NEO BANKING USING CONTAINERIZED APPLICATION

Submitted by

MOHAMMED ARISH RAHUMAN A	**(714017104049)**
NITHEESH N	**(714017104060)**
FAYAZ AHAMED D	**(714017104030)**

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

SRI SHAKTHI INSTITUTE OF ENGINEERING

AND TECHNOLOGY (AUTONOMOUS),

COIMBATORE 641 062

Autonomous Institution,

Accredited by NAAC with “A” Grade

MAY 2021

BONAFIDE CERTIFICATE

Certified that this Report titled **“NEO BANKING USING CONTAINERIZED APPLICATION”** is the bonafide work of **“MOHAMMED ARISH RAHUMAN.B (714017104049), NITHEESH.N(714017104060) AND FAYAZ AHAMED.D (714017104030)”,** who carried out the work under my supervision. Certified further that to the best of my knowledge the work reported herein does not from part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE	**SIGNATURE**
Dr.K.E.Kannammal	Mrs.N.Saranya
HEAD OF THE DEPARTMENT	**SUPERVISOR**
Professor and Head,	Assistant Professor,
Department of CSE,	Department of CSE,
Sri Shakthi Institute of Engineering	Sri Shakthi Institute of Engineering
and Technology,	and Technology,
Coimbatore- 641 062.	Coimbatore- 641 062.

Submitted for the project work viva voce Examination held on…………….

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We express our deepest gratitude to our **Chairman Dr.S.Thangavelu** for his continuous encouragement and support throughout our course of study.

We are thankful to our **Secretary Er.T.Dheepan** for his unwavering support during the entire course of this project work.

We are also thankful to our **Joint Secretary Mr.T.Sheelan** for his support during the entire course of this project work.

We are very grateful to our **Principal Dr.A.R.Ravi Kumar** for his magnanimity in allowing us to avail the facilities in the department.

We are deeply indebted to our **Head of the Department,** Computer Science and Engineering, **Dr.K.E.Kannammal,** for providing us with the necessary facilities.

It's a great pleasure to thank our **Project Guide Mr.E.Subramanian,** for her valuable technical suggestions and continuous guidance throughout this project work.

We are also thankful to our **Project Coordinator Mrs.M.Ambika** Assistant Professor, **Mr.R.Venkatesh** Assistant Professor of Computer Science and Engineering, for providing us with necessary facilities and encouragement.

We solemnly extend our thanks to all the teachers and non-teaching staff of our department, family and friends for their valuable support.

MOHAMMED ARISH RAHUMAN B
NITHEESH N
FAYAZ AHAMED D

ABSTRACT

The objective of the system is to find whether the Transaction in Cloud is a genuine one or not. This is done by authenticating the web application by using a EC2 Server on Amazon Web Service, which can be obtained by implemented by WebSocket using API. After authenticating the web application, the authorized users will be allowed to access the application to get various services and provide information that includes transactions and with different kind of the users in a role-based web application. Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and deploy it as one package. So, the application runs quickly and reliably from one computing environment to another. Amazon EC2 provides resizable, secure compute capacity in the cloud via a VM and elastic web-scale computing so you or your developers can build failure-resistant apps in the cloud. Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. The system will check the user's existence in the database and provide the set of services with respect to the role of the user. The application is based on two-tier architecture. The EC2 will help to find the fraud application and business logic helps in authenticating the application, authorizing the users and providing services. The technologies are chosen by keeping the compatibility and performance as the constraints for the application

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AWS	Amazon Web Services
EC2	Elastic Cloud Computing
API	Application programming Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
UI	User Interface
UX	User Experience
DB	Data Base
TCP	Transmission Control Protocol
IP	Internet Protocol
WAP	Wireless Application Protocol
WAE	Wireless Application Environment
WTP	Wireless Transaction Protocol
WLTS	Wireless Transport Layer Security
RAM	Random Access Memory
RBI	Reserve Bank of India
PIN	Personal Identification Number

NEFT	National Electronic Funds Transfer
QR	Quick Response
GHz	Giga Hertz
AI	Artificial Intelligence
WHO	World Health Organization
ID3	Iterative Dichotomized 3
IDE	Integrated Development Environment
LINUX	Lovable Intellect Not Using XP
NA	Not Available
NB	Naive Bayes
OS	Operating System

CHAPTER 1

INTRODUCTION

Neo banks are challenging the universal banking model through a low-cost structure, feature-rich products/services and easy accessibility. Their Innovation engine focuses on three key pillars of Customer experience, User convenience and Simplified processes. Platform-centric models via open banking and APIs is also enabling Neo banks to expand user base, growing commission income and in offering increased potential for data monetization. The Neo & Challenger banks have a strong cost efficiency driven by less complex IT systems, simpler product set, lower real estate and distribution costs and more streamlined operating models. Demand-pull for Neo & Challenger Banks is rooted in their ability to offer a faster and transparent model, lower fees, superior CX and a goaloriented business aimed at improving household financial wellness. Neo & Challenger Banks are redesigning their business models around customer-centricity, for significant user growth. A few of them such as Chime, Revolut, N26 and Compte-Nickel have acquired a million-plus user base with total transactions value running into $4-$18 Bn. The Digital Banks are also leading on customer satisfaction metrics. US Digital Banks' customers are 83% satisfied as against 76% satisfaction rate for UK customers. In both the markets, customers report the lowest satisfaction with Top 50 Global banks.

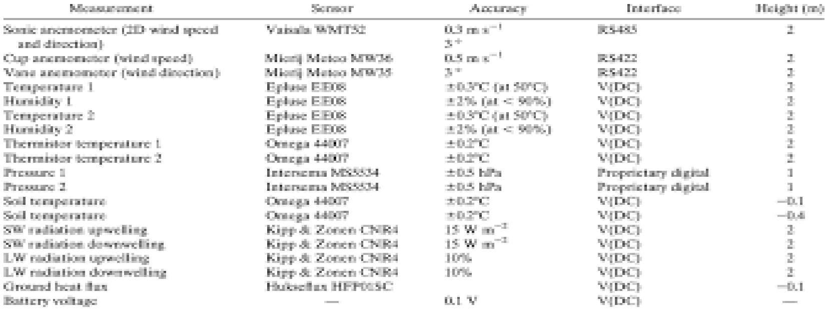
Neo Banking' has become a buzzword in 2020. Neo Banks are digital banks that operate purely online with no physical branch. Given the intensive expenses associated with setting up physical banks, especially in remote locations, digital banks are a much more cost-effective and scalable option. The need becomes even greater in a pandemic-ridden, socially distanced world that we live in today.

Globally, the neo banking model has seen a rise in uptake. Countries outside India have independent, virtual banks exclusively offering digital services. In India however, the model has been different given the Reserve Bank of India (RBI) presently does not allow pure-play digital banks to operate yet. Indian Neo Banks like NiYO, RazorPayX, Instant Pay etc., collaborate with traditional banks and support them with customer acquisition as well as new-age digital services. Owing to regulatory compliance, Neo Banks in India are expected to become mainstream in the next 2-3 years. In the meanwhile, the country will see the rise of a Hybrid banking model, which will become the norm.

In India ICICI bank has put some of its application on Microsoft Azure. The reason why Banks where not using cloud earlier was since Banks has some compliance policy regarding data security and confidentiality and now most of the big cloud providers are following those compliances so slowly banks are opening up towards public cloud. Hopefully in this year we will see other banks moving some of their workloads to public cloud.

1.1 AMAZON WEB SERVICES

Amazon Web Services (AWS) is a subsidiary of Amazon providing on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis. These cloud computing web services provide a variety of basic abstract technical infrastructure and distributed computing building blocks and tools. One of these services is Amazon Elastic Compute Cloud (EC2), which allows users to have at their disposal a virtual cluster of computers, available all the time, through the Internet. AWS's version of virtual computers emulates most of the attributes of a real computer, including hardware central processing units (CPUs) and graphics processing units (GPUs) for processing; local/RAM memory; hard-disk/SSD storage; a choice of operating systems; networking; and pre-loaded application software such as web servers, databases, and customer relationship management (CRM). The AWS technology is implemented at server farms throughout the world, and maintained by the Amazon subsidiary. Fees are based on a combination of usage (known as a "Pay-as-you-go" model), hardware, operating system, software, or networking features chosen by the subscriber required availability, redundancy, security, and service options. Subscribers can pay for a single virtual AWS computer, a dedicated physical computer, or clusters of either. As part of the subscription agreement, Amazon provides security for subscribers' systems. AWS operates from many global geographical regions including 6 in North America. Amazon markets AWS to subscribers as a way of obtaining large scale computing capacity more quickly and cheaply than building an actual physical server farm. All services are billed based on usage, but each service measures usage in varying ways. As of 2017, AWS owns a dominant 33% of all cloud (IaaS, PaaS) while the next two competitors Microsoft and Google have 18%, 9% respectively according to Synergy Group.



Measurement	Sensor	Accuracy	Interface	Height (m)
Sonic anemometer (2D wind speed and direction)	Vaisala WMT52	$0.3\ m\ s^{-1}$ 3°	RS485	2
Cup anemometer (wind speed)	Mierij Meteo MW36	$0.5\ m\ s^{-1}$	RS422	2
Vane anemometer (wind direction)	Mierij Meteo MW35	3°	RS422	2
Temperature 1	Epluse EE08	±0.3°C (at 50°C)	V(DC)	2
Humidity 1	Epluse EE08	±2% (at < 90%)	V(DC)	2
Temperature 2	Epluse EE08	±0.3°C (at 50°C)	V(DC)	2
Humidity 2	Epluse EE08	±2% (at < 90%)	V(DC)	2
Thermistor temperature 1	Omega 44007	±0.2°C	V(DC)	2
Thermistor temperature 2	Omega 44007	±0.2°C	V(DC)	2
Pressure 1	Intersema MS5534	±0.5 hPa	Proprietary digital	1
Pressure 2	Intersema MS5534	±0.5 hPa	Proprietary digital	1
Soil temperature	Omega 44007	±0.2°C	V(DC)	−0.1
Soil temperature	Omega 44007	±0.2°C	V(DC)	−0.4
SW radiation upwelling	Kipp & Zonen CNR4	$15\ W\ m^{-2}$	V(DC)	2
SW radiation downwelling	Kipp & Zonen CNR4	$15\ W\ m^{-2}$	V(DC)	2
LW radiation upwelling	Kipp & Zonen CNR4	10%	V(DC)	2
LW radiation downwelling	Kipp & Zonen CNR4	10%	V(DC)	2
Ground heat flux	Hukseflux HFP01SC		V(DC)	−0.1
Battery voltage	—	0.1 V	V(DC)	—

Table 1.2 AWS Quantities Measured

1.2 API GATE WAY.

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales. Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. API developers can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud. API Gateway creates RESTful APIs that: Are HTTP-based.

API TYPES

- RESTful APIs
- WEBSOCKET APIs

1.2.1 RESTful APIs

Build RESTful APIs optimized for serverless workloads and HTTP backends using HTTP APIs. HTTP APIs are the best choice for building APIs that only require API proxy functionality. If your APIs require API proxy functionality and API management features in a single solution, API Gateway also offers REST APIs.

1.2.2 WEBSOCKET APIs

Build real-time two-way communication applications, such as chat apps and streaming dashboards, with WebSocket APIs. API Gateway maintains a persistent connection to handle message transfer between your backend service and your clients.

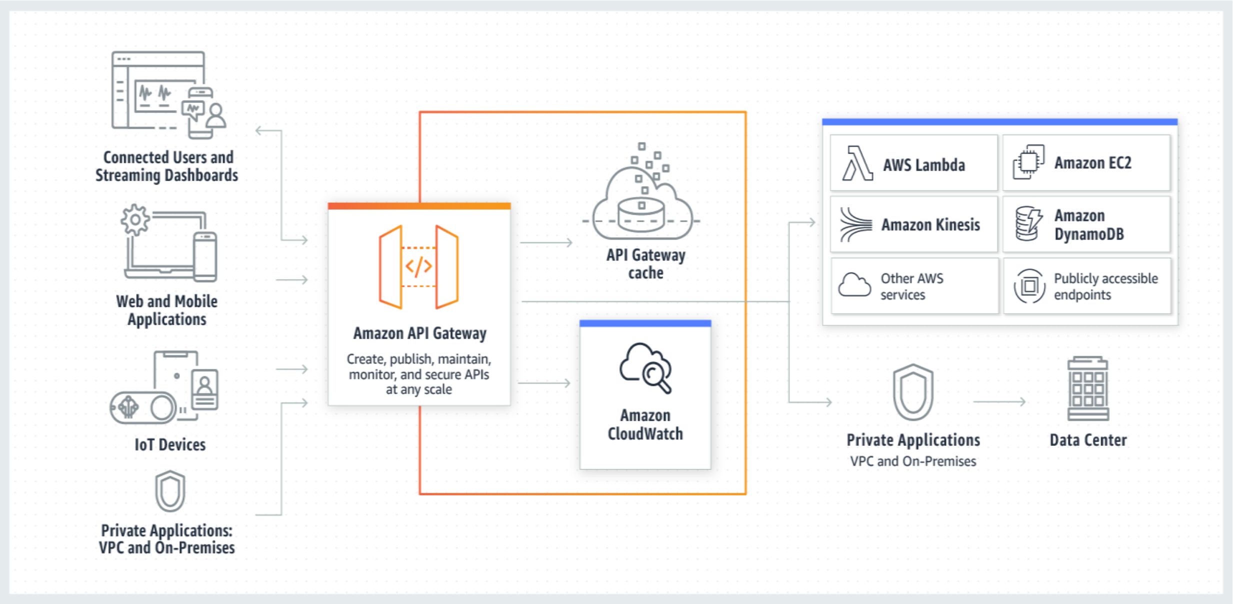
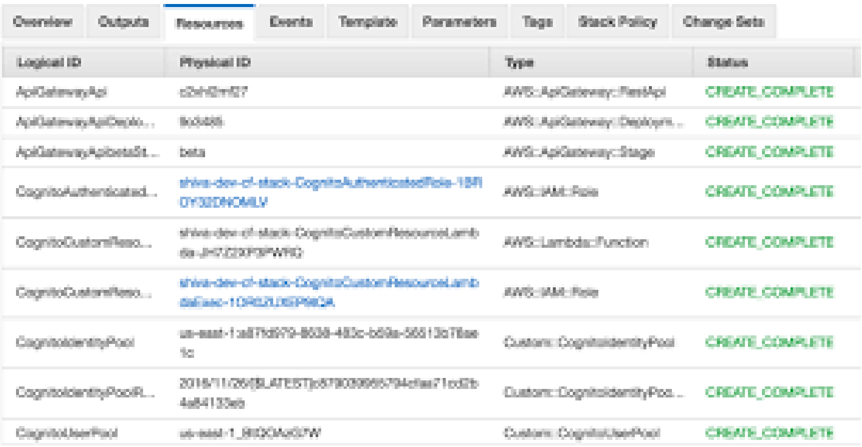

Connected Users and Streaming Dashboards
Web and Mobile Applications
IoT Devices
Private Applications: VPC and On-Premises
Amazon API Gateway
Create, publish, maintain, monitor, and secure APIs at any scale
API Gateway cache
Amazon CloudWatch
AWS Lambda
Amazon EC2
Amazon Kinesis
Amazon DynamoDB
Other AWS services
Publicly accessible endpoints
Private Applications
VPC and On-Premises
Data Center

Fig 1.1 API Gateway Works.



