, the customer will be prompt to click "Proceed to Checkout" button after selecting GCash as method of payment to complete the transaction.
Step 6: After clicking "Proceed to Checkout" button, customer will be redirected to GCash gateway and will be asked for GCash registered mobile number and MPIN or will ask for fingerprint biometric to access GCash wallet.
Step 7: If GCash credentials are validated successfully, an OTP will be sent with the GCash registered mobile number for verification and when OTP is valid the specific amount will be deducted to the current GCash wallet. Payment is successful.

- Security:

Multi-Factor Authentication - Authentication and Verification
The new customer account created by admin will be prompt to add extra security layer using the integration of 'Security Question' as means of user authentication and security measures.
One-Time Password (OTP) - an authentication layer which is
expected to be triggered once request for verification was performed like after providing login credentials or related to payment process. This integration used API call request from third party provider which will be used in the coded syntax that will communicate that will serve as verifier of user authenticity when doing transactions in the system.
SMS Notification - is a messaging service which also uses API as means of point of contact between the code that will be triggered in the event that some transaction has made like new OTP was created due to login verification, new bill has been created with the link, payment confirmation and even the failed/canceled transactions related to payment.
Electronic Mail Service - is an existing way to perform an exchange of files and communication. This integration is known for this purpose, however, in this system this could be triggered also like SMS when new invoice has been created for the customers.
Tokens/Hash - Tokens are used to be a sensitive identifier, it is almost a combination of numbers, letters and symbol to create a unique id. In this development, it was used for session tracking and expiration, also with the payment link one-time use. The method is just simply use randomization or hashing algorithm that will be called 'authentication' through passwords and payment details.
Passphrase Strength Checker - Some of the sites do not have
this technology, where this integration will use some trick to css and javascript. However, this will support the authentication process where it will help the customers on how to create their passwords when they need to reset it. By these means, they can visualize how strong and weak the password they have created purposely to keep their personal profile authenticity.

3.4. Project tools

The tools that have been used to develop the NCTVN Billing and Online Payment Portal with Multi-layer Authentication using One-Time Password (OTP) are the following:

- PHP –is a scripting language, in addition to system functionality such as add, update, and delete modules.
- MySQL/MariaDB – relational database management system that is used to organize the records of the system.
- Bootstrap 5 Technology – primarily used for the user interface or form design and layout of the system.
- VSCode/Sublime – text editor used for coding, programming and debugging.
- XAMPP – offline package that consists of Apache, MySQL/MariaDB and PHP and for the offline setup as part of development startegy
- PayMongo Payment Solution API – online platform used for the payment module of the project.
- Semaphore - SMS API that is used for SMS Notifcation and OTP Verification
- Google Auth - use google authorization using ReCapthca service using version 2
- Exonhost - domain and hosting provider as cloud server where the system is configured and compiled to access it live.
- Tokenization/Hash - an innovative technology tool used in payment verification and session expiry.

4. Methodology

The information's collected and processed are discussed in this chapter. This is the method by which the system would be developed. The proponent makes use of historical data, interviews, public research, and other research methods in making the project. In this approach, it will describe the process of all the functionalities in the system from both customer and admin.

- Development Approach

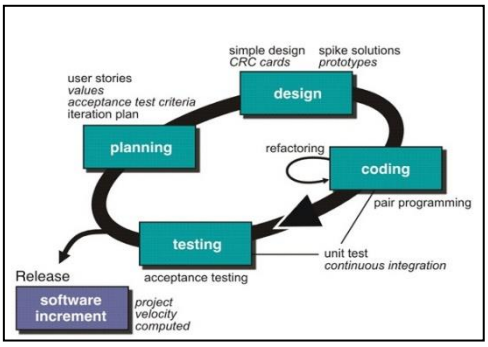


Fig. 5: System Development Approach.

Proponents choose an agile approach in developing the system. The proponent chooses a method that requires a process where the requirements cannot be fully predicted from the start but will always alter as projects go. Hence, proponents must use a methodology that is capable and can adapt to changing requirements at any stage in the project development life cycle.

The major focus of XP technique is the ability to accept changes that are unavoidable when creating projects. And that is what the proponents are looking for in the study conducted. It starts with planning and finishes with the final result, where the system is fully functional. Following the aspects of the XP technique appropriately helped the system's development. The following are the stages that proponents began to go through. Agile methods are the newest development approach, and attempt to develop a system incrementally by building a series of prototypes and constantly modifying them to user needs. Agile methods commonly employ a spiral model, which illustrates a series of iterations or updates depending on customer feedback. development strategy, people, tasks, timetables, and costs must be managed effectively using project management tools and techniques.

a) Planning Phase

The processed was provided by the NCTVN Cable Network Company – Technical Staff. The researcher conducted an interview and collected all the needed information regarding NCTVN business process. These data will be used in the study specifically to determine how customers will engage to the company in the availment of their services and how the company staff will attend to every usual transaction within the company. The area of coverage of NCTVN has reach nearby municipalities and main branch is situated in Kidapawan City. There are an approximate 9 municipalities covered by their services and an approximate 7253 total number of customers who availed their services. Ideally, the plan is to transform manual process to automated.

Context Flow Diagram

The proponents have presented the context flow process of the system where it described how data are handled and processed accordingly. This context flow will include the manual process and how to develop with the new proposed approach.