Logical ID	Physical ID	Type	Status
ApiGatewayApi	c2vh2mf27	AWS::ApiGateway::RestApi	CREATE_COMPLETE
ApiGatewayApiDeplo...	9o0495	AWS::ApiGateway::Deploym...	CREATE_COMPLETE
ApiGatewayApibetaSt...	beta	AWS::ApiGateway::Stage	CREATE_COMPLETE
CognitoAuthenticated...	shiva-dev-cf-stack-CognitoAuthenticatedRole-1BR0Y32DNOMLV	AWS::IAM::Role	CREATE_COMPLETE
CognitoCustomReso...	shiva-dev-cf-stack-CognitoCustomResourceLambda-JH7Z2XF9PWRG	AWS::Lambda::Function	CREATE_COMPLETE
CognitoCustomReso...	shiva-dev-cf-stack-CognitoCustomResourceLambdaExec-1OR62UX6P8QA	AWS::IAM::Role	CREATE_COMPLETE
CognitoIdentityPool	us-east-1:a87fd979-8638-483c-b59a-56513b78ae1c	Custom::CognitoIdentityPool	CREATE_COMPLETE
CognitoIdentityPoolR...	2018/11/26/[$LATEST]c879030865794cfae71cd2b4a84133eb	Custom::CognitoIdentityPoo...	CREATE_COMPLETE
CognitoUserPool	us-east-1_8tXOAzG7W	Custom::CognitoUserPool	CREATE_COMPLETE

Table 2.2 API Gateway

1.3 SALT ALGORITHMS

Hashing is a one-way function where data is mapped to a fixed-length value. Hashing is primarily used for authentication. Salting is an additional step during hashing, typically seen in association to hashed passwords, that adds an additional value to the end of the password that changes the hash value produced. A cryptographic salt is made up of random bits added to each password instance before its hashing. Salts create unique passwords even in the instance of two users choosing the same passwords. Salts help us mitigate hash table attacks by forcing attackers to re-compute them using the salts for each user as AES-256 is the technology we use to encrypt data in AWS, including Amazon Simple Storage Service (S3) server-side encryption.

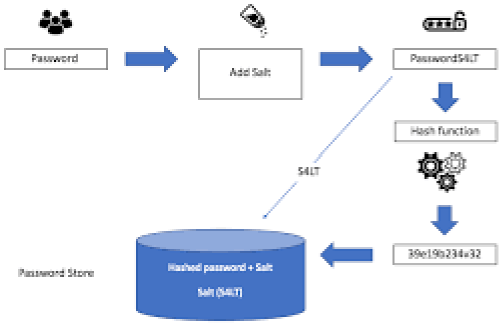


Fig 1.2 Salting Password (Encryption & Decryption)

The APIs created with Amazon API Gateway expose HTTPS endpoints only. API Gateway doesn't support unencrypted (HTTP) endpoints. For greater security, you can choose a minimum Transport Layer Security (TLS) protocol version to be enforced for your API Gateway custom domain. You can choose either a TLS version 1.2 or TLS version 1.0 security policy. WebSocket APIs and HTTP APIs support only TLS 1.2. To learn more, see Choosing a minimum TLS version for a custom domain in API Gateway.

1.4 FUTURE OF AMAZON WEB SERVICES.

In the first quarter of 2020, AWS revenues grew by 33% compared to Q4 2019. This shows the continued growth that AWS tends to enjoy in the market. With the Coronavirus pandemic crisis, the need to move to the cloud has increased, and reports have shown that spending on cloud computing across enterprises has increased. Cloud computing has been transforming the way people work and access information & data globally. With cloud computing, one is able to get on-demand delivery of IT resources over the internet with different efficient price models. Thanks to cloud computing, organizations no longer have to maintain physical data centers and servers, while still being able to access technology services – computing power, storage, and databases from the cloud service providers. The three most popular models of cloud computing are IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) and SaaS (Software-as-a-Service).

There are many different cloud service providers in the market, such as, Amazon AWS, Microsoft Azure, Google Cloud Platform, etc. Of these, AWS has been the most popular cloud service provider across the world, and has consistently held the number one position in the cloud computing market in terms of market shares of the cloud service providers.

1.5 APPLICATION.

a. **AWS Application in Business Stream**

AWS helps the business to build the app and generate new revenue streams quickly. Through this, you can easily develop applications for your business purpose. Amazon EC2 has a number of different performance levels to support your application's requirement. AWS Identity and access management allow you to monitor your web application. Moreover, it helps you to monitor unauthorized access. With the help of AWS management kit, you can easily deploy and manage your applications so that you can focus on other aspects of your application. AWS brings together the service needed to build and run your application seamlessly. This provides you with more time for creating value for your business.

Enterprises require their software to run 24×7. They are building business applications in the cloud to increase their revenue. Small as well as large scale industries are running their business applications in the cloud for a better growth, to increase their revenue and to maximize profit. New business should generate a good outcome and it can be reached by providing a better service in the field of competition. There are many benefits while using AWS in business such as-

- Pay as you go
- Easy and Scalable
- Accessible and fast

b. **AWS Application in content Management System**.

AWS provides quality work which makes their customers a permanent one. The content provided by the user is confidential and secure. AWS uses high-speed servers which helps the user to easily complete their task. The fast processing databases which are fully managed and known for its scalability and low latencies are there for help. It is a durable and secure technology platform. To ensure the safety and integrity of your data, Amazon's data centers and services have several levels of security. is playing a major role.

C. **Conclusion**

Hence, in this AWS Tutorial, we studied Applications of Amazon Web Services. Amazon cloud is the secure and reliable platform which saves your money and time. The applications of AWS are only for business and private (small-scale) purpose. Furthermore, if you have a query, feel free to ask in the comment section.

CHAPTER 2

LITERATURE REVIEW

Neo Banking refers to the delivery of services and applications over the Internet, instead of a local hard drive or a physical on-premises data center to individual customers, small, medium and large organizations. The next element that lies ahead are the services cloud technology offers which cover a wide range including data storage and computing resources such as RAM, CPU etc.

Internet and the Banking System:

The rapid growth of the Web creates a tremendous opportunity for new businesses, but also requires a new way of viewing the market place for the community banker. "Experts estimates that consumer use of on-line banking services will increase over 20-fold by the end of the century. Geography and the number of branches become irrelevant and community banks are able to offer the same level of service and convenience to customers as the largest banks. In the past, over 60% of existing bank customers have cited their bank selection to be based on convenience of location. For the customers of today, convenience of location includes the availability of 24-hour access via the Internet." (Wilson, 1996).

Seitz and Stickel (1999) considered that financial service companies are using the Internet as a new distribution channel. The goals are:

1. Complex products may be offered in an equivalent quality with lower costs to more potential customers
2. There may be contacts from each place of earth at any time of day and night

Seybold (1998) identifies 8 critical success factors for Neo Banking:

- Own the customer’s total experience
- Streamline business processes that impact the customer.
- Provide a 360-degree view of customer relationship.
- Let customers help themselves.
- Help customers do their job.
- Deliver personalized service

Banking becomes a pleasure as the transactions and services become instant with Neo Bank online Internet banking. The services provided are totally secure and unique. These cover online account transactions and operations, credit card and account applications and payments, share trading and investments through mutual funds, bill payments, statement generation and a virtual demo of each service.

From the perspective of banking products and services being offered through Internet, Internet banking is nothing more than traditional banking services delivered through an electronic communication backbone, viz, Internet. But, in the process it has thrown open issues which have ramifications beyond what a new delivery channel would normally envisage and, hence, has compelled regulators world over to take note of this emerging channel. Some of the distinctive features of i-banking are:

1. It removes the traditional geographical barriers as it could reach out to customers of different countries / legal jurisdiction. This has raised the question of jurisdiction of law / supervisory system to which such transactions should be subjected,
2. It has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges,
3. Security of banking transactions, validity of electronic contract, customers' privacy, etc., which have all along been concerns of both bankers and supervisors have assumed different dimensions given that Internet is a public domain, not subject to control by any single authority or group of users,
4. It poses a strategic risk of loss of business to those banks who do not respond in time, to this new technology, being the efficient and cost-effective delivery mechanism of banking services,
5. A new form of competition has emerged both from the existing players and new players of the market who are not strictly banks.

Internet – its basic structure and topology

Internet is a vast network of individual computers and computer networks connected to and communicate with each other using the same communication protocol – TCP/IP (Transmission Control Protocol / Internet Protocol). When two or more computers are connected a network is created; connecting two or more networks create ‘internetwork’ or Internet. The Internet, as commonly understood, is the largest example of such a system. Internet is often and aptly described as ‘Information Superhighway’, a means to reach innumerable potential destinations. The destination can be any one of the connected networks and host computers. TCP / IP protocol is insecure because data packets flowing through TCP / IP networks are not normally encrypted. Thus, anyone who interrupts communication between two machines will have a clear view of the data, passwords and the like. This has been addressed through Secured Socket Layer (SSL), a Transport Layer Security (TLS) system which involves an encrypted session between the client browser and the web server.

Wireless Application Protocol (WAP):

WAP is the latest industry standard which provides wireless access to Internet through handheld devices like a cellular telephone. This is an open standard promoted by WAP forum and has been adopted by world’s all major handset manufacturers. WAP is supplemented by Wireless Application Environment (WAE), which provides industry wise standard for developing applications and services for wireless communication networks. This is based on WWW technology and provides for application for small screens, with interactive capabilities and adequate security. Wireless Transaction Protocol (WTP), which is the equivalent of TCP, sets the communication rules and Wireless Transport Layer Security (WTLS) provides the required security by encrypting all the session data. WAP is set to revolutionize the commercial use of net.

The entry of Neo banks.

Internet banking, both as a medium of delivery of banking services and as a strategic tool for business development, has gained wide acceptance internationally and is fast catching up in India with more and more banks entering the fray. India can be said to be on the threshold of a major banking revolution with net banking having already been unveiled. A recent questionnaire to which 46 banks responded, has revealed that at present, 11 banks in India are providing Internet banking services at different levels, 22 banks propose to offer Internet banking in near future while the remaining 13 banks have no immediate plans to offer such facility.

At present, the total Internet users in the country are estimated at 9 lakhs. However, this is expected to grow exponentially to 90 lakhs by 2003. Only about 1% of Internet users did bank online in 1998. This increased to 16.7% in March 2000. The growth potential is, therefore, immense. Further incentives provided by banks would dissuade customers from visiting physical branches, and thus get ‘hooked’ to the convenience of arm-chair banking. The facility of accessing their accounts from anywhere in the world by using a home computer with Internet connection, is particularly fascinating to Non-Resident Indians and High Net worth Individuals having multiple bank accounts.

Costs of banking service through the Internet form a fraction of costs through conventional methods. Rough estimates assume teller cost at Re.1 per transaction, ATM transaction cost at 45 paise, phone banking at 35 paise, debit cards at 20 paise and Internet banking at 10 paise per transaction. The cost-conscious banks in the country have therefore actively considered use of the Internet as a channel for providing services. Fully computerized banks, with better management of them customer base is in a stronger position to cross-sell their products through this channel.

Products and services offered

Banks in India are at different stages of the web-enabled banking cycle. Initially, a 35 bank, which is not having a web site, allows its customer to communicate with it through an e-mail address; communication is limited to a small number of branches and offices which have access to this e-mail account. As yet, many scheduled commercial banks in India are still in the first stage of Internet banking operations.

With gradual adoption of Information Technology, the bank puts up a web-site that provides general information on the banks, its location, services available e.g. loan and deposits products, application forms for downloading and e-mail option for enquiries and feedback. It is largely a marketing or advertising tool. For example, Vijaya Bank provides information on its web-site about its NRI and other services. Customers are required to fill in applications on the Net and can later receive loans or other products requested for at their local branch. A few banks provide the customer to enquire into his demat account (securities/shares) holding details, transaction details and status of instructions given by him. These web sites still do not allow online transactions for their customers.

Some of the banks permit customers to interact with them and transact electronically with them. Such services include request for opening of accounts, requisition for cheque books, stop payment of cheques, viewing and printing statements of accounts, movement of funds between accounts within the same bank, querying on status of requests, instructions for opening of Letters of Credit and Bank Guarantees etc. These services are being initiated by banks like ICICI Bank Ltd., HDFC Bank Ltd. Citibank, Global Trust Bank Ltd., UTI Bank Ltd., Bank of Madura Ltd., Federal Bank Ltd. etc. Recent entrants in Internet banking are Allahabad Bank (for its corporate customers through its ‘Allnet’ service) and Bank of Punjab Ltd. State Bank of India has announced that it will be providing such services soon. Certain banks like ICICI Bank Ltd., have gone a step further within the transactional stage of Internet banking by allowing transfer of funds by an account holder to any other account holder of the bank.

System architecture and design

Appropriate system architecture and control is an important factor in managing various kinds of operational and security risks. Banks face the risk of wrong choice of technology, improper system design and inadequate control processes. For example, if access to a system is based on only an IP address, any user can gain access by masquerading as a legitimate user by spoofing IP address of a genuine user. Numerous protocols are used for communication across Internet. Each protocol is designed for specific types of data transfer. A system allowing communication with all protocols, say HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), telnet etc. is more prone to attack than one designed to permit say, only HTTP.

Choice of appropriate technology is a potential risk banks face. Technology which is outdated, not scalable or not proven could land the bank in investment loss, a vulnerable system and inefficient service with attendant operational and security risks and also risk of loss of business.

Many banks rely on outside service providers to implement, operate and maintain their 45 e-banking systems. Although this may be necessary when banks do not have the requisite expertise, it adds to the operational risk. The service provider gains access to all critical business information and technical systems of the bank, thus making the system vulnerable. In such a scenario, the choice of vendor, the contractual arrangement for providing the service etc., become critical components of banks' security. Bank should educate its own staff and over dependencies on these vendors should be avoided as far as possible.

Not updating bank's system in keeping with the rapidly changing technology, increases

operational risk because it leaves holes in the security system of the bank. Also, staff may fail to understand fully the nature of new technology employed. Further, if updating is left entirely at customers' end, it may not be updated as required by the bank. Thus, education of the staff as well as users plays an important role to avoid operational risk.

Technology and Security Standards For Internet Banking

The Internet has provided a new and inexpensive channel for banks to reach out to their customers. It allows customers to access banks’ facilities round the clock and 7 days a week. It also allows customers to access these facilities from remote sites/home etc. However, all these capabilities come with a price. The highly unregulated Internet provides a less than secure environment for the banks to interface. The diversity in computer, communication and software technologies used by the banks vastly increases the challenges facing the online bankers. In this chapter, an effort has been made to give an overview of the technologies commonly used in Internet banking. An attempt has been made to describe concepts, techniques and technologies related to privacy and security including the physical security. The banks planning to offer Internet banking should have explicit policies on security. An outline for a possible framework for security policy and planning has also been given. Finally, recommendations have been made for ensuring security in Internet banking.

Computer networking & Internet

The purpose of computer networking is sharing of computing resources and data across the whole organization and the outside world. Computer Networks can be primarily divided into two categories based on speed of data transfers and geographical reach. A Local area network (LAN) connects many servers and workstations within a small geographical area, such as a floor or a building. Some of the common LAN technologies are 10 MB Ethernet, 100 MB Ethernet, 1GB Ethernet, Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM). The data transfer rates here are very high. They commonly use broadcast mode of data transfer. The Wide Area Network (WAN), on the other hand, is designed to carry data over great distances and are generally point-to-point. Connectivity in WAN set-up is provided by using dial-up modems on the Public Switched Telephone Network (PSTN) or leased lines, VSAT networks, an Integrated Services Digital Network (ISDN) or T1 lines, Frame Relay/X.25 (Permanent Virtual Circuits), Synchronous Optical Network (SONET), or by using Virtual Private Networks (VPN) which are software-defined dedicated and customized services used to carry traffic over the Internet. The different topologies, technologies and data communication protocols have different implications on safety and security of services.

To standardize on communications between systems, the International Organization of Standards developed the OSI model (the Open System Interconnection Reference Model) in 1977. The OSI breaks up the communication process into 7 layers and describe the functions and interfaces of each layer. The important services provided by some of the layers are mentioned below. It is necessary to have a good understanding of these layers for developing applications and for deploying firewalls (described later).

Application Layer: Network Management, File Transfer Protocol, Information validation, Application-level access security checking.

Session Layer: establishing, managing and terminating connections (sessions) between applications

Transport Layer: Reliable transparent transfer of data between end points, end to end recovery & flow control.

Network Layer: Routing, switching, traffic monitoring and congestion control, control of network connections, logical channels and data flow.

Data Link Layer: Reliable transfer of data across physical link and control of flow of data from one machine to another.