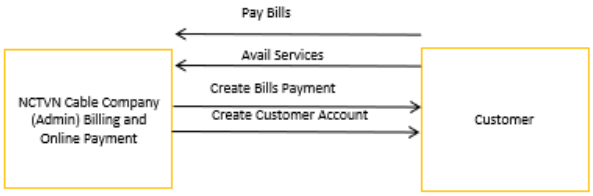


Fig. 6: Context Flow Diagram.

In this figure it shows the context flow diagram of how NCTVN and customer will engage through the process. In the implementation of this system, the proponents will consolidate all active customers who has availed their services and will manage through creating individual account upon availment of services and will create bill as payment for the service. As shown, it is relative that company will integrate payment system as part of business process

- Existing Process

Fig. 7: NCTVN Existing Process.

The figure above describes the existing process of NCTVN cable Network Company. The existing process of the company considered using manual process where their customers are expected to inquire regarding the services in their physical office or through social media as a third-party communication media. When a customer is interested to apply for a cable service, they have to choose what plan they want upon inquiry, then the encoder, which is the administrator of the system, will create an excel file with their own format in collecting the customer's information, then save the file to their local machine. On the other hand, the payment also will be billed manually where encoder will create it one-by-one and the company will hire collectors to deliver the said billing statement by area of assignment. During the payment process, the customer shall go to the office directly to secure their payment where they can receive their official receipt. When the bill-distributor/collector delivers their bill, the customer who received their billing can make payments with the bill-distributor/collector directly.

- Proposed Process

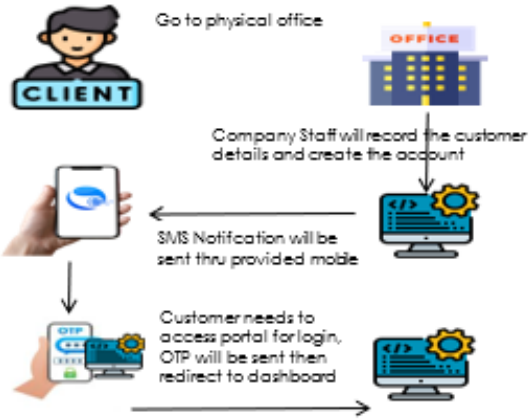


Fig. 8: Proposed Process.

In the figure 8. shows the proposed process for the new approach of the company where the manual process transforms into automated. In the figure, the customer will inquire for the services they want to avail but the encoder will save the information of the customer in cloud server using domain and hosting. After the customer's account was successfully created by the system administrator. The SMS notification will be sent to the provided contact number informing the customer that the account has successfully created with the unique account number and password. Also, thru SMS notification, the customer will be instructed where to access the online portal to login the given credentials. If the credentials are validated correctly, the SMS API will be triggered to send a One-Time Password as verification code that the customer has really had an account in the system. When OTP is provided correctly then the customer will be redirected to their individual dashboard. If credentials are not provided successfully, the system will display error of "Password is Wrong/Incorrect" or "Account Not Found". This layer is one the authentication method where customer will be validated and verified accordingly. Also, if OTP is wrong the system will be triggered to display an error like "OTP is Wrong". The chance to access the system dashboard is not possible if the user cannot provide the correct credentials, while another layer using the combination of hash strings conversion to password can prevent from security vulnerabilities.

- System Requirements Specification

In this stage, Proponents show how the user can engage with the system and vice versa at this point. This may comprise both functional and non-functional requirements.

- Functional Requirements

The functional requirements are the processes and activities that a system must be able to do. NCTVN Billing and Online Payment Portal integrated with multi-layer authentication using One-Time Password (OTP). These are the following that admin and customers can do:
Login Module - This module enables the website to determine whether the user is an authorized user.
Dashboard Module - This module permits the admin and customer to manipulate all the processes like managing customers, bill, helpdesk, tickets, and website settings with the privilege to edit, delete and update record information.
SMS API and Payment Gateway - This module will be Integrate to process the SMS Notification and Payment Gateway.
Forgot Password - This module allows the user as customer to change their password.

- Non-functional Requirements

Security: The NCTVN Billing and Online Payment
Portal integrated with multi-layer authentication using One-Time Password (OTP) use email and password (converted into hash) for admin login and use Account No (combination of current year + 6 digits random numbers) and password (combination of md5 and sha1) for customers. This security is layered through the use of API and firewall to secure attacks and illegal cyber activities.
Usability and NCTVN Billing and Online Pay
Compatibility ment Portal integrated with multi-layer authentication using One-Time Password (OTP) can be access by system administrator through desktop computers as long as it is connected to network or mobile and handheld devices. For customers, they are prompt to download NPay App for ease of mobile application use. The system itself is very understandable and predictable, hence, the develop functionalities are easy to handle.
Availability: The system's availability is primarily de
pendent on internet access, to fully access and
experience system usability. In fact, that the system is securely hosted in the cloud server.
Accessibility: The ability of the system in terms of perfor and
Runtime: ance in processing functionalities and specific
Performance: function where user has the correct infomation and workflow process in accessing the system features.

b) Design Phase

After planning, the proponent define and describe what features are best to add in the development of the system. By considering the idea and the practices which is need to transform for a new approach, the system was designed according to the specific user where in customer

- the viewing of bill, transaction history, creation of ticket and account profile were designed specifically for customers and grant privilege that can update an account and change password recovery. For admin, all privileges has granted with data to manage customer records, manage bills, post announcement, manage tickets, and adding data like plan type, advisory category and area of coverage. This development was designed through bootstrapping as template and PHP as language for development.

- System Design

In this stage, the proponent provides the system design, including architectures, modules, and interfaces where the process is described, at this phase. The proponent also exhibit their System Flowchart, Use Case Diagram, and Infrastructure. Below are the processes where proponents defined the development of the system.

- System Flowchart

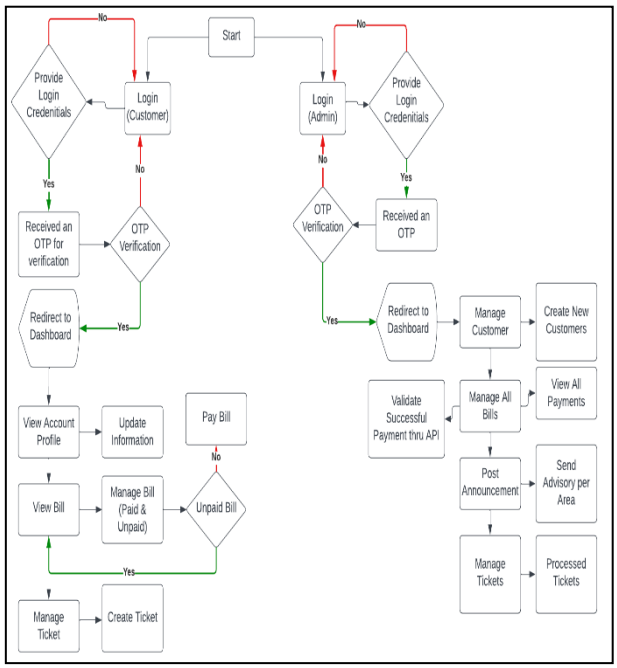


Fig. 9: System Flow Diagram.

In Figure 9 shows the proponent's System Flow for their system. The first requirements in gaining access is to provide login credentials where for customers are need to provide Account No and Password while the admin will provide email and password. In the admin side which has all the privileges to use and manipulate all the features, once the login is validated correctly it will be redirected to OTP verification which is the authentication layer for verification of identity which is the main purpose of the integration of the Billing and Online Payment Portal for NCTVN. Once OTP is verified, the system will automatically redirect the admin to their dashboard. Referring to the system flow, the admin can manage all the customer records that can update and even delete a customer's record if necessary, also can manage all bills while checking which bill has not yet paid, on due date, has successfully paid and can create bill to all or individually.

Hence, there is also a feature to create and post advisory to customer's per area if there were to announced scheduled service interruption, also can manage all tickets as to support to customers of their concerns and can manipulate the site data by putting data to corresponding settings. In customers, which will interact as the buyer of the services, the main transaction would be the payment transaction. NPay App is developed intended only to track bill and pay their bills in the essence to experience ease of access and availability of the business process. In the flow, customers can only view bill and pay the unpaid bill, update their information, can track transaction history and create ticket for their issues and concerns.

In recurring process, where the figure above describes how the will interact or give instructions prior to the authentication process initiated. In both customer and admin login, invalid credentials will always redirect the user to the first process which to provide credentials for each login process. Unsuccessful transaction can hold user activity by not possibly gain access and use the system services.

- Use Case Diagram

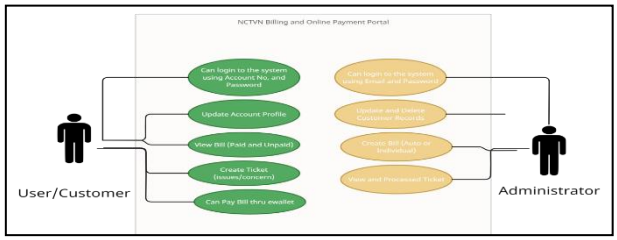


Fig. 10: Use Case Diagram.

In figure 10 is the use case diagram of the system which shows the interactions between the Admin and the Customer where admin has the full privileges to update, delete and add data to the back end while customer has limited interaction in the use of the system. In this diagram, login process is a prerequisite before can perform transaction inside each individual dashboard.

By the integration of the multi-layer factor authentication, it will maintain the system security and data control where the system involves with personal information and financial aspect. This SMS API and Payment Gateway integration can really secure the process and coincide to the main purpose and objective in developing this process for the proponent.

- System Infrastructure

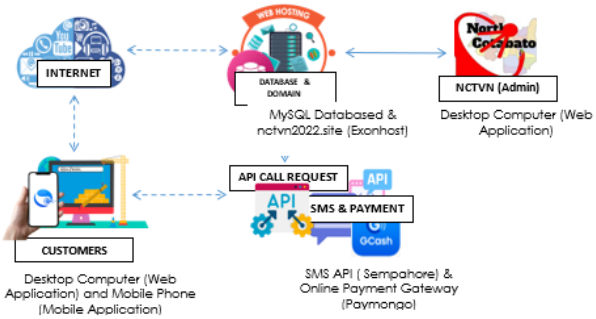


Fig. 11: System Infrastructure.