Protocols: The data transmission protocol suite used for the Internet is known as the Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet is primarily a network of networks. The networks in a particular geographical area are connected into a large regional network. The regional networks are connected via a high speed "back bone". The data sent from one region to another is first transmitted to a Network Access Point (NAP) and are then routed over the backbone. Each computer connected to the Internet is given a unique IP address (such as 142.16.111.84) and a hierarchical domain name (such as cse.iitb.ernet.in). The Internet can be accessed using various application-level protocols such as FTP (File Transfer Protocol), Telnet (Remote Terminal Control Protocol), Simple Mail Transport Protocol (SMTP), Hypertext Transfer Protocol (HTTP). These protocols run on top of TCP/IP. The most 52 innovative part of the Internet is the World Wide Web (WWW). The web uses hyperlinks, which allow users to move from any place on the web to any other place. The web consists of web pages, which are multimedia pages composed of text, graphics, sound and video. The web pages are made using Hypertext Markup Language (HTML). The web works on a client-server model in which the client software, known as the browser, runs on the local machine and the server software, called the web server, runs on a possibly remote machine. Some of the popular browsers are Microsoft Internet Explorer and Netscape Navigator.

Information only systems: General-purpose information like interest rates, branch locations, product features, FAQs, loan and deposit calculators are provided on the bank's web (WWW) site. The sites also allow downloading of application forms. Interactivity is limited to a simple form of 'e-mail'. No identification or authentication of customers is done and there is no interaction between the bank's production system (where current data of accounts are kept and transactions are processed) and the customer.

Electronic Information Transfer System: These systems provide customerspecific information in the form of account balances, transaction details, statement of account etc. The information is still largely 'read only'. Identification and authentication of customer takes place using relatively simple techniques (like passwords). Information is fetched from the Bank's production system in either the batch mode or offline. Thus, the bank's main application system is not directly accessed.

Fully Transactional System: These systems provide bi-directional transaction capabilities. The bank allows customers to submit transactions on its systems and these directly update customer accounts. Therefore, security & control system need to be strongest here.

Application architecture

A computer-based application may be built as a monolithic software, or may be structured to run on a client–server environment, or even have three or multi-tiered architecture. A computer application typically separates its 3 main tasks: interactions with the user, processing of transactions as per the business rules, and the storage of business data. The three tasks can be viewed as three layers, which may run on the same system (possibly a large, proprietary computer system), or may be separated on to multiple computers (across the Internet), leading to three-tier or multi-tier architecture.

Security and Privacy Issues

Terminology

Security: Security in Internet banking comprises both the computer and communication security. The aim of computer security is to preserve computing resources against abuse and unauthorized use, and to protect data from accidental and deliberate damage, disclosure and modification. The communication security aims to protect data during the transmission in computer network and distributed system.

Authentication: It is a process of verifying claimed identity of an individual user, machine, software component or any other entity. For example, an IP Address identifies a computer system on the Internet, much like a phone number identifies a telephone. It may be to ensure that unauthorized users do not enter, or for verifying the sources from where the data are received. It is important because it ensures authorization and accountability. Authorization means control over the activity of user, whereas accountability allows us to trace uniquely the action to a specific user. Authentication can be based on password or network address or on cryptographic techniques

Access Control: It is a mechanism to control the access to the system and its facilities by a given user up to the extent necessary to perform his job function. It provides for the protection of the system resources against unauthorized access. An access control mechanism uses the authenticated identities of principals and the information about these principals to determine and enforce access rights. It goes hand in hand with authentication. In establishing a link between a bank's internal network and the Internet, we may create a number of additional access points into the internal operational system. In this situation, unauthorized access attempts might be initiated from anywhere. Unauthorized access causes destruction, alterations, theft of data or funds, compromising data confidentiality, denial of service etc. Access control may be of discretionary and mandatory types.

Data Confidentiality: The concept of providing for protection of data from unauthorized disclosure is called data confidentiality. Due to the open nature of Internet, unless otherwise protected, all data transfer can be monitored or read by others. Although it is difficult to monitor a transmission at random, because of numerous paths available, special programs such as “Sniffers”, set up at an opportune location like Web server, can collect vital information. This may include credit card number, deposits, loans or password etc. Confidentiality extends beyond data transfer and include any connected data storage system including network storage systems. Password and other access control methods help in ensuring data confidentiality.

Data Integrity: It ensures that information cannot be modified in unexpected way. Loss of data integrity could result from human error, intentional tampering, or even catastrophic events. Failure to protect the correctness of data may render data useless, or worse, dangerous. Efforts must be made to ensure the accuracy and soundness of data at all times. Access control, encryption and digital signatures are the methods to ensure data integrity.

Non-Repudiation: Non-Repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that data 58 has been received or to protect the recipient against false denial by the sender that the data has been sent. To ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communication or transaction.

Security Audit Trail: A security audit refers to an independent review and examination of system's records and activities, in order to test for adequacy of system controls. It ensures compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in the control, policy and procedures. Audit Trail refers to data generated by the system, which facilitates a security audit at a future date.

Authentication Technique

As mentioned earlier, authentication is a process to verify the claimed identity. There are various techniques available for authentication. Password is the most extensively used method. Most of the financial institutions use passwords along with PIN (Personal Identification Number) for authentication. Technologies such as tokens, smart cards and biometrics can be used to strengthen the security structure by requiring the user to possess something physical.

Token technology relies on a separate physical device, which is retained by an individual, to verify the user's identity. The token resembles a small hand-held 60 card or calculator and is used to generate passwords. The device is usually synchronized with security software in the host computer such as an internal clock or an identical time-based mathematical algorithm. Tokens are well suited for one-time password generation and access control. A separate PIN is typically required to activate the token. Smart cards resemble credit cards or other traditional magnetic stripe cards, but contain an embedded computer chip. The chip includes a processor, operating system, and both Read Only Memory (ROM) and Random Access Memory (RAM). They can be used to generate one-time passwords when prompted by a host computer, or to carry cryptographic keys. A smart card reader is required for their use.

Biometrics involves identification and verification of an individual based on some physical characteristic, such as fingerprint analysis, hand geometry, or retina scanning. This technology is advancing rapidly, and offers an alternative means to authenticate a user.

Firewalls

The connection between internal networks and the outside world must be watched and monitored carefully by a gatekeeper of sorts. Firewalls do this job. Otherwise, there is a risk of exposing the internal network and systems, often leaving them vulnerable and compromising the integrity and privacy of data. Firewalls are a component or set of components that restrict access between a protected network and the outside world (i.e., the Internet). They control traffic between outside and inside a network, providing a single entry point where access control and auditing can be imposed. All firewalls examine the pieces or packets of data flowing into and out of a network and determine whether a particular person should be given access inside the network. As a result, unauthorized computers outside the firewall are prevented from directly accessing the computers inside the internal network. Broadly, there are three types of firewalls i.e., Packet filtering firewalls, Proxy servers and stateful inspection firewall. · Packet filtering routers: Packet filtering routers are the simplest form of firewalls. They are connected between 61 the host computer of an Internal network and the Internet gateway.

The bastion host directs message accepted by the router to the appropriate application servers in the protected network. Their function is to route data of a network and to allow only certain types of data into the network by checking the type of data and its source and destination address. If the router determines that the data is sourced from an Internet address which is not on its acceptable or trusted sources list, the connection would be simply refused. The advantage of this type of firewall is that it is simple and cheaper to implement and also fast and transparent to the users. The disadvantage is that if the security of the router were compromised, computers on the internal network would be open to external network for attacks. Also, the filtering rules can be difficult to configure, and a poorly configured firewall could result in security loopholes by unintentionally allowing access to an internal network.

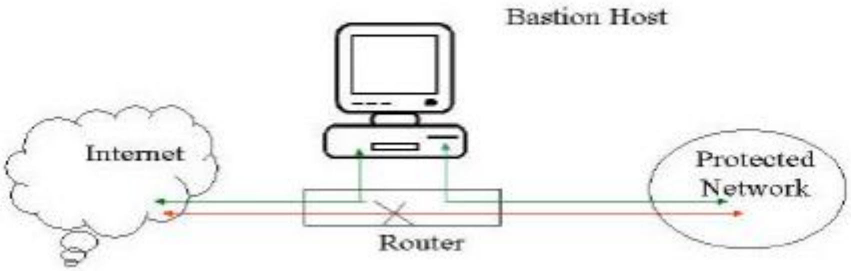


Fig. 2: A filtering router with a bastion host or proxy server

Proxy servers:

Proxy servers control incoming and outgoing traffic for a network by executing specific proxy program for each requested connection. If any computer outside the internal network wants to access some application running on a computer inside the internal network, then it would actually communicate with the proxy server, and proxy server in turn will pass the request to the internal computer and get the response which will be given to the recipient (outside user). That is, there is no direct connection between the internal network and Internet. This approach allows a high level of control and in-depth 62 monitoring using logging and auditing tools. However, since it doubles the amount of processing, this approach may lead to some degradation in performance. shows a typical firewall organization consisting of 'militarized zone' that separates the protected network from the Internet.

Stateful Inspection firewall:

This type of firewalls thoroughly inspects all packets of information at the network level as in the case of proxy servers. Specifications of each packet of data, such as the user and the transportation method, the application used are all queried and verified in the inspection processes. The information collected is maintained so that all future transmissions are inspected and compared to past transmission. If both the "state" of the transmission and the "context" in which it is used deviate from normal patterns, the connection would be refused. This type of firewalls are very powerful but performance would also decline due to the intensive inspection and verification performed.

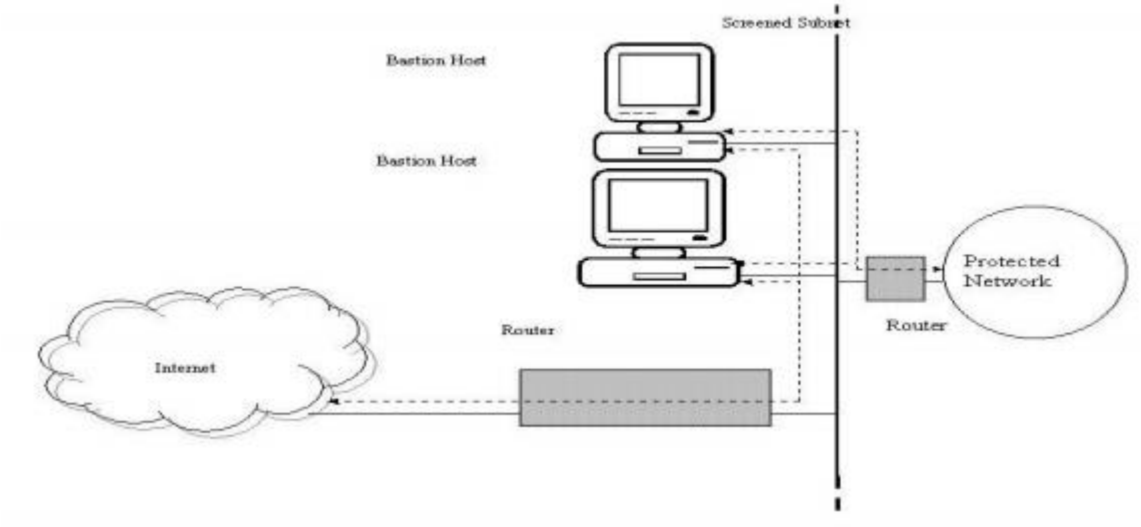


Fig.6.3 : Creating a 'Militarized Zone" to protect internal systems

Regulatory and supervisory concerns

Banking on the Internet provides benefits to the consumer in terms of convenience, and to the provider in terms of cost reduction and greater reach. The Internet itself however is not a secure medium, and thus poses a number of risks of concern to regulators and supervisors of banks and financial institutions. World over, regulators and supervisors are still evolving their approach towards the regulation and supervision of Internet banking. Regulations and guidelines issued by some countries include the following.

1. Requirement to notify about web site content
2. Prior authorization based on risk assessment made by external auditors
3. On-site examination of third party service providers
4. Off-site policing the perimeters to look for infringement.

5. Prohibition on hyper links to non bank business sites

6. Specification of the architecture

In some countries supervisors have followed a ‘hands-off’ approach to regulation of such activities, while others have adopted a wait and watch attitude. This chapter suggests approaches to supervision of Internet banking activities, drawing upon the best international practices in this area as relevant to the Indian context.

Payment Gateway

An externally shared service, which will develop, as the pivot of the Internet banking would be the payment gateway. With the increasing popularity of “e-Commerce” i.e., buying and selling over the Internet, electronic payments and settlements for such 90 purchases, is a natural and expected requirement. Banks, which are the vital segment of the payment system in the country, will therefore be required to equip themselves to meet this emerging challenge. In its basic form, the ‘Inter-Bank Payment Gateway’ for payments and settlements of e-Commerce transactions is not very different from the traditional cheque clearing system, which is perhaps the most widely prevalent form of Inter-Bank settlement of funds, or the net settlement system of the international card agencies like Visa, Master Cards and American Express, for the credit card payments. With the emergence of the Internet and the ability to buy and sell over the Internet, it has become imperative to deploy a similar Inter-Bank Payment Gateway to facilitate authorization for payments and settlement between participating institutions for commercial transactions carried out over the Internet. No one particular model for setting up an Inter-Bank Payment Gateway for such payments has been established as yet and we are, therefore, in a situation where the regulatory and supervisory framework itself needs to be evolved. Given the above considerations, the following framework for setting up Inter-Bank **Payment Gateways for Internet payments:**

Only institutions that are members of the cheque clearing system in the country may be permitted to participate in the Inter-Bank Payment Gateway initiatives for Internet payments.

Both ‘net-settlement’ and ‘gross-settlement’ capabilities might be necessary, net settlement being the settlement mode for transaction below a certain pre-specified threshold value and gross settlement for transactions higher than the pre-specified value.The Inter-Bank Payment Gateway should have one nominated bank as the clearing bank to settle all transactions.

The approval for setting up the Inter-Bank Payment Gateway should be granted only by the Reserve Bank of India, in their capacity as the Regulator of banks and Payment Systems in the country. The norms to become eligible to set up the Inter Bank Payment Gateway should be specified by the Reserve Bank of India, on the basis of which institutions may seek formal approval to set up the Inter-Bank Payment Gateway.

It is expected that there will not be more than two or three Inter Bank Payment Gateways in the Country and all banks who wish to participate in the payment and settlement for e-Commerce transactions originated over the Internet could become a member of one or more of these Inter-Bank Payment Gateways. All payments routed through the Inter-Bank Gateways should only cover direct debits and direct credits to the accounts maintained with the participating Banks by the parties involved in the e-Commerce transaction.

Payments effected using credit cards should not be routed through the Inter-Bank Payment Gateway. These should be authorized by the payer bank (i.e., acquiring bank) directly through its credit card authorization capability. It should be obligatory on the part of the Inter-Bank Payments Gateway to establish, at any time, the Complete trace of any payment transactions routed through it. The trace should cover date and time stamp when the transaction was originated and authorized, the payee details (account number and name of the payee bank), the payers details (account number and name of the payer bank), as well as a unique Transactional Reference Number (TRN) provided by both the Payee Bank and Payer Bank for each transaction.

Connectivity between the Inter-Bank Payment Gateway and the computer system of the member Banks should be achieved using a leased line network (not over the Internet), with appropriate data encryption standards. All settlements over the Inter-Bank Payment Gateway should be intra-day, as far as possible in real time. Until the exchange control aspects with regard to cross-border issues of eCommerce ransactions are fully discussed and documented, payment and settlement of such transactions should not be permitted over the Inter-Bank Payment Gateway. 12. Only Inter Bank Payments and Settlements (i.e., transactions involving more than one Bank) should be routed through the Inter-Bank Payment Gateway. Intra-bank payments (i.e., transactions involving only one Bank) should be handled by the bank's own internal system. The responsibility for the credit risk associated with every payment transaction routed over the Inter Bank Payment Gateway will rest with the appropriate Payee The mandate and the related documentation (that would form the basis for effecting payments for transactions carried out over the Internet) should be bilateral in nature. All transactions must be authenticated using a user ID and password. SSL/128-bit encryption must be used as the minimum level of security. As and when the regulatory framework is in place, all such transactions should be digitally certified by one of the licensed Certification Authorities. The Service Provider who is responsible for the operations of the Inter-Bank Payment Gateway must ensure adequate firewalls and related security measure to ensure privacy to the participating institution, i.e., every institution can access data pertaining to only itself and its customer transactions. Internationally accepted standards such as ISO8583 must be used for transmitting payment and settlement messages over the Network. 18. It may also be appropriate to have a panel of approved Auditors who will be required to certify the security of the entire infrastructure both at the Inter-Bank Payment Gateway as well as the participating institution's end prior to making the facility available for customer use. A process of perpetual audit must also be instituted.