In figure 11. Shows the system infrastructure for hardware, software, networks and facilities upon which the system services are built. As per infrastructure setup, internet has the important role in the structure where it provides access to the system processes and functionalities. The direct interaction or use of the users (referring to admin and customer) of the system is possible through the internet service. The use of API integrates specifically for the payment gateway and SMS notification features. The customers can access the application through the use of mobile while system admin has to manage all privileges over web application.

c) Coding Phase

The system development has utilized the use of PHP programming language as the main tool for this development. PHP is used bootstrap technology as template foundation and structure. As to the objective of this project, the proponent targeted to create a system that vigorously generated pages fast and easily in which the proponent's find it very helpful. In customers experience, the developer has integrated GoNative platform which approach is to develop the online payment portal as direct interface for customers. In which, the web and mobile development has achieved.

d) Testing Phase

Testing phase was one of the important procedures in the system development cycle in which the entire functionalities can be tested and determine common errors before publish it to live server and to determine whether objectives are being met. The researchers conduct a quality assurance and testing between new users and the proponents to test if the system has intervened with the solutions with regards of the system. As part of testing strategy, the researcher invited some of the technical staff from NCTVN who usually engage or use the system and check every features functionality. There are three testing phases: In the first testing phase, the system developed by the proponent was tested by NCTVN's admin, who discovered that the OTP code that was supposed to be transmitted to the user's registered phone for identity verification wasn't received. The log-in process was repeated as it wasn't received the first time. The tester suggested that, in order to avoid prolonged waiting, the system should offer a resend option for OTP. Additionally, a redundant button was noticed on the electronic receipt. After making the payment, the user will receive an invoice through email. Consequently, the PAY NOW button is still visible and present on the received email invoice even after the monthly amount paid has been paid and it was suggested to remove the PAY button. To proceed in the 2nd phase of testing, the proponents assured to apply the suggestions gathered from the NCTVN staffs and it was successfully added on the system.

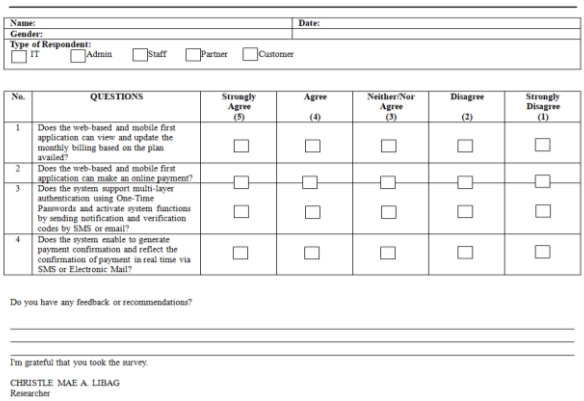
The system created by the proponent was tested in the second phase of testing by the proponent's advisor. After testing, it was discovered that the system's temporary password, which was issued after the registration procedure, can be used until the user remembered to change it, and they may purposely visit and update their password in their account profile in the menu bar. As a result of outdated changing of password, it is not safe for the customer's account. As suggested, upon log-in using the temporary password, there should be a prompt message asking to change password immediately after successfully log-in. In addition, Billing statement, transaction history and ticket list can be viewed or downloaded from dashboard in pdf form. During testing, the researcher will take note all of the suggestions and recommendations of the proponents for improvement and debugging. The simulation will give weigh to which functionality also will be removed or to add. All the suggestions were adopted and it was successfully added on the system.

For the last phase, as the system's billing, payment and security algorithm and other suggestions applied from the other phase. The proponent proceeded to the third phase of testing for the finalization of the testing. Some of NCTVN subscribers was selected to test the said system and for collecting of data. The method of collecting data is questionnaire method since questionnaire is also a practical way to gather data and it is the best way to get results and it covers every aspect of topic.

Approach like Cluster Sampling is used to avoid expensive cost and time constrain. In the used of sampling approach the researcher divided the sampling area into a small concentrations or clusters of sampling units [9].

- Evaluation Instrument:

Below are some of the snapshots of the testing criteria:



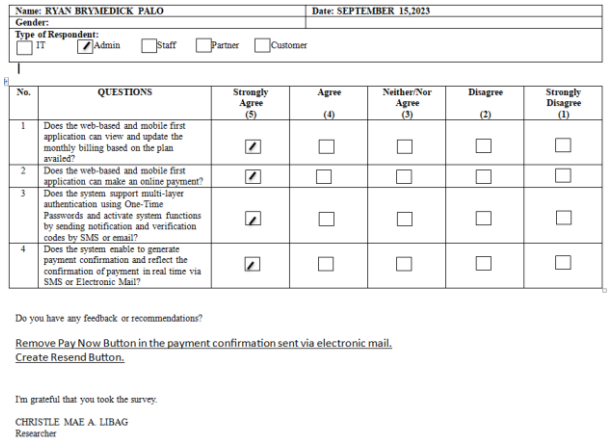
Name:	Date:
Gender:	
Type of Respondent: ☐ IT ☐ Admin ☐ Staff ☐ Partner ☐ Customer	

No.	QUESTIONS	Strongly Agree (5)	Agree (4)	Neither/Nor Agree (3)	Disagree (2)	Strongly Disagree (1)
1	Does the web-based and mobile first application can view and update the monthly billing based on the plan availed?	☐	☐	☐	☐	☐
2	Does the web-based and mobile first application can make an online payment?	☐	☐	☐	☐	☐
3	Does the system support multi-layer authentication using One-Time Passwords and activate system functions by sending notification and verification codes by SMS or email?	☐	☐	☐	☐	☐
4	Does the system enable to generate payment confirmation and reflect the confirmation of payment in real time via SMS or Electronic Mail?	☐	☐	☐	☐	☐

Do you have any feedback or recommendations?

I'm grateful that you took the survey.

CHRISTLE MAE A. LIBAG
Researcher



Name: RYAN BRYMEDICK PALO	Date: SEPTEMBER 15,2023
Gender:	
Type of Respondent: ☐ IT ☑ Admin ☐ Staff ☐ Partner ☐ Customer	

No.	QUESTIONS	Strongly Agree (5)	Agree (4)	Neither/Nor Agree (3)	Disagree (2)	Strongly Disagree (1)
1	Does the web-based and mobile first application can view and update the monthly billing based on the plan availed?	☑	☐	☐	☐	☐
2	Does the web-based and mobile first application can make an online payment?	☑	☐	☐	☐	☐
3	Does the system support multi-layer authentication using One-Time Passwords and activate system functions by sending notification and verification codes by SMS or email?	☑	☐	☐	☐	☐
4	Does the system enable to generate payment confirmation and reflect the confirmation of payment in real time via SMS or Electronic Mail?	☑	☐	☐	☐	☐

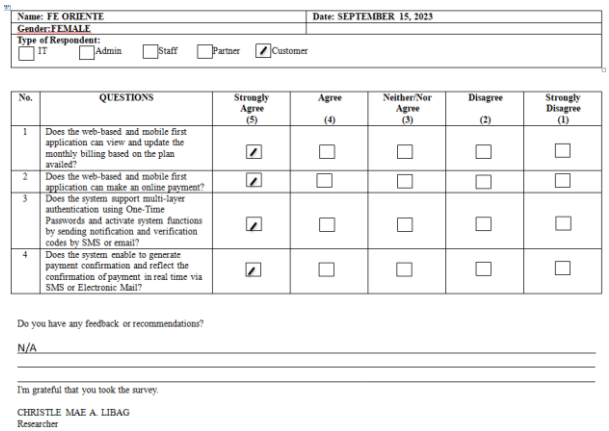
Do you have any feedback or recommendations?

Remove Pay Now Button in the payment confirmation sent via electronic mail.
Create Resend Button.

I'm grateful that you took the survey.

CHRISTLE MAE A. LIBAG
Researcher

Fig. 12: Web Testing NCTVN Admin.



Name: FE ORIENTE	Date: SEPTEMBER 15, 2023
Gender:FEMALE	
Type of Respondent: ☐ IT ☐ Admin ☐ Staff ☐ Partner ☑ Customer	

No.	QUESTIONS	Strongly Agree (5)	Agree (4)	Neither/Nor Agree (3)	Disagree (2)	Strongly Disagree (1)
1	Does the web-based and mobile first application can view and update the monthly billing based on the plan availed?	☑	☐	☐	☐	☐
2	Does the web-based and mobile first application can make an online payment?	☑	☐	☐	☐	☐
3	Does the system support multi-layer authentication using One-Time Passwords and activate system functions by sending notification and verification codes by SMS or email?	☑	☐	☐	☐	☐
4	Does the system enable to generate payment confirmation and reflect the confirmation of payment in real time via SMS or Electronic Mail?	☑	☐	☐	☐	☐

Do you have any feedback or recommendations?

N/A

I'm grateful that you took the survey.

CHRISTLE MAE A. LIBAG
Researcher

Fig. 13: Mobile Testing NCTVN Customer.

In this study, the Regular customers of NCTVN, currently active consumer and a male and female participant ages 18 to 60 years old of the 8 municipalities of North Cotabato are the target respondents. In this study the number of all the subscriber of NCTVN has approximately 7253 subscribers and the researcher get at least 250 respondents (subscribers) in all areas covered by NCTVN Services. This sample has a 90% percent confidence level with a value of z-score of 1.65, and ±5% percent margin of error. To get the number of respondents this formula is used:

$$\frac{\frac{z^2 \times p(1-p)}{e^2}}{1+\left(\frac{z^2 \times p(1-p)}{e^2 N}\right)}$$

Somehow, there are some failed results experienced by the customers upon testing specially in receiving the notification and paying online due to the internet and cellular signal. But, this result was easily resolved by finding a place where signal is strong and can support the accomplishment of the payment process and successfully receiving the notification.

Meanwhile, a person that is not an active consumer or not a consumer of NCTVN is barred from participating. Respondent who feel awkward or hesitate to answering the survey questionnaire have the option of withdrawing from participation. Their decision not to participate is considered.

- User Acceptance Testing

In this test, the users had given the opportunity to interact with the system and the evaluation sheet use to validate the functions and characteristics of the developed system. The researcher visited the NCTVN office and conducted a testing with the NCTVN personnel, and customers in different areas covered by the services of NCTVN. Testing was done with the actual users or clients of the application and the main goal of testing is to check if system objectives was meet. After collecting the data, the results were analyzed using a Weighted Mean. Lickert Scale was used to determine the average responses for each item. Given the 1-5 options. (5) Strongly Agree, (4) Agree, (3) Neither/Nor Agree (2)Disagree, and (1) Strongly Disagree. In interpreting the weighted mean, the following scale was used: Strongly Agree (4.51-5.00), Agree (3.51-4.50), Agree (2.51-3.50), Fair (1.51-2.50), and Disagree (1.50 and below).

Two Hundred Fifty (250) subscribers of NCTVN were selected as respondents. There are four (4) items in the test questionnaire. Item(1) has a weighted mean of 4.95 under Strongly Agree, which means that the system proposed allowed the user to view and update the monthly billing base on the plan availed of the subscriber. Item (2) has a weighted mean of 4.92 under Strongly Agree, It indicates that users of the web-based and mobile-first application can pay online and have the confirmation of their payment reflected in real-time as long as they have an active internet or mobile service connection. Item (3) has a weighted mean of 4.95 under Strongly Agree, which refers to the test case to confirm the credentials of the registered users using integrated multi-layer authentication and the usage of a One-Time Password (OTP), in which the subscribers accept and agree effectiveness of the security with their payment and account information. Lastly, the item (4) has a weighted mean 4.91 under Strongly Agree, which means the system proposed Enables the subscribers successfully received the system generate payment confirmation via SMS or Electronic Mail and notify them by their billing statement electronically.