Where the Bank is required to inform visitors to its own Web Site about the Portals with whom they have a payment arrangement or Portals that the bank would want its customers to visit. These out-bound hyperlinks are unlikely to have any major security implications to the bank. In order to reflect the stability of the banking system, banks should not be seen as sponsors of or promoters of the products of unrelated businesses or of any businesses, which they are not licensed to run. The hyperlinks should hence be confined to only those portals with which they have a payment arrangement or the sites of their subsidiaries or principals.

The second type of hyperlink is where the Portal sites link to the bank site to pass information pertaining to a payment by one of their Internet Shoppers. This usually involves making a URL (Universal Resource Locator) link to the bank site to request authorization for payment. Such links deliver to the bank site information regarding the customer (typically his registration no) and the value of the payment to be authorized. Unless the bank exercises the right level of authentication and security, this type of URL links can be the source of a number of security breaches. It is therefore imperative that every bank ensures at least the following minimum-security precautions in order that the bank's as well as its customer's interests are protected.

Upon receiving the URL request from the Portal site, the bank should authenticate the customer who has originated the transaction by asking him to key in, on the browser screen, his user ID and password which the bank would have provided him to facilitate access to his accounts with the bank. Upon such authentication and due verification, the bank should re-submit the transaction information on the customer's browser terminal i.e., the name of the Portal site to whom the payment is to be affected as well as the value of the transactions and seek the explicit approval of the customer to authorize the payment. Depending on the nature of the payment, the payment authorization request should be routed either to the credit card authorizing system if payment is requested using credit card, or to the banks' host system in case of a direct debit or to the Inter-Bank Payment Gateway in case of debit to customer account in another bank. Upon receiving the payment authorization, the bank should return the URL request to 94 the originating Portal, with a unique reference number for the transaction, as a conformation to pay as per the settlement cycle agreed with the Portal. All interactions with the Portal sites as well as the customers browser terminal should be secured using SSL/128 bit encryption as a minimum requirement and should in due course be also augmented with the digital certification requirement as and when digital certificate deployment is enabled in the country. It was deliberated whether banks undertaking Internet banking should be subject to an additional capital charge because of the potentially higher proneness to unexpected losses. As yet standards have not been developed for measuring additional capital charge on account of operational risks. However, this will be covered in a way once the banks move towards risk-based supervision where supervisory intervention will be linked to the risk profile of individual institutions. In such a scenario, an enhanced supervisory risk assessment on this account could warrant an additional capital charge.

CHAPTER 3

SYSTEM SPECIFICATION

3.1 SOFTWARE REQUIREMENTS

This section gives the details of the software that are used for the development.

Operating System: Windows & Linux

Application: Docker, Apache

Language: Php

Database: MySQL

3.2 HARDWARE REQUIREMENTS

This section gives the details and specification of hardware on which the system is expected to work.

Processor: Intel Dual Core (minimum)

CPU clock: 2.93GHz and above

Hard disk capacity: 260 GB and above

Memory: 1GB and above

Monitor: Any monitor

Keyboard: Standard 108keys

Mouse: Any mouse

CHAPTER 4

SOFTWARE DESCRIPTION

4.1 Dockers

Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and deploy it as one package. It is an open platform for developing, shipping, and running applications. Docker enables you to separate your applications from your infrastructure so you can deliver software quickly. With Docker, you can manage your infrastructure in the same ways you manage your applications and Docker Swarm and is meant to coordinate clusters of nodes at scale in production in an efficient manner.

4.2 COINTAINERS

AWS Containers services. Share and deploy container software, publicly or privately. Run containerized applications or build microservices. Run Amazon ECS in your own data center. Manage containers with Kubernetes. Create and operate Kubernetes clusters on your own infrastructure. Containers provide a standard way to package your application's code, configurations, and dependencies into a single object. Containers share an operating system installed on the server and run as resource-isolated processes, ensuring quick, reliable, and consistent deployments, regardless of environment. Containers rely on virtual isolation to deploy and run applications that access a shared operating system kernel without the need for virtual machines. Containers hold components such as files, libraries and environment variables necessary to run desired software.

4.3 MySQL

MySQL is a relational database management system based on SQL – Structured Query Language. The application is used for a wide range of purposes, including data warehousing, e-commerce, and logging applications. The most common use for MySQL however, is for the purpose of a web database. MySQL is the world's most popular open-source relational database and Amazon RDS makes it easy to set up, operate, and scale MySQL deployments in the cloud. With Amazon RDS, you can deploy scalable MySQL servers in minutes with cost-efficient and resizable hardware capacity.

4.4 ELASTIC CLOUD COMPUTING (EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. An EC2 instance is nothing but a virtual server in Amazon Web services terminology. It stands for Elastic Compute

Cloud. An on-demand EC2 instance is an offering from AWS where the subscriber/user can rent the virtual server per hour and use it to deploy his/her own applications.

An EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure. AWS is a comprehensive, evolving cloud computing platform; EC2 is a service that allows business subscribers to run application programs in the computing environment.

CHAPTER 5

SYSTEM ANALYSIS

5.1 EXISTING SYSTEM

The Online Banking System as of now deals with a single sign-in log on and it will not be secure as expected. If a customer logs on from an unknown system outside the usual access device there are chances that it can be hacked easily and this might end up with a lot of issues. There are chances that if the user forgets the password and supposedly changes it and writes down the same somewhere and forgets to erase it or scramble it, there are chances that anyone can misuse the login. But it is not fully filled with all necessary requirement due to Network traffic happen while truncation occurs with low phase in network. Process through the business logic is very less intensive in the portal time out due to scalability is low and completion of truncation may take long time in the application. Platform with Invoicing, Bulk Payouts, APIs & more is not able to completed. Transactions happens but process has not fully completed.

Disadvantages

- Network Traffic.
- Truncation transactions Failure.
- Portal Time Out
- Scalability & Process is too low.
- Poor Business Logic

5.2 PROPOSED SYSTEM

Once a customer logs in he or she has to generate a transaction password for online banking transactions. It will be an additional password apart from the login username and password credentials. The third security system can be provided by adding a graphical password generator which needs to be punched in before confirming an online transaction. This will involve password strength meter also. Authentication is an activity of linking an independent or an individual process on the basis of username and password which basically consists of characters, numbers, alphanumeric values, special characters etc. Most of the authentications are complex, though they seem to be boring to the users and are very hard to remember. Every one of us, use the simple textual passwords which can be easily guessed by the attacker.

Let us try a New methodology to improve the authentication process using graphical password generation by making the user selects his/her own set of passwords as a series of clicks on the image which we will store it as a pattern and for each click the strength of the password is calculated and can be used to classify the password as Low/Medium/High. Our Online Banking approach will be a click-based graphical passwords authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), the country of France (from a map of the world), the city of Nice (from a map of France), a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge.

The best Business Logics is been implemented with end-to-end transaction is been encrypted with secure payment through the cloud. ultimately leads to increased productivity, efficiency, flexibility, cost-effectiveness and an improved bottom-line. Rapid customer acquisition through quicker account setup, faster approval of loans, reduced paperwork, fraud detection, mobile deposits are only some of the benefits that customers can enjoy with hybrid banking,

Advantages

- This application is effective and saves the time.
- Heavy load can be balanced.
- Scalability and highly Securable.
- The database in Lightsail.
- Server less work load

CHAPTER 6

SYSTEM MODULES

The lists of modules used in this work are:

1. Customer
    a. Transaction History
    b. Transfer Funds
    c. ATM Simulator
    d. Submit Grievance
2. Admin
    a. Add Customer
    b. Manger Customer
    c. Customer Grievance
    d. Post News

6.1 CUSTOMER

6.1.1 Transaction History

This Module the customer can see the history of whole truncation which was done customer and getting the relevant information in the transaction history in the application. The first module handles account creation for a new customer. The account can be Savings account, Term (Fixed) account. The details of the customer and his account are being fed to the database through a registration form which is validated by the bank prior to addition to the database. Once the request is approved the user can remit the amount and open the account.

6.1.2 Transfer Fund

The second module consists of the various transactions that the customer can carry out. The main transactions include deposit, withdrawal and money transfer. In this module bank administrator gives the user ID and password in order to perform online transactions. The user is also given the privilege to change his password which will be automatically updated to the database. Each account holder can deposit and withdraw money into the bank through this module.

6.1.3 ATM Simulator

The purpose of this program is to simulate a simple Automatic Teller Machine (ATM). The ATM is used by customers of a bank. Each customer has a customer number and a Personal Identification Number (PIN). Both must be typed into the simulation to gain access to the accounts and This learning object is an introduction to using a cash machine (ATM). Learn the basics of using a cash machine and then try our cash machine simulator to get Money.

6.1.4 Submit Grievance

They can fill with the required details in which Fill in the details, attach documents as per files selected for upload and fill in the 'Grievance Description click on 'Preview and Submit' to preview and submit grievance. It stores in the data base and resolve by teams.

6.2 ADMIN

In admin you can raise the Query where it can be solved with in an hour which is specified with AI bot. Admin his responsible in Assist and support banking staff in handling customers' requests and needs. Sell banking products and services to customers. Create and implement innovative methods in banking administration aspects. Target and capture customers to increase banking business and he is the key person to manage the customer details and credential.

6.2.1. Add Customers

The Admin can add multiple number of customers to the database in which separate individual containers is been created, So the transaction and management will be zero traffic with high scalability.

6.2.2 Manage Customers

Management of customer with scalability where easy managed using the Load Balancer from the side of Admin. Containers will multiple for specific customer it is easy to fetch the details by cloud application.

6.2.3 Customer Grievance

The customer can fill with the required details in which Fill in the details, attach documents as per files selected for upload and fill in the 'Grievance Description click on 'Preview and Submit' to preview and submit grievance. It stores in the data base and resolve by teams.

6.2.4 Post New

You are looking at documentation for an older release. For the latest information, see the current release documentation and Post-coordinated Codes and Has Concept Modifier Relationship. Though it may not be explicitly shown in a particular Template, the use of any coded