Question	Strongly Agree (5)	Agree (4)	Neither/ Nor Agree (3)	Disagree (2)	Strongly Disagree (1)	Result	Remarks
1	238*5=1190	12*4=48				(1190+48)/250 **=4.95**	**Strongly Agree**
2	233*5=1165	13*4=52	4*3=12			(1165+52+12)/250 **=4.92**	**Strongly Agree**
3	241*5=1205	5*4=20	4*3=12			(1205+20+12)/250 **=4.95**	**Strongly Agree**
4	236*5=1180	6*4=24	8*3=24			(1180+24+24)/250 **=4.91**	**Strongly Agree**

Table 3: Matrix of Test Result

Statistic	Description
N	Population Size
e	Margin of Error (as a decimal)
z	Confidence Level (as a z-score)
p	Percentage Value (as a decimal)

e) Implementation

Based on the series of tests of the system, the objectives of the project have been achieved, and it is ready for the implementation of the Billing and Online Payment Portal with Multilayer Authentication Using One-Time Password for NCTVN Cable Network in four (4) stages. (1) User/s. Prior to the full implementation of the system, the NCTVN Cable Network management should consider the needs of assigning personnel to manage the system within the company who are ready to be trained. (2) Installation. In this stage, the goal is to prepare all the necessary tools, hardware, and software for the installation and configuration of the system at the head end of the NCTVN Cable Network. The assigned personnel will assist during the installation process. (3) Exploration. The proponent will conduct an orientation for the assigned personnel with regards to the full operation of the system. It is also essential for them to be aware of how the NCTVN Cable Network clients will utilize the system. (4) Implementation. The primary goal of this phase is to fully implement the Billing and Online Payment Portal with Multilayer Authentication Using One-Time Password for the NCTVN Cable Network, improve, and streamline the billing and online payment collection services. In addition, the researchers and the NCTVN Cable Network will discuss the full implementation of the said system and launch to public users and target users as well.

5. Results and discussion

The findings revealed that the app was fully functional and had well-designed functionalities.

The following results were reached in accordance with the objectives. The customers who choose to use the NCTVN Billing and online payment portal with multi-factor authentication using one-time password can register and access their account using the web-based and mobile first application to view and update their monthly billing base on the plan availed once it was reflected on the system. These results are evidence that the NCTVN Company will have an opportunity to lessen the cost covered for their man power where the company can reduce number of workforces.

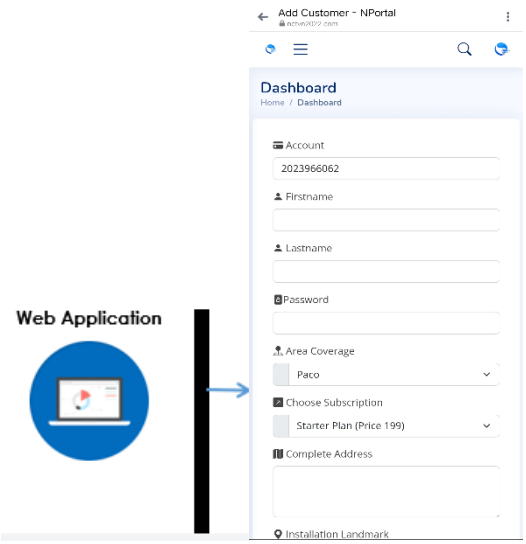


Fig. 14: Registration from Admin Site.

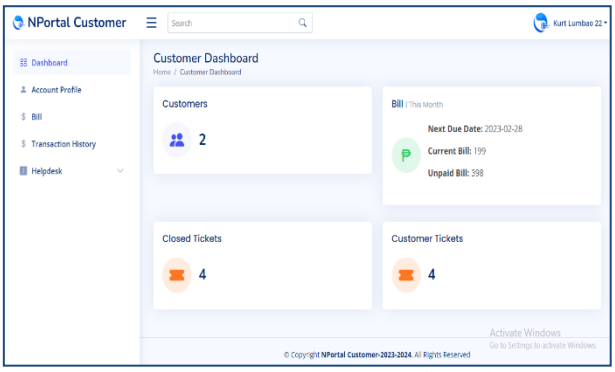


Fig. 15: Accessing Customer's Account Using Web-Based.

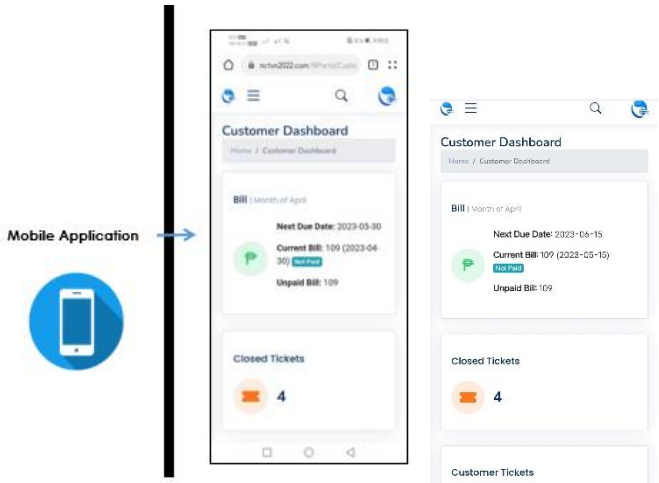


Fig. 16: Accessing Customer's Account Using Mobile Application.

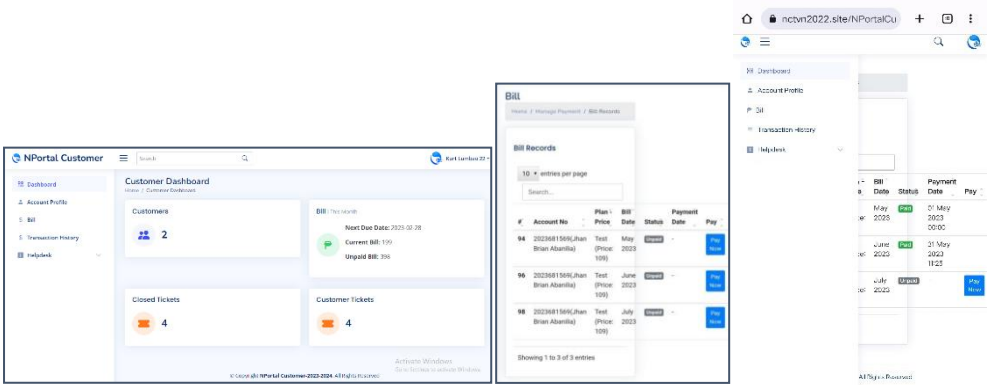


Fig. 17: View And Update Their Monthly Billing Rate.

Using the NCTVN Billing and online payment portal with multi-factor authentication using one-time password the customer can access the system through web-based and mobile first application to create payment online. It shows that this system offers a better solution to the consumers' issue of making payments on-site and over the counter in order to secure the payment obligation. By this process, the admin will no longer need to accommodate a large number of clients who wants to pay their bill over-the-counter. The clients can also save money on their transportation for they can now pay via the NPay App.

Fig. 18: Create Payment Using Web and Mobile Application.

The customers are confident in using the NCTVN Billing And online payment portal by integrating multi-factor authentication using One Time Password to the system. The customers testing results proves that the multi-factor enable system processes through sending of notification and verification be prompt to add extra security layer using the integration of 'Security Question' as means of user authentication and security measures,

One time password (OTP) API call request from third party provider which will be used in the coded syntax that will communicate that will serve as verifier of user authenticity when doing transactions in the system through SMS or electronic email, providing an unique and Log-in account from the admin system, and a tokenization was added as sensitive identifier and was used for session tracking and expiration, also with the payment link one-time use.

From the entire multi-factor authentication mentioned above the customer can guarantee that the data collection, billing features and online payment is protected as they test the system. The integration of multi factor authentication in the system will cover up the worries of both customer and admin. It will lessen the risk of untrusted actions from some of the collectors not only by the said company but also to the other company that has the same manual collection process.

Lastly, using the system it enables the system to generate payment confirmation via SMS or Electronic Mail and as a result, it was confirmed that every payment made by the customer there is a reflected confirmation of payment in real time via SMS or Email. Through this process the customer can check anytime and updated directly every payment made.

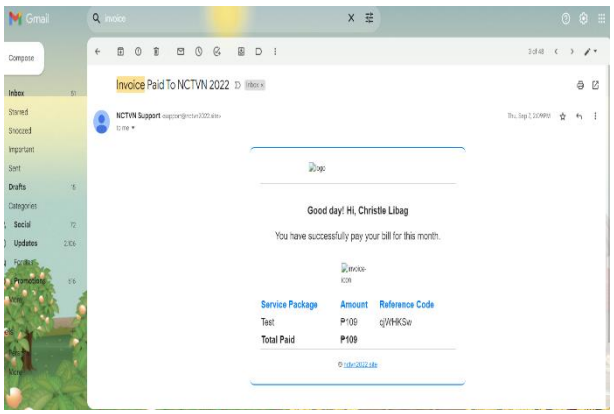


Fig. 19: Reflect the Confirmation of Payment Via E-Mail.

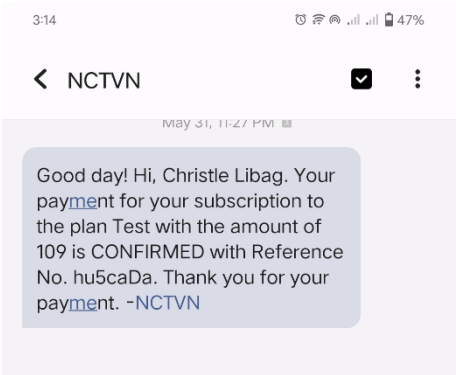


Fig. 20: Reflect the Confirmation of Payment Via SMS.

6. Conclusion and recommendation

6.1. Conclusion

Based on the outcome analysis, the design and development of the billing and online payment portal with multifactor authentication through the use of time based on a one-time password for NCTVN Cable Network in Kidapawan City were completely developed and fully operational. The web-based and mobile-first application that will allow the user to view and update their monthly billing based on the plan they availed of was fully developed and functional. The development of a web-based and mobile-first application that can make online payments integrated with a multi-layer using a one-time password with system-enabled processes by sending notification and verification codes through SMS or electronic mail is fully functional. It was ensured that the data collection, billing features, and online payment were protected. The system was also enabled to generate payment confirmations via SMS or electronic mail.