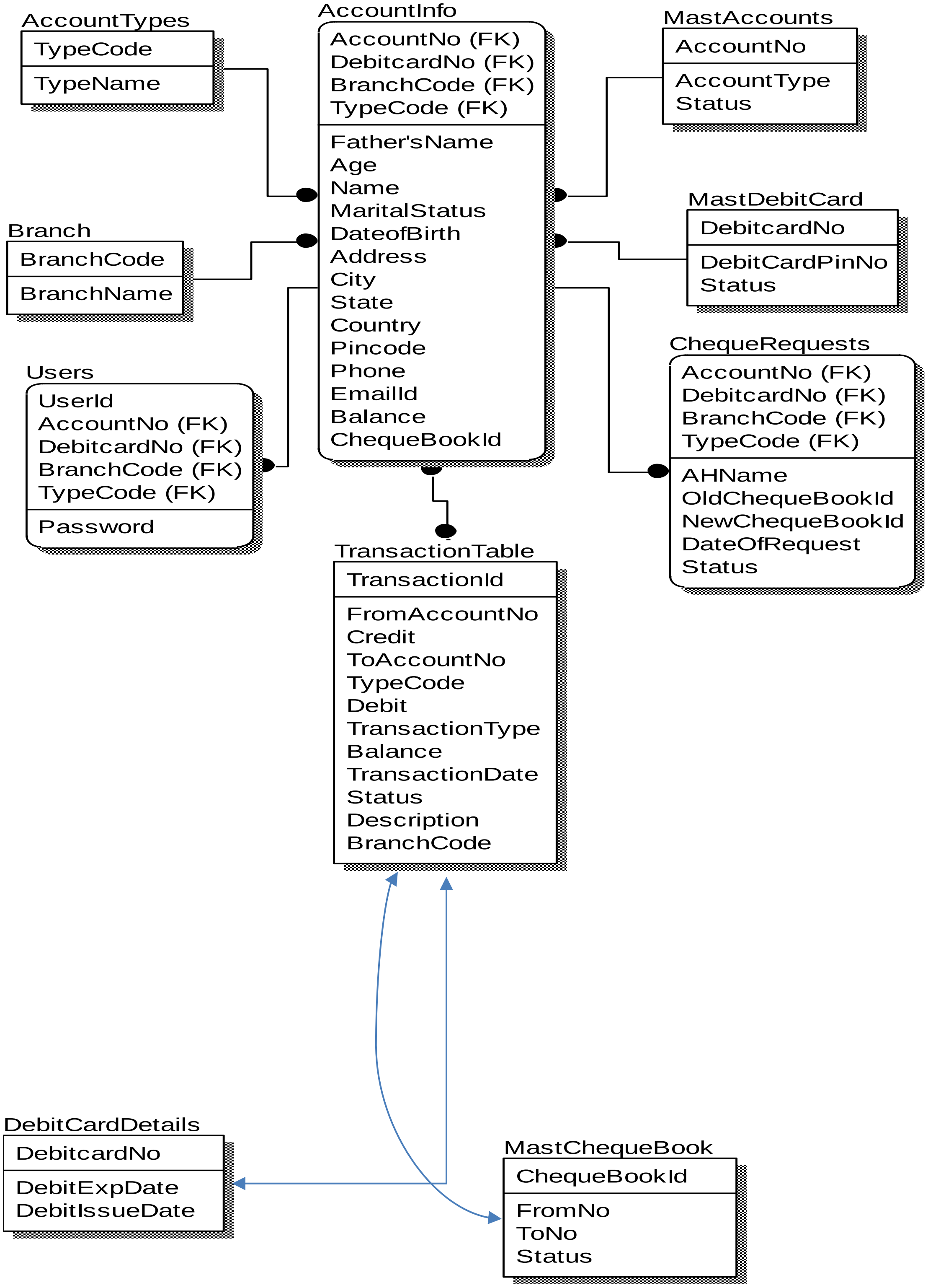
CHAPTER 7

DESIGN AND IMPLEMENTATION

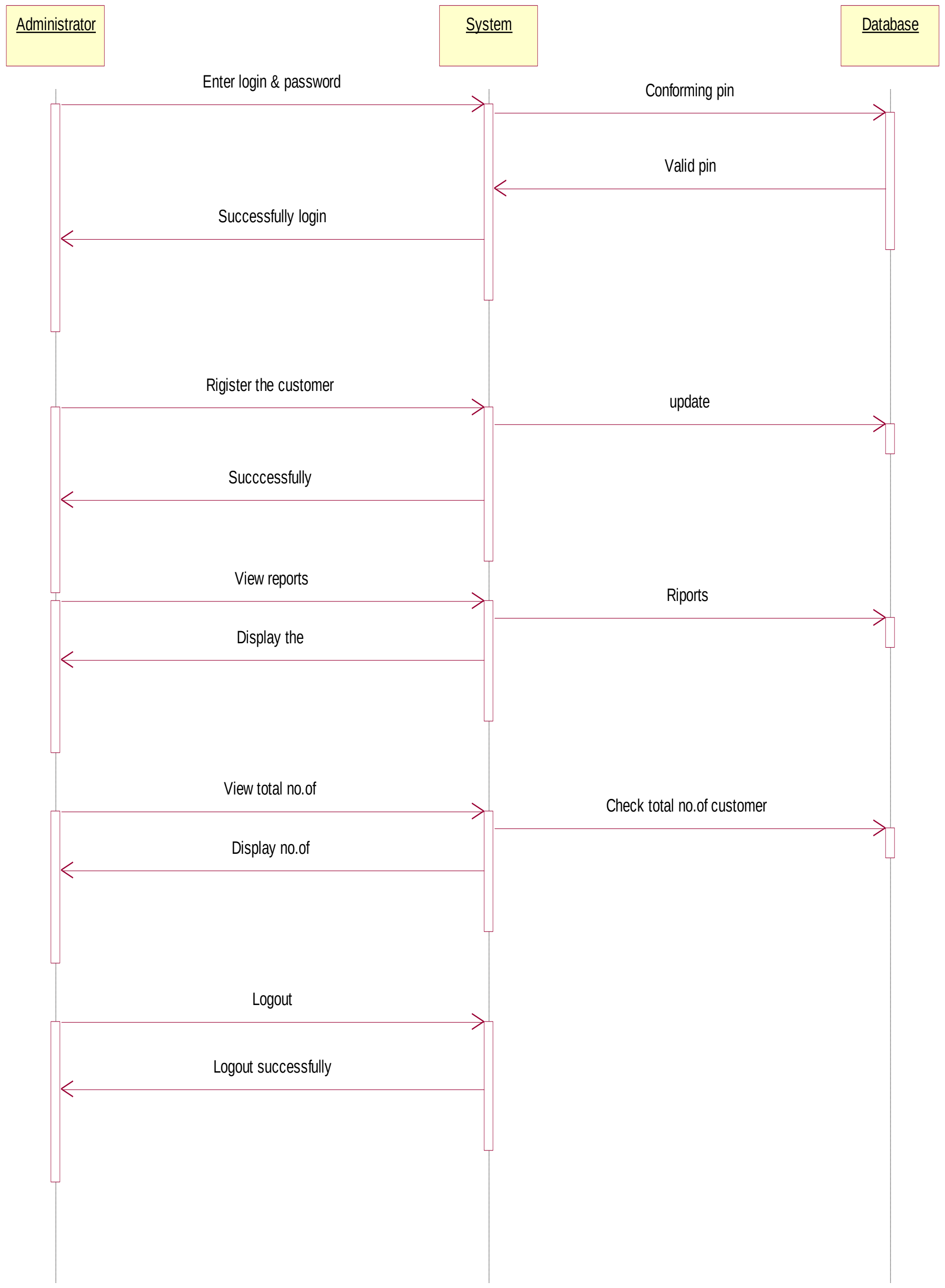
Enjoy Instant Fund Transfers, Automate Payments & Earn Rewards for Saving Money. Apply Now. The NeoBanking With An Online Savings Account. You'll Never Have to Visit A Branch Again. Spend Intelligently. Digital Banking Platform. Track your expenses. Finding a best banking service of the future is not such a bad idea, right? After all, technology that disrupts the banking industry, if used properly, can become its savior. Unfortunately, today, we can’t bring you incredible news that we invented a time machine, but we can still offer something extremely valuable. We have spent the last few months combining our knowledge and experience from engineering dozens of financial services in UXDA with recent trends in the financial industry to create Fintech case study of the mobile only NetBank in UX design and Neo bank Price Now, Best Place to Buy Neo bank. Pemex’s the fastest Neo bank futures exchange. Buy Neo bank With Credit/Debit Cards, Zero Trading Fees/Buy in Minutes/100X Leverage. Simulated Trading. Zero-Fee Spot. Spot Contract Trading.

7.1 METHODS USED FOR IMPLEMENTATIONS

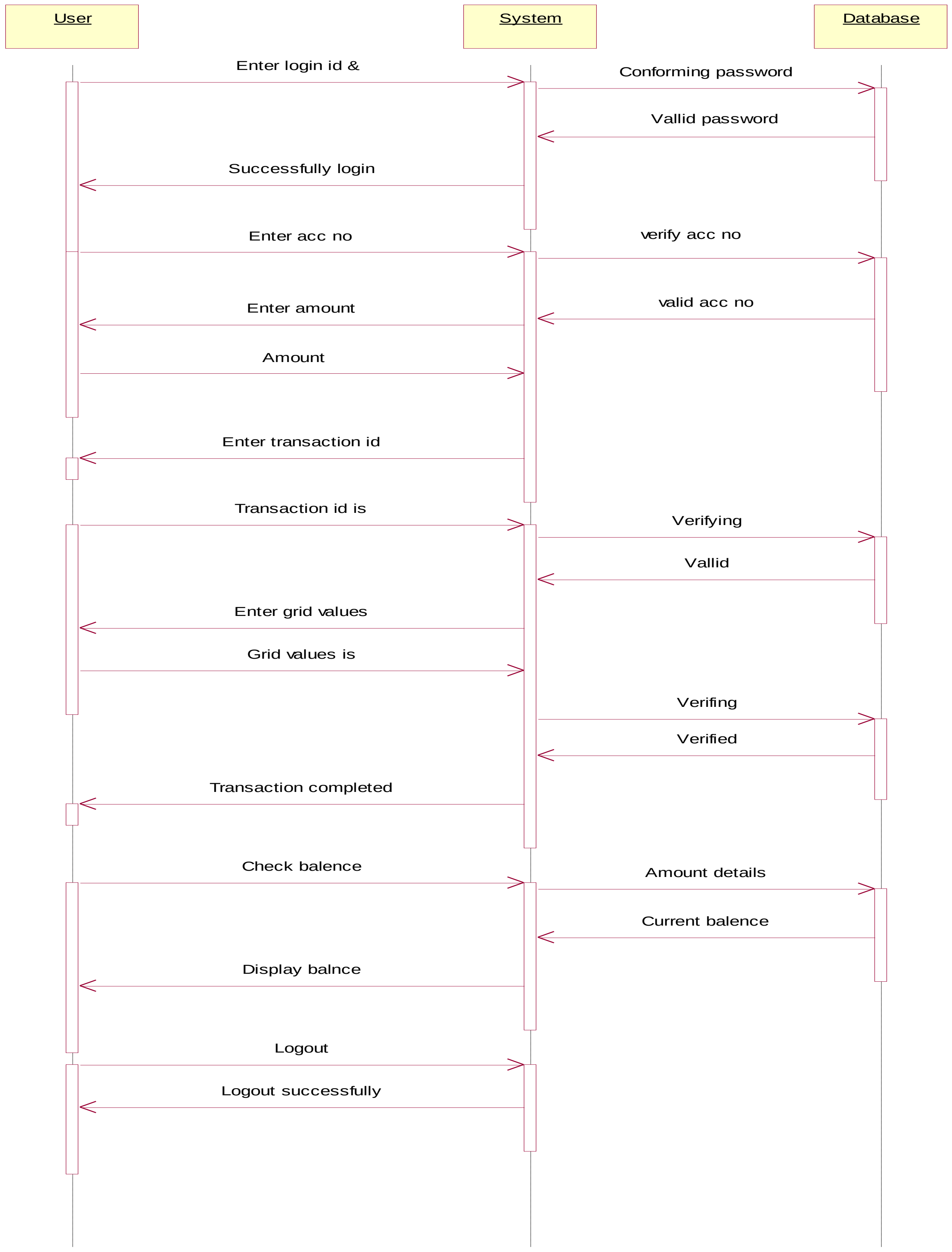
7.1.1 Class Diagram



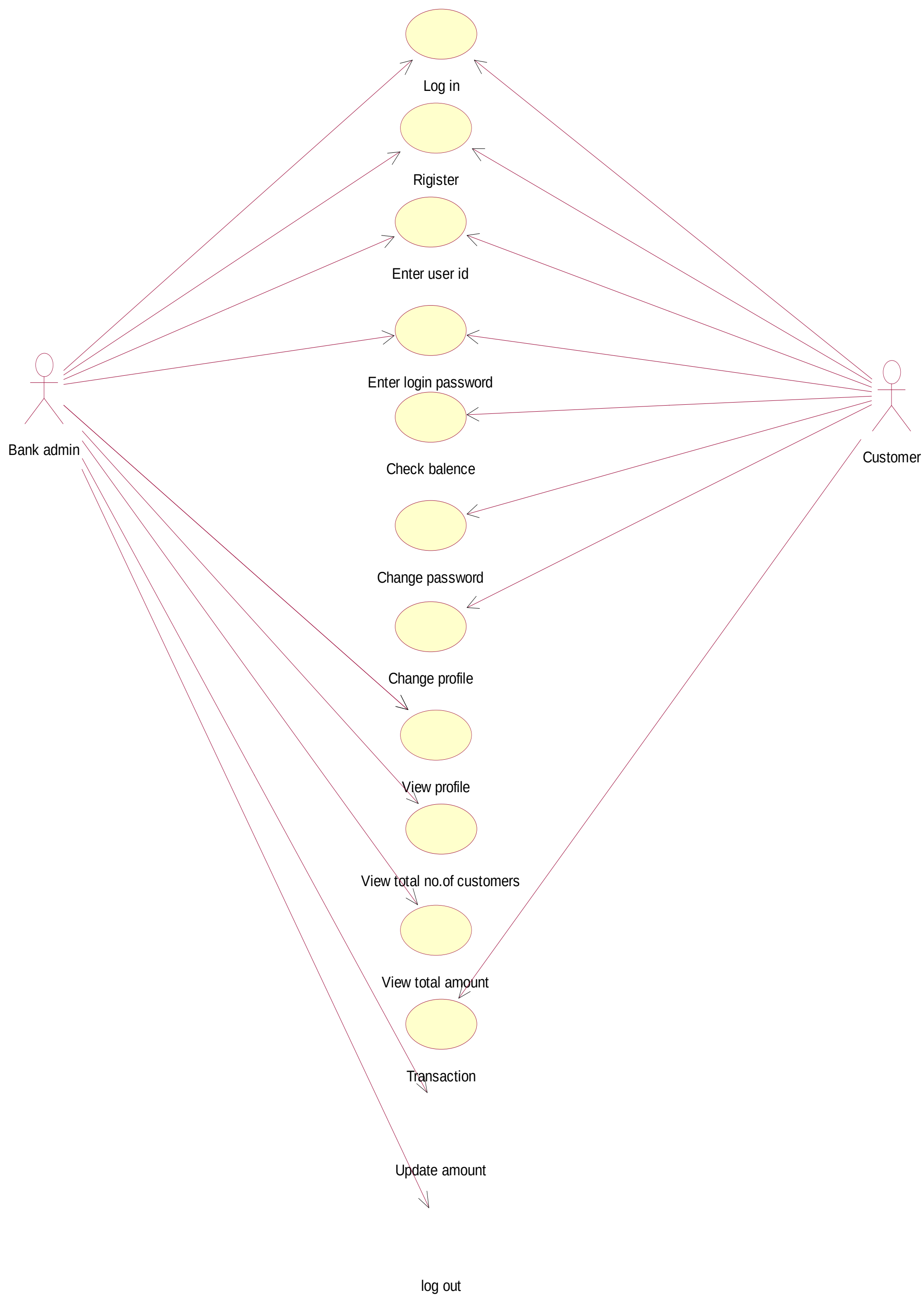
7.1.2 Sequence and Collaboration Diagrams



7.1.3 User Sequence diagram



7.1.4 Use case Diagrams



7.1.5 IMPLEMENTING MICROSERVICES

- API
- DOCKERS

As you progress in your education as a developer, you will sooner or later understand the benefits that a container system like Docker has to offer: you can specify your environment in code, without all the Slack messages to system engineers or the headaches that go into standing up consistently provisioned servers. Likewise, you have probably understood the appeal of microservices as a solution to the problems of a monolithic application mired in its own debt-ridden smell.This article offers some insights into how you can leverage Docker in the development flow of your microservices. Development of a microservice itself ought to be fairly straight-forward; from an environment perspective, developing one should not be all that different than developing a more traditional application. Perhaps your microservice needs to support an API endpoint or two you need it to connect to a couple data models like MySQL or Redis, and you can get off to the races pretty quickly.

This is Docker 101 stuff. You can tap into well-supported existing Docker projects like Laradock or NoDock (for PHP and Node.js respectively), which offer developers an integrated Docker environment that supports an array of common technologies networked together via docker-compose. he first heads-up I'd like to give anyone working with Docker is that its pace of development has been pretty fast: even fairly recent courses may refer to commands or utilities that have already been deprecated (eg, docker-machine). Be prepared to grit your teeth a bit, scratch your head, and navigate some unfamiliar error messages. Once you get past the bouncers, however, membership in the Docker club is worth it. Of course, before we begin, make sure you've got the Docker toolbox on your computer. See Docker.com to download the client for your host operating system (the CE Community Edition version is fine for our purposes).If you need to run a specific technology such as a scripting language or operating system, chances are good that someone has already created a Docker image for it. Docker Hub is your friend when it comes to reusing code that others have so generously shared. Remember: do not reinvent wheels! Note that for some reason, the site is labeled to search for containers, when you are in fact searching for images. Remember: containers are templates -- multiple container instances can be created from a single image template.In a nutshell, your interactions here should revolve around cloning the container (using the clone command) and then running an instance of it (using the run command). For example, this is all you need to do get a working copy of Postgres:

7.1.6 IMPLEMENTATION OF LOAD BALANCER & COINTAINERS

Software-based load balancers can be classified into two broad categories: installable load balancers and Load Balancer as a Service (LBaaS). Some examples of installable software load balancers are: Nginx, Varnish, HAProxy and LVS. These load balancers require installation, configuration as well management First, we need to create

Docker hosts in which we can run the containers. If you are not familiar with Docker, we recommend reading more about launching Docker hosts and containers in our previous article Docker containers on OpenStack VMs first. In this entry, we launch two OpenStack VMs running Ubuntu 14.04 on different deployments. The easiest way to launch the VMs is to use the Dashboard.

The VMs being launched should have a public IP address in order to be directly addressable over the internet. Then, we need to keep the TCP port 2376 open for communication in order to run with Docker. Additionally, the TCP port 80 (HTTP) needs to be open in order to access the load balancer and ports 8080 and 8081 so that the reverse proxy server can reach the upstream servers that will be accessible on that ports. Once the VMs are launched and operating, we make them Docker hosts with docker-machine using the generic driver. We can do so by executing this command from the local environment for both VMs:

7.1.7 IMPLEMENT ELASTIC CLOUD COMPUTING WITH PHP & MySQL

This examines the process of using Amazon Web Services (AWS) EC2 as a platform for a database backed web application. It describes how to deploy an EC2 instance and a RDS instance, how to connect the EC2 instance and the RDS instance, how to connect PHP to the RDS database, and how to retrieve data. Learners will come away with an understanding of how to deploy EC2 with an application whether that application is PHP based or using another language. Requirements include basic understanding of SSH (Secure Shell), MySQL databases, and access to an AWS account (i.e., capable of deploying EC2 and RDS instances, working with security groups, key pairs, snapshots, and billing).

- Understand how to deploy an EC2 instance using Amazon Linux
- Learn how to install Apache, PHP, and MySQL on EC2
- Discover how to connect an EC2 instance to RDS and retrieve data
- Examine the differences between AWS EC2, Elastic Beanstalk, and Lightsail
- Explore the basics of EC2 storage and networking

Steve Suehring is an Assistant Professor of Computing and New Media Technologies at the University of Wisconsin-Stevens Point. Steve teaches courses on server and cloud engineering, systems design, LAMP stack programming, big data, and more. Prior to joining the faculty, Steve spent 20 years in the industry as a technical architect, systems engineer, and network administrator.

7.1.8 Final Combating

Finally, All need to combine and o use an external database with an application running in Elastic Beanstalk, first launch a DB instance with Amazon RDS. When you launch an instance with Amazon RDS, it is completely independent of Elastic Beanstalk and your Elastic Beanstalk environments, and will not be terminated or monitored by Elastic Beanstalk. Use the Amazon RDS console to launch a Multi-AZ MySQL DB instance. Choosing a Multi-AZ deployment ensures that your database will fail over and continue to be available if the source DB instance goes out of service.

EC2 instance – An Amazon Elastic Compute Cloud (Amazon EC2) virtual machine configured to run web apps on the platform that you choose.Each platform runs a specific set of software, configuration files, and scripts to support a specific language version, framework, web container, or combination of these. Most platforms use either Apache or NGINX as a reverse proxy that sits in front of your web app, forwards requests to it, serves static assets, and generates access and error logs.

Instance security group – An Amazon EC2 security group configured to allow inbound traffic on port 80. This resource lets HTTP traffic from the load balancer reach the EC2 instance running your web app. By default, traffic isn't allowed on other ports.

Load balancer – An Elastic Load Balancing load balancer configured to distribute requests to the instances running your application. A load balancer also eliminates the need to expose your instances directly to the internet.

Load balancer security group – An Amazon EC2 security group configured to allow inbound traffic on port 80. This resource lets HTTP traffic from the internet reach the load balancer. By default, traffic isn't allowed on other ports.

Auto Scaling group – An Auto Scaling group configured to replace an instance if it is terminated or becomes unavailable.

PHP – A storage location for your source code, logs, and other artifacts that are created when you use Elastic Beanstalk.

Amazon API Gate way – There are load on the instances in your environment and that are triggered if the load is too high or too low. When an alarm is triggered, your Auto Scaling group scales up or down in response.

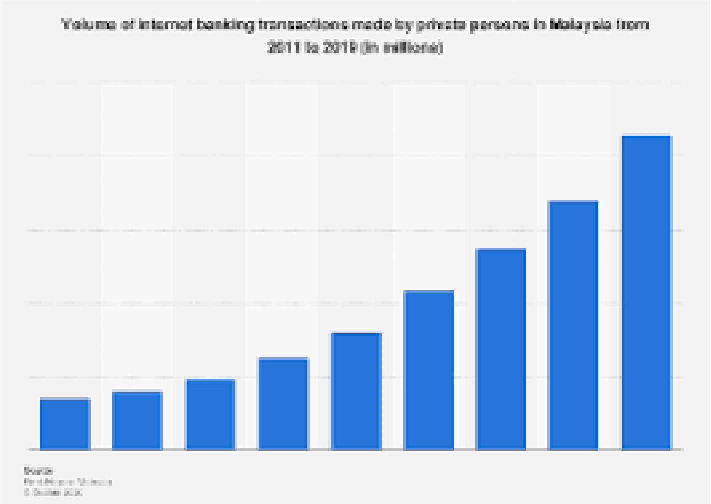
Domain name – A domain name that routes to your web app in the form subdomain.region.elasticbeanstalk.com.

CHAPTER 8

RESULT AND DISCUSSION

Phishing is a trick to trap a user to give his/her personal information. A Hacker creates a duplicate website which is a replica of the original genuine website. Now, the Hacker sends an e-mail to a user (here, a bank customer) giving a link and saying that his account needs to be updated or his account has been locked and asking him to send his account details immediately. Now, the customer may fall for his trick and clicks the link, because the link would look similar to the genuine bank's link (under which, the hacker's URL is hidden in that). Now, when the link is clicked, the customer is re-directed to that fake website (created by hacker). Customer thinks that he has reached a genuine website and gives his account details and personal details thinking that the e-mail is from genuine website. The account details are now re-directed to the Hacker. Thus, the Hacker is successful in cheating the customer.

ANTI – PHISHING is the solution to get rid of this problem. This Anti-Phishing is nothing but "preventing the phishing".Creating a cipher key (an encrypted code) in the customer's username, password or in a/c no., which is not recognized in the hacker's fake website, is considered as one of the best solutions



Source

Bank Negara Malaysia

© Statista 2020

Figure 8.1 Graph of Neo Banking evalution

CHAPTER 9

CONCLUSION AND FUTURE WORK

9.1 CONCLUSION

The main aim of developing software is to provide all information that is required by the users. User friendliness is a must that is the user must get the details without complicated searching procedures. Other important requirements of software are data security, extensibility and maintainability. All these features are included in this web application. The project greatly helped in understanding the various phases in website development and exposure to a new developer platform MS Visual Studio PHP and database MS SQL Server.

Offers more than just regular banking services to corporate users by providing them data on analytics, automated payments system, payroll maintenance etc. Corporates may find it convenient to raise short term funds within quick time on the basis of transactions. Products and services rendered and built on disruptive technologies are increasingly being placed in the hands of end customers, and the behaviors of banks are changing in terms of customer convenience, transparency, pricing and customer service. AS the business and operational models

9.2 FUTURE WORK

This research can be enhanced by improving the Higher level by using Serverless architecture and manages the large number of translations using Load Balancer with Payment Gateway. Improving the Business Logics with higher level of the algorithms by modifying existing algorithms on multiple containers using the light weigh instance of docker in WebSocket's and REST API's.

APPENDICES

APPENDIX 1: SOURCE CODE

MYSQL

```
-- phpMyAdmin SQL
Dump

-- version 4.8.4

--
https://www.phpmyadm
in.net/

--

-- Host: 127.0.0.1

-- Generation Time: Sep
28, 2019 at 10:00 AM

-- Server version:
10.1.37-MariaDB

-- PHP Version: 7.3.1


SET SQL_MODE =
"NO_AUTO_VALUE_
ON_ZERO";
SET AUTOCOMMIT =
0;
START
TRANSACTION;
SET time_zone =
"+00:00";



/*!40101 SET
@OLD_CHARACTER
_SET_CLIENT=@@C
HARACTER_SET_CLI
ENT */;
/*!40101 SET
@OLD_CHARACTER
_SET_RESULTS=@@
CHARACTER_SET_R
ESULTS */;
```

```
/*!40101 SET
@OLD_COLLATION_
CONNECTION=@@C
OLLATION_CONNEC
TION */;
/*!40101 SET NAMES
utf8mb4 */;


--
-- Database:
`net_banking`
--


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


--
-- Table structure for
```

```
table `admin`

--


CREATE TABLE
`admin` (
  `id` int(11) NOT
NULL,
  `uname` char(25)
DEFAULT NULL,
  `pwd` char(25)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;


--
-- Dumping data for
table `admin`
--
```

```
INSERT INTO `admin`

(`id`, `uname`, `pwd`)

VALUES

(1, 'admin',

'password123');


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

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

-


--

-- Table structure for

table `beneficiary1`

--


CREATE TABLE

`beneficiary1` (

  `benef_id` int(11)
NOT NULL,
  `benef_cust_id` int(11)
DEFAULT NULL,
  `email` varchar(30)
DEFAULT NULL,
  `phone_no`
varchar(20) DEFAULT
NULL,
  `account_no` int(11)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;


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


--
```

```
-- Table structure for
table `beneficiary2`
--

CREATE TABLE
`beneficiary2` (
  `benef_id` int(11)
NOT NULL,
  `benef_cust_id` int(11)
DEFAULT NULL,
  `email` varchar(30)
DEFAULT NULL,
  `phone_no`
varchar(20) DEFAULT
NULL,
  `account_no` int(11)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
```

```
CHARSET=latin1;


--
-- Dumping data for
table `beneficiary2`
--


INSERT INTO
`beneficiary2`
(`benef_id`,
`benef_cust_id`,
`email`, `phone_no`,
`account_no`)
VALUES
(1, 1,
'joey@gmail.com',
'984141', 12345678),
(2, 3, 'ross@gmail.com',
'98989898', 11223344);
```

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

--
-- Table structure for
table `beneficiary3`
--

CREATE TABLE
`beneficiary3` (
  `benef_id` int(11)
NOT NULL,
  `benef_cust_id` int(11)
DEFAULT NULL,
  `email` varchar(30)
DEFAULT NULL,
  `phone_no`
```

```
varchar(20) DEFAULT
NULL,
  `account_no` int(11)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;


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


--
-- Table structure for
table `customer`
--


CREATE TABLE
`customer` (
  `cust_id` int(11) NOT
NULL,
  `first_name`
varchar(30) DEFAULT
NULL,
  `last_name`
varchar(30) DEFAULT
NULL,
  `gender` varchar(10)
DEFAULT NULL,
  `dob` date DEFAULT
NULL,
  `aadhar_no` int(11)
DEFAULT NULL,
  `email` varchar(30)
DEFAULT NULL,
  `phone_no`
varchar(20) DEFAULT
NULL,
  `address` varchar(255)
DEFAULT NULL,
  `branch` varchar(30)
DEFAULT NULL,
  `account_no` int(11)
DEFAULT NULL,
  `pin` int(4) DEFAULT
NULL,
  `uname` varchar(30)
DEFAULT NULL,
  `pwd` varchar(30)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;


--
-- Dumping data for
table `customer`
```

```
--

INSERT INTO
`customer` (`cust_id`,
`first_name`,
`last_name`, `gender`,
`dob`, `aadhar_no`,
`email`, `phone_no`,
`address`, `branch`,
`account_no`, `pin`,
`uname`, `pwd`)
VALUES
(1, 'Joey', 'Tribbiani',
'male', '1970-05-18',
12345,
'joey@gmail.com',
'984141', 'Newyork',
'newyork', 12345678,
1234, 'joey',
'password'),
(2, 'Racheal', 'Green',
'female', '1985-12-28',
5555,
'racheal@gmail.com',
'9841414', 'Central
Perk', 'newyork',
112233, 1234, 'racheal',
'password'),
(3, 'Ross', 'Geller',
'male', '2001-01-12',
11223344,
'ross@gmail.com',
'98989898', 'Newyork',
'newyork', 11223344,
1111, 'ross', 'password');


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

```
--

-- Table structure for

table `news`

--


CREATE TABLE

`news` (

  `id` int(10)

UNSIGNED NOT

NULL,

  `title` varchar(40)

DEFAULT NULL,

  `created` datetime

DEFAULT NULL

) ENGINE=InnoDB

DEFAULT

CHARSET=latin1;


--
```

```
-- Dumping data for
table `news`
--

INSERT INTO `news`
(`id`, `title`, `created`)
VALUES
(1, 'Hello World !',
'2017-09-06 15:45:25'),
(2, 'The First News !',
'2017-09-06 15:45:55'),
(3, 'Increasing Interest
Rates !', '2017-09-06
15:46:21'),
(4, 'GST on banking',
'2017-11-19 16:39:35'),
(5, 'RBI allows PMC
Bank customers to
withdra', '2019-09-27
```

```
21:07:12'),
(6, 'New Post', '2019-
09-28 13:35:58');


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


--
-- Table structure for
table `news_body`
--


CREATE TABLE
`news_body` (
  `id` int(10)
UNSIGNED NOT
NULL,
  `body` text
```

```
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;


--
-- Dumping data for
table `news_body`
--


INSERT INTO
`news_body` (`id`,
`body`) VALUES
(1, '\"Lorem ipsum
dolor sit amet,
consectetur adipiscing
elit, sed do eiusmod
tempor incididunt ut
labore et dolore magna
aliqua. Ut enim ad
minim veniam, quis
```

nostrud exercitation

ullamco laboris nisi ut

aliquip ex ea commodo

consequat. Duis aute

irure dolor in

reprehenderit in

voluptate velit esse

cillum dolore eu fugiat

nulla pariatur.

Excepteur sint occaecat

cupidatat non proident,

sunt in culpa qui officia

deserunt mollit anim id

est laborum.\"'),

(2, 'What is Lorem

Ipsum? Lorem Ipsum is

simply dummy text of

the printing and

typesetting industry.

Lorem Ipsum has been

the industry\'s standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus

PageMaker including versions of Lorem Ipsum. Why do we use it? It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using \'Content here, content here\', making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for \'lorem ipsum\' will uncover many web sites still in their infancy. Various versions have evolved over the years, sometimes by accident, sometimes on purpose (injected humour and the like). Where does it come from? Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of \"de Finibus Bonorum et Malorum\" (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, \"Lorem ipsum dolor sit amet..\", comes from a line in section 1.10.32. The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from \"de Finibus Bonorum et Malorum\" by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham. Where can I get some? There are many variations of passages of Lorem Ipsum available, but the majority have suffered alteration in some form, by injected humour, or randomised words which don\'t look even slightly believable. If you are going to use a passage of Lorem Ipsum, you need to be sure there isn\'t anything embarrassing hidden in the middle of text. All the Lorem Ipsum generators on the

Internet tend to repeat predefined chunks as necessary, making this the first true generator on the Internet. It uses a dictionary of over 200 Latin words, combined with a handful of model sentence structures, to generate Lorem Ipsum which looks reasonable. The generated Lorem Ipsum is therefore always free from repetition, injected humour, or non-characteristic words etc.'),

(3, 'This is to inform that as of today interest

```
rates will increase by
4.6% on loans and
decrease by 5.8% on
deposits. Effective
immediately. '),
(4, 'This is to inform
that GST shall be
applied on all usages of
:\r\n1. Credit
Cards\r\n2. Debit
Cards\r\n3. Internet
Banking\r\nat a nominal
(nationally applied) rate
of 18%.\r\n'),
(5, 'Mumbai: The
Reserve Bank of India
(RBI) has eased the
restrictions on
depositors of Punjab &
Maharashtra
```

Cooperative Bank (PMC Bank), two days after it put a Rs 1,000 cap on the money a saver could withdraw, triggering protests.\r\n\r\nA depositor in the Mumbaibased bank can withdraw up to Rs 10,000, the RBI said in a press release on Thursday.\r\n\r\nThis will allow more than 60% of the depositors withdraw their entire account balance, according to the central bankâ€™s calculation.\r\n\r\nThe

Rs 1,000 cap was set on September 24. The RBI said it hiked the limit after an initial assessment of the bankâ€™s liquidity position by an administrator appointed by it.\r\n\r\nThe RBI said it had identified â€œmajor financial irregularities, failure of internal control and systems of the bank and wrong/under-reporting of its exposures under various off-site surveillanceâ€• that it conducted.'),

(6, 'Write the content

```
here!');


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

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

-


--

-- Table structure for

table `passbook1`

--


CREATE TABLE

`passbook1` (

  `trans_id` int(11) NOT

NULL,

  `trans_date` datetime

DEFAULT NULL,

  `remarks`

varchar(255)
```

```
DEFAULT NULL,
  `debit` int(11)
DEFAULT NULL,
  `credit` int(11)
DEFAULT NULL,
  `balance` int(11)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;

--
-- Dumping data for
table `passbook1`
--

INSERT INTO
`passbook1` (`trans_id`,
`trans_date`, `remarks`,
`debit`, `credit`,
`balance`) VALUES
(1, '2019-09-27
21:00:06', 'Opening
Balance', 0, 5000000,
5000000),
(2, '2019-09-27
21:09:38', 'Received
from: Racheal Green,
AC/No: 112233', 0,
10000, 5010000),
(3, '2019-09-28
13:37:08', 'Received
from: Racheal Green,
AC/No: 112233', 0,
50000, 5060000);


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

```
--

-- Table structure for

table `passbook2`

--



CREATE TABLE

`passbook2` (

  `trans_id` int(11) NOT

NULL,

  `trans_date` datetime

DEFAULT NULL,

  `remarks`

varchar(255)

DEFAULT NULL,

  `debit` int(11)

DEFAULT NULL,

  `credit` int(11)

DEFAULT NULL,
  `balance` int(11)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;


--
-- Dumping data for
table `passbook2`
--


INSERT INTO
`passbook2` (`trans_id`,
`trans_date`, `remarks`,
`debit`, `credit`,
`balance`) VALUES
(1, '2019-09-27
21:05:28', 'Opening
Balance', 0, 150000,
150000),

(2, '2019-09-27

21:09:38', 'Sent to: Joey

Tribbiani, AC/No:

12345678', 10000, 0,

140000),

(3, '2019-09-28

13:37:08', 'Sent to: Joey

Tribbiani, AC/No:

12345678', 50000, 0,

90000),

(4, '2019-09-28

13:37:25', 'Cash to Self',

10000, 0, 80000);


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

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

-


--
```

```
-- Table structure for
table `passbook3`
--

CREATE TABLE
`passbook3` (
  `trans_id` int(11) NOT
NULL,
  `trans_date` datetime
DEFAULT NULL,
  `remarks`
varchar(255)
DEFAULT NULL,
  `debit` int(11)
DEFAULT NULL,
  `credit` int(11)
DEFAULT NULL,
  `balance` int(11)
DEFAULT NULL
) ENGINE=InnoDB
DEFAULT
CHARSET=latin1;