6.2. Recommendation

Based on the results of this study, the researcher recommends additional features in the system for future use and upgrading. First, develop a system function that can filter the payment once there are three (3) consecutive unpaid bill reflected in their billing statement and provide a Disconnection letter. Second, to further developed the system in terms of interface, content, behavior and algorithm to give the best user experience. And lastly, for a full admin system process, connect the developed system to the existing billing and payment system of the NCTVN Company to provide a factual report, and proper formatting of document report including the signatories.

Acknowledgement

In all your ways I acknowledge you Oh! Lord for all the wisdom, strength, and knowledge in exploring things, to surpass all the trials and giving determination to pursue my study and make my study possible.
I would like to express my deepest gratitude and warmest appreciation to the following people, who, in any way have contributed and inspired me to the overall success of my educational journey.
To my family, and especially to my partner Paul P. Libag, MIT. Without all of you I will not dream for these. But you inspired me to dream high and achieve more. Thank you for showing me your support in all means. Thank you for encouraging me when I feel down, stress, and struggled in my study.

References

[1] Christoph Ungerer, Alberto Portugal, Martin Molinuevo and Natasha Rovo. (May 2020) Recommendations To Leverage E-Commerce During The Covid-19 Crisis. https://doi.org/10.1596/33750.
[2] Hamed Taherdoost (September 2023) Billing and Payment Systems https://doi.org/10.1007/978-3-031-39626-7_6.
[3] Hendricks, Mwapwele,2023. A systematic literature review on the factors influencing e-commerce adoption in developing countries. https://doi.org/10.1016/j.dim.2023.100045.
[4] Pandey and Pal, 2020. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International Journal of Information Management, 55 (2020), Article 102171 https://doi.org/10.1016/j.ijinfomgt.2020.102171.
[5] S. Alabi, M. White, N. Beloff, 2020. Contactless palm vein authentication security technique for better adoption of e-commerce in developing countries. Science and Information Conference, Springer, Cham pp. 380-390 https://doi.org/10.1007/978-3-030-52243-8_27.
[6] Wadhawan, N., & Arya, R.K., 2020. Understanding e-commerce: A Study with reference to competitive economy.
[7] Cedillo, Garcia, Cardenas and Berme, 2018. A Systematic Literature Review of Electronic Invoicing, Platforms, and Notification Systems. International Conference on eDemocracy and eGovernment. https://doi.org/10.1109/ICEDEG.2018.8372338.
[8] MA, Siqi; FENG, Runhan; LI, Juanru; LIU, Yang; NEPAL, Surya; BERTINO, Elisa; DENG, Robert H.; MA, Zhuo; and JHA, Sanjay, 2019. An empirical study of SMS one-time password authentication in Android apps. (2019). In *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019). 339-354. Research Collection School of Information Systems.* https://doi.org/10.1145/3359789.3359828.
[9] Lauren Thomas. 2020. Cluster Sampling
[10] Preeti Chandrakar & Hari Om, 2017. A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. https://doi.org/10.1016/j.comcom.2017.05.009.
[11] Barkadehi, Ogbanufe & Kim, 2018. Comparing fingerprint -based biometrics authentication versus traditional authentication methods for e-payment. https://doi.org/10.1016/j.dss.2017.11.003.
[12] Chandrakar and Om, 2017. *An efficient two-factor remote user authentication and session key agreement scheme using Rabin Cryptosystem., Redirecting*. Available at: https://doi.org/10.1016/j.dss.2017.11.003.
[13] Muhammad Arif Hussin1, Mohd Fadzil Abdul Kadir2, Siti Aswani Mohd Ghazali3, Shariful Hafizi Md Hanafiah4, Aznida Hayati Zakaria, October 2020. The Effectiveness of Web System and Mobile Applications for their end-users. International Journal of Engineering Trends and Technology. https://doi.org/10.14445/22315381/CATI3P224.
[14] MA, Siqi; FENG, Runhan; LI, Juanru; LIU, Yang; NEPAL, Surya; BERTINO, Elisa; DENG, Robert H.; MA, Zhuo; and JHA, Sanjay. An empirical study of SMS one-time password authentication in Android apps. (2019). *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019). 339-354. Research Collection School of Information Systems. Available at: https://ink.library.smu.edu.sg/sis_research/4628* https://doi.org/10.1145/3359789.3359828.
[15] Bee Bee Chua and Laurel Evelyn Dyson. the ISO 9126 model to the evaluation of an elearning system. Faculty of Information Technology. University of Technology, Sydney, AUSTRALIA
[16] UNNIMAYA PRAKASAN (Reg No. SM21COM017) (March,2023) A STUDY ON IMPACT OF ONLINE PAYMENT APPLICATIONS AMONG YOUNGSTERS WITH REFERENCE TO GOOGLE PAY.
[17] CHEANG XIN, YI LIM, JAS MIN, NG KHA, YONG THOR, MIN HUI. (May 2023) ONLINE PAYMENT SCAM: WHAT HAVE CAUSED IT?
[18] Chris Stefanadis (August 2002) Vol 8. No. 7. Why Hasn't Electronic Bill Presentment and Payment Taken Off?
[19] Bills, Steve. 2002. "Will MasterCard Speed Past EBPP's Snails?" American Banker 167, January 24, p. 1.
[20] Janmaya Kumar Mishra, Midhunchakkaravarthy Janarthanan. 2022. Volume 60, Part 2, Pages 939-944 https://doi.org/10.1016/j.matpr.2021.11.077.
[21] Deonesio G. Tico.2016.Development of School Portal System with SMS Notification for Sultan Kudarat State University Kalamansig Campus.