--
-- Dumping data for
table `passbook3`
--


INSERT INTO
`passbook3` (`trans_id`,
`trans_date`, `remarks`,
`debit`, `credit`,
`balance`) VALUES
(1, '2019-09-28
13:35:27', 'Opening
Balance', 0, 800000,
800000);
```

```
--

-- Indexes for dumped
tables

--



--

-- Indexes for table
`admin`

--

ALTER TABLE
`admin`

  ADD PRIMARY KEY
(`id`);



--

-- Indexes for table
`beneficiary1`

--

ALTER TABLE
```

```
`beneficiary1`
  ADD PRIMARY KEY
(`benef_id`),
  ADD UNIQUE KEY
`benef_cust_id`
(`benef_cust_id`),
  ADD UNIQUE KEY
`email` (`email`),
  ADD UNIQUE KEY
`phone_no`
(`phone_no`),
  ADD UNIQUE KEY
`account_no`
(`account_no`);


--
-- Indexes for table
`beneficiary2`
--
```

```
ALTER TABLE
`beneficiary2`
  ADD PRIMARY KEY
(`benef_id`),
  ADD UNIQUE KEY
`benef_cust_id`
(`benef_cust_id`),
  ADD UNIQUE KEY
`email` (`email`),
  ADD UNIQUE KEY
`phone_no`
(`phone_no`),
  ADD UNIQUE KEY
`account_no`
(`account_no`);


--
-- Indexes for table
`beneficiary3`
```

```
--

ALTER TABLE
`beneficiary3`
  ADD PRIMARY KEY
(`benef_id`),
  ADD UNIQUE KEY
`benef_cust_id`
(`benef_cust_id`),
  ADD UNIQUE KEY
`email` (`email`),
  ADD UNIQUE KEY
`phone_no`
(`phone_no`),
  ADD UNIQUE KEY
`account_no`
(`account_no`);


--

-- Indexes for table
```

```
`customer`

--

ALTER TABLE

`customer`

  ADD PRIMARY KEY

(`cust_id`),

  ADD UNIQUE KEY

`aadhar_no`

(`aadhar_no`),

  ADD UNIQUE KEY

`email` (`email`),

  ADD UNIQUE KEY

`phone_no`

(`phone_no`),

  ADD UNIQUE KEY

`account_no`

(`account_no`),

  ADD UNIQUE KEY

`uname` (`uname`);
```

```
--
-- Indexes for table
`news`
--
ALTER TABLE `news`
  ADD PRIMARY KEY
(`id`);


--
-- Indexes for table
`news_body`
--
ALTER TABLE
`news_body`
  ADD PRIMARY KEY
(`id`);


--
```

```
-- Indexes for table
`passbook1`
--
ALTER TABLE
`passbook1`
  ADD PRIMARY KEY
(`trans_id`);


--
-- Indexes for table
`passbook2`
--
ALTER TABLE
`passbook2`
  ADD PRIMARY KEY
(`trans_id`);


--
-- Indexes for table
```

```
`passbook3`
--
ALTER TABLE
`passbook3`
  ADD PRIMARY KEY
(`trans_id`);


--
--
AUTO_INCREMENT
for dumped tables
--


--
--
AUTO_INCREMENT
for table `admin`
--
ALTER TABLE
```

```
`admin`
  MODIFY `id` int(11)
NOT NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
2;


--
--
AUTO_INCREMENT
for table `beneficiary1`
--
ALTER TABLE
`beneficiary1`
  MODIFY `benef_id`
int(11) NOT NULL
AUTO_INCREMENT;


--
```

```
--
AUTO_INCREMENT
for table `beneficiary2`
--
ALTER TABLE
`beneficiary2`
  MODIFY `benef_id`
int(11) NOT NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
3;


--
--
AUTO_INCREMENT
for table `beneficiary3`
--
ALTER TABLE
`beneficiary3`
```

```
  MODIFY `benef_id`
int(11) NOT NULL
AUTO_INCREMENT;

--
--
AUTO_INCREMENT
for table `customer`
--
ALTER TABLE
`customer`
  MODIFY `cust_id`
int(11) NOT NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
4;

--
--
```

```
AUTO_INCREMENT
for table `news`
--
ALTER TABLE `news`
  MODIFY `id` int(10)
UNSIGNED NOT
NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
7;

--
--
AUTO_INCREMENT
for table `news_body`
--
ALTER TABLE
`news_body`
  MODIFY `id` int(10)
```

```
UNSIGNED NOT
NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
7;


--
--
AUTO_INCREMENT
for table `passbook1`
--
ALTER TABLE
`passbook1`
  MODIFY `trans_id`
int(11) NOT NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
4;
```

```
--

--
AUTO_INCREMENT
for table `passbook2`

--
ALTER TABLE
`passbook2`
  MODIFY `trans_id`
int(11) NOT NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
5;


--

--
AUTO_INCREMENT
for table `passbook3`

--
ALTER TABLE
```

```
`passbook3`

  MODIFY `trans_id`
int(11) NOT NULL
AUTO_INCREMENT,
AUTO_INCREMENT=
2;

COMMIT;


/*!40101 SET
CHARACTER_SET_C
LIENT=@OLD_CHAR
ACTER_SET_CLIENT
*/;

/*!40101 SET
CHARACTER_SET_R
ESULTS=@OLD_CH
ARACTER_SET_RES
ULTS */;

/*!40101 SET
COLLATION_CONNE
```

```
CTION=@OLD_COLL
ATION_CONNECTIO
N */;
```

PHP Index

```
<?php
    include "header.php";
    include "navbar.php";

    if
(isset($_GET['loginFail
ed'])) {
        $message =
"Invalid Credentials !
Please try again.";
        echo "<script
type='text/javascript'>al
ert('$message');</script
>";
```

```
    }
?>

<!DOCTYPE html>
<html>
<head>
    <meta
name="viewport"
content="width=device-
width, initial-
scale=1.0">
    <link rel="stylesheet"
href="home_style.css">
</head>

<body>
    <div class="flex-
container-background">
        <div class="flex-
```

```
container">
      <div
class="flex-item-0">
        <h1
id="form_header">You
r Bank at Your
Fingertips.</h1>
      </div>
    </div>

    <div class="flex-
container">
      <div
class="flex-item-1">
        <form
action="customer_login
_action.php"
method="post">
          <div
```

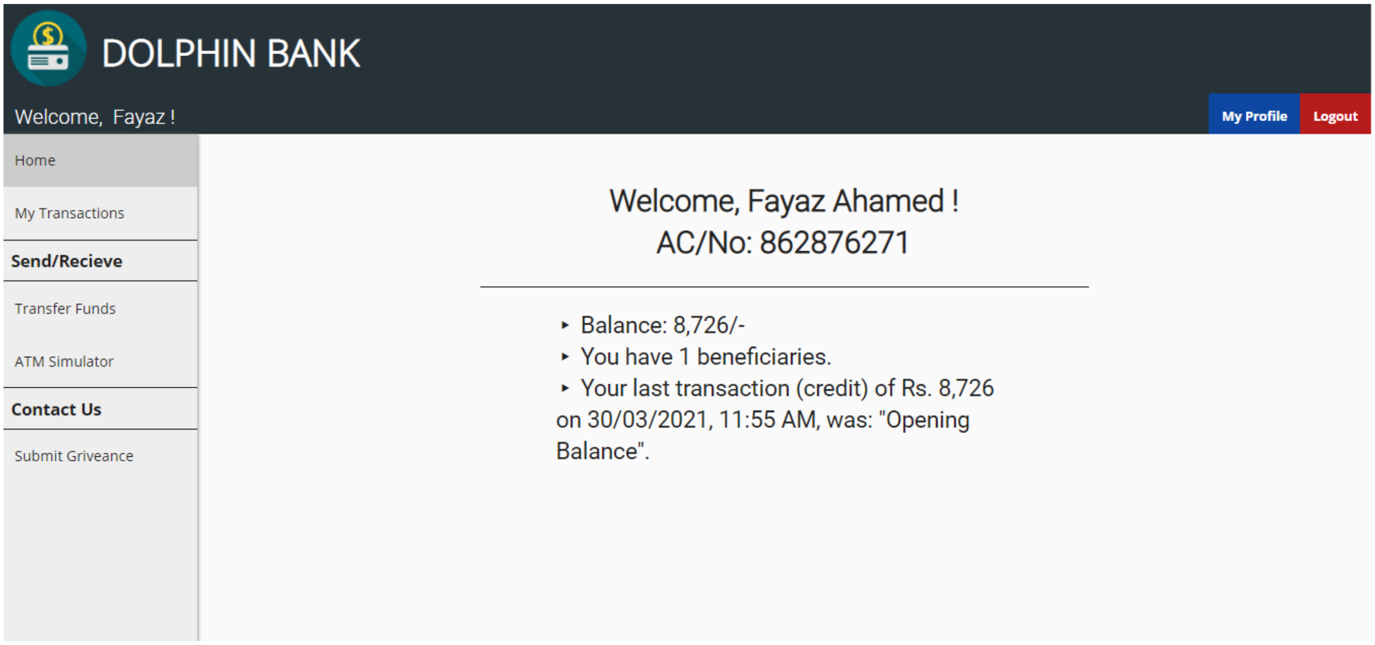
```
class="flex-item-
login">


<h2>Welcome</h2>
                </div>



                <div
class="flex-item">
                   <input
type="text"
name="cust_uname"
placeholder="Enter
your Username"
required>
                </div>



                <div
class="flex-item">
                   <input
```

```
type="password"
name="cust_psw"
placeholder="Enter
your Password"
required>
                    </div>

                    <div
class="flex-item">
                        <button
type="submit">Login</
button>
                    </div>
                </form>
            </div>
        </div>

    </div>
```

```
</body>

</html>



<?php include

"easter_egg.php"; ?>
```

APPENDIX 2: SCREENSHOTS

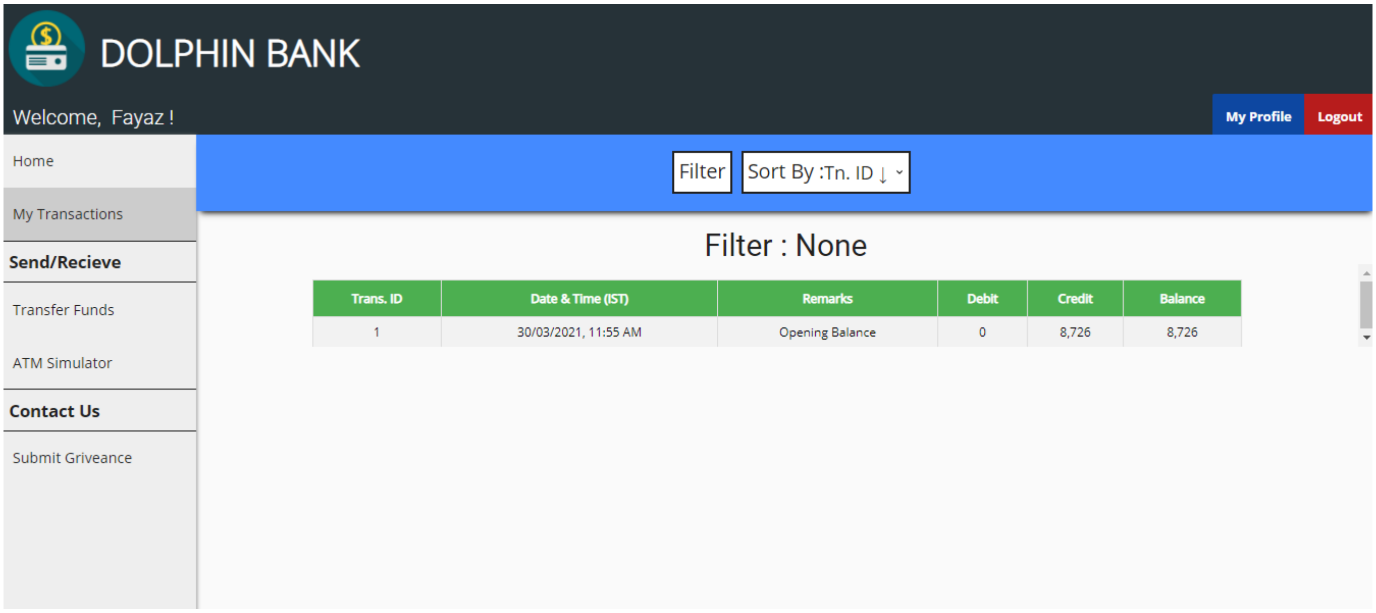
Customer



Welcome, Fayaz Ahamed !
AC/No: 862876271

- Balance: 8,726/-
- You have 1 beneficiaries.
- Your last transaction (credit) of Rs. 8,726 on 30/03/2021, 11:55 AM, was: "Opening Balance".

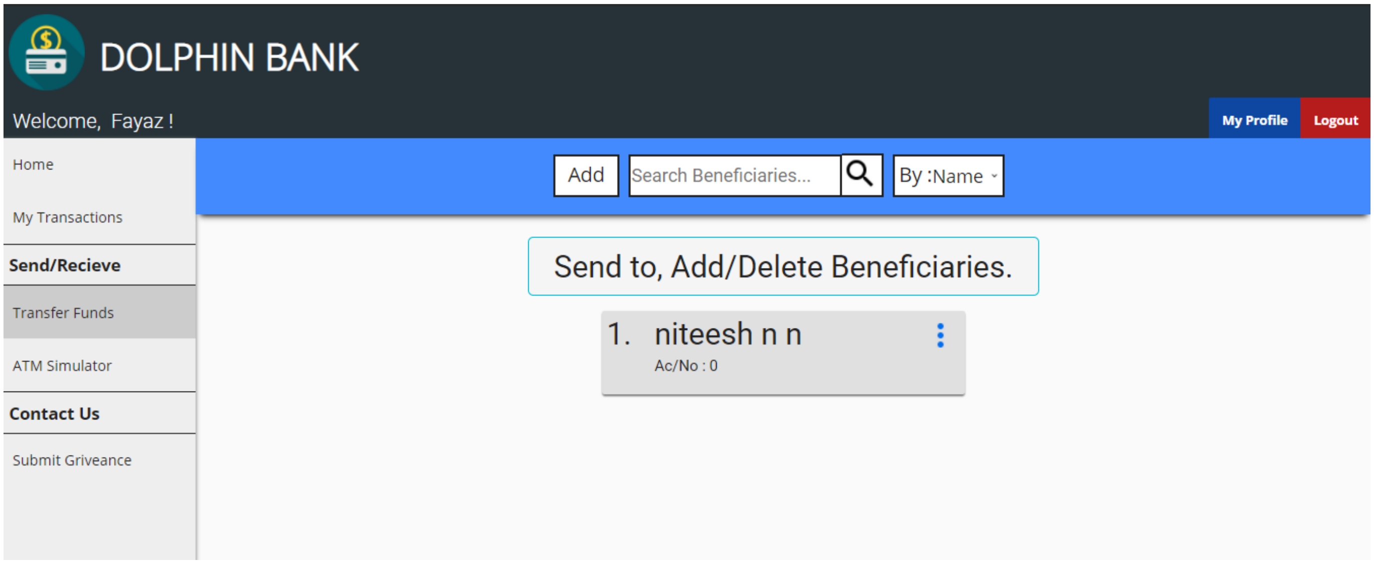
Fig 1 Customer Page



Filter : None

Trans. ID	Date & Time (IST)	Remarks	Debit	Credit	Balance
1	30/03/2021, 11:55 AM	Opening Balance	0	8,726	8,726

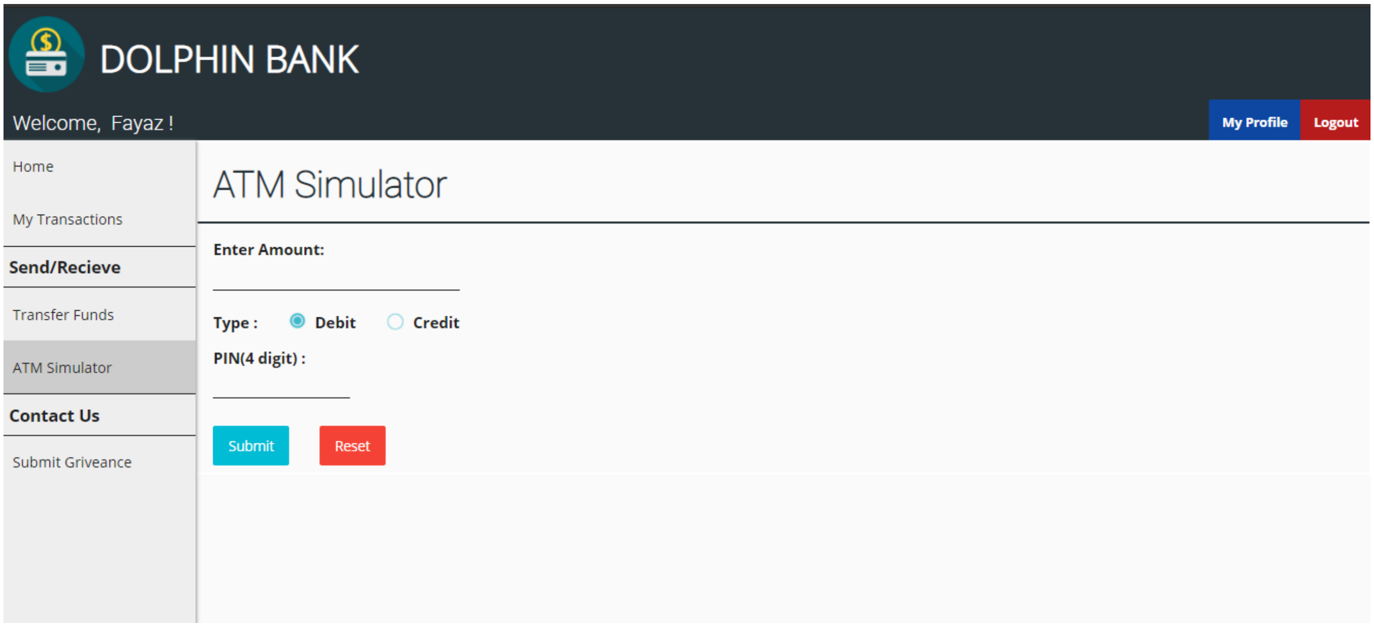
Fig 1.1 Customer Transaction



Send to, Add/Delete Beneficiaries.

1. niteesh n n
Ac/No : 0

Fig 1.2 Transfer Funds



ATM Simulator

Enter Amount:

Type : ● Debit ○ Credit

PIN(4 digit) :

Fig 1.3 ATM Simulator

Admin

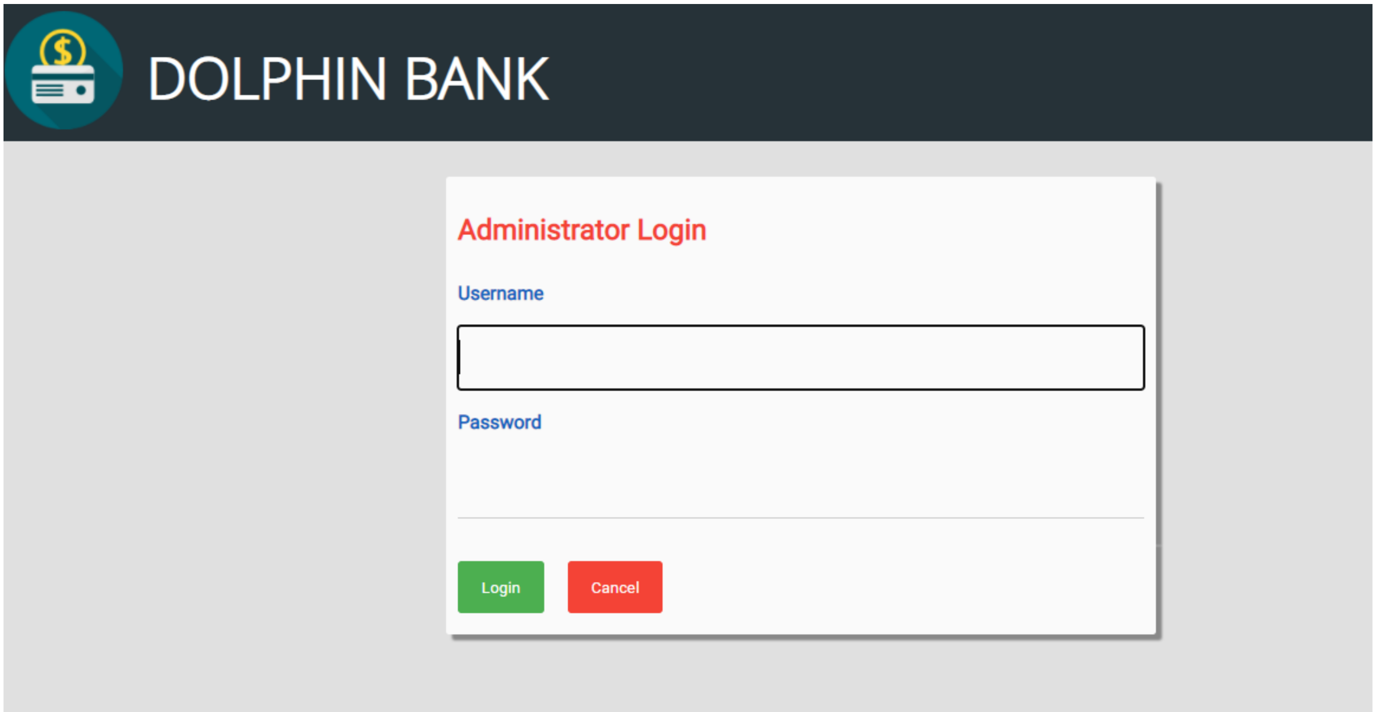
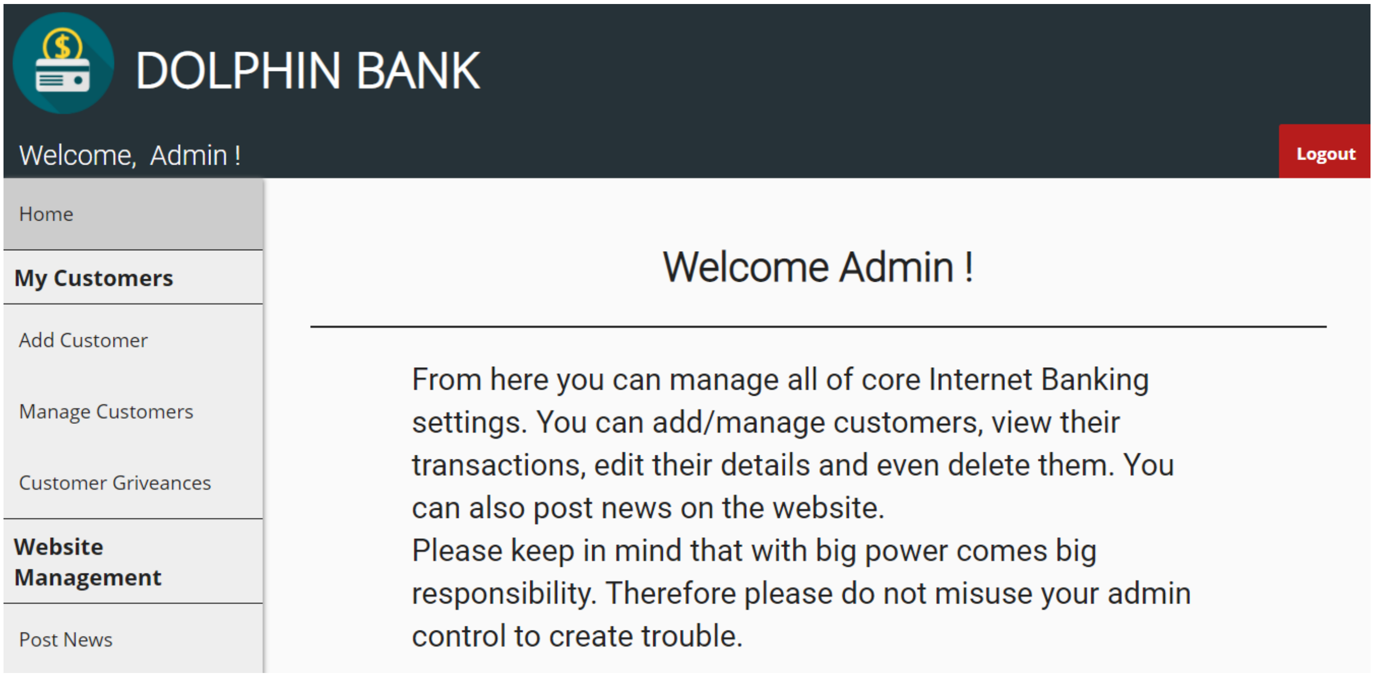


Figure 2.1 Admin page

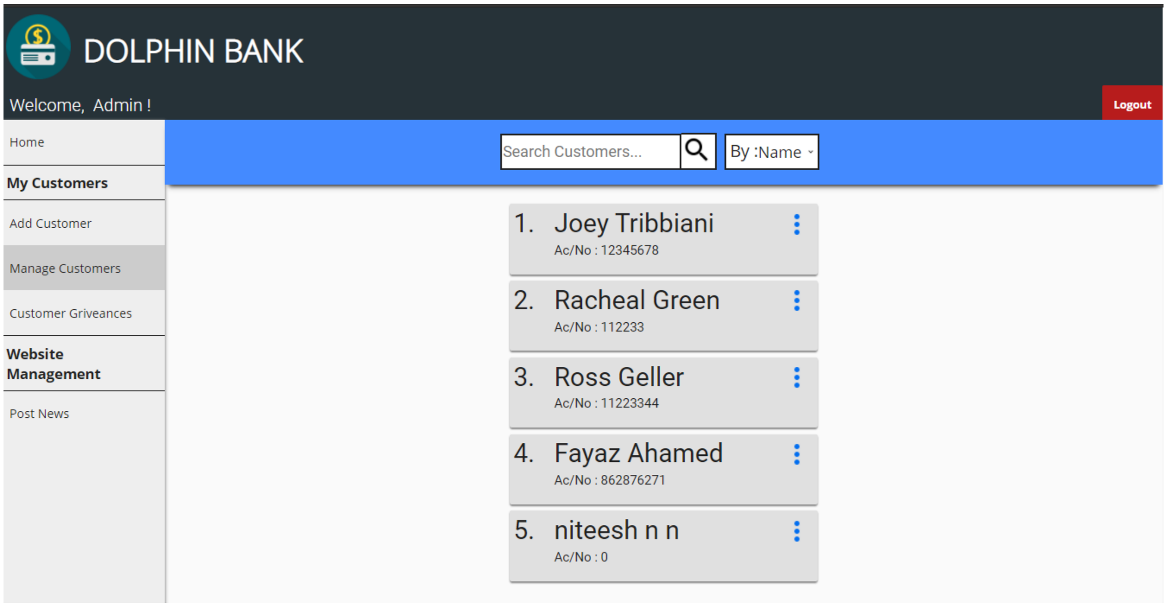


Welcome Admin !

From here you can manage all of core Internet Banking settings. You can add/manage customers, view their transactions, edit their details and even delete them. You can also post news on the website.

Please keep in mind that with big power comes big responsibility. Therefore please do not misuse your admin control to create trouble.

Fig 2.2 Admin Home page.



1. Joey Tribbiani
Ac/No : 12345678

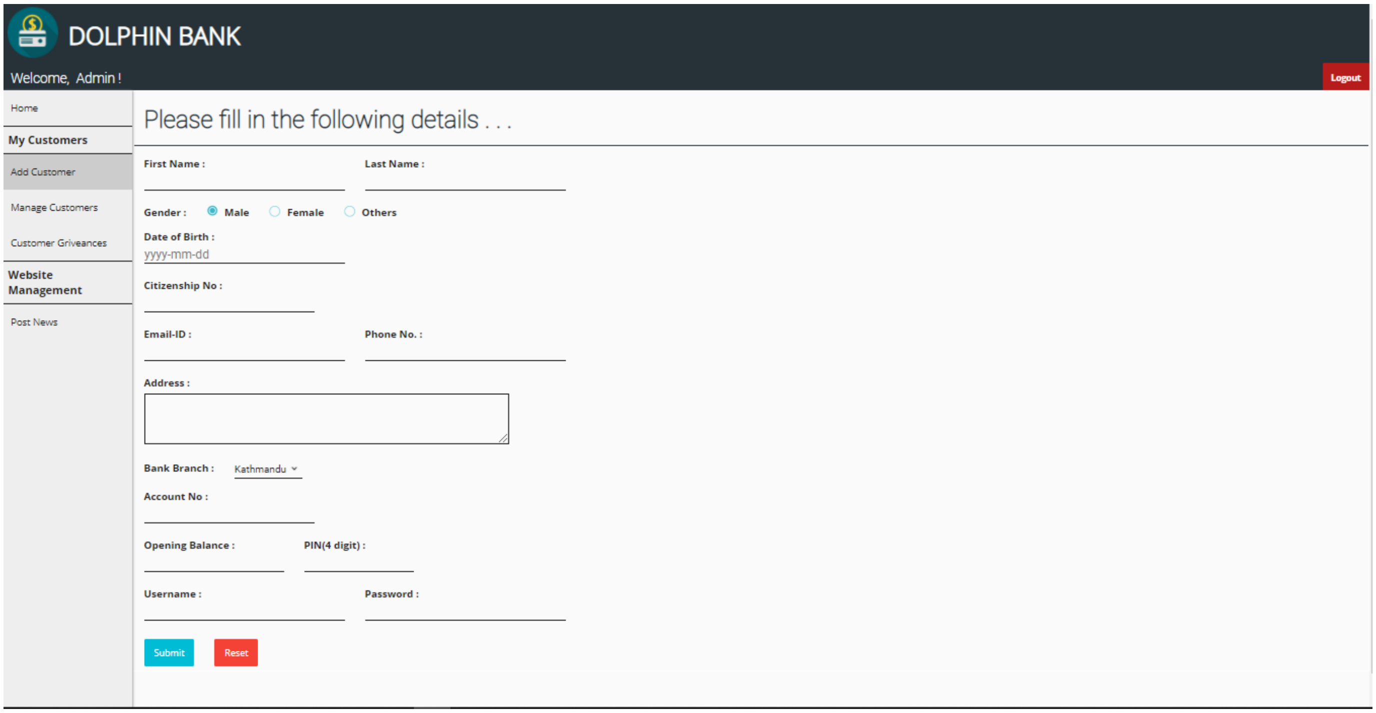
2. Racheal Green
Ac/No : 112233

3. Ross Geller
Ac/No : 11223344

4. Fayaz Ahamed
Ac/No : 862876271

5. niteesh n n
Ac/No : 0

Figure 2.3 Manage Customers



Please fill in the following details . . .

First Name :
Last Name :
Gender : ● Male ○ Female ○ Others
Date of Birth : yyyy-mm-dd
Citizenship No :
Email-ID :
Phone No. :
Address :
Bank Branch : Kathmandu
Account No :
Opening Balance :
PIN(4 digit) :
Username :
Password :

Figure A.2.4 Add Customer.

REFERENCES

[1]. “Banking on Cloud”, Daniel Benton and Walid Negm, 2010.

[2]. Farzad Sabahi, “Cloud Computing Security Threats and Responses”, Faculty of Computer Engineering Azad University, 2001 IEEE.

[3]. Chang-Lung Tsai Uei-Chin Lin et, “Information Security Issue of Enterprises Adopting the Application of Cloud Computing”, Chinese Culture University, 2011 IEEE.

[4]. Farzad Sabahi, “Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges”, International Journal on Advances in ICT for Emerging Regions, September, 2011.

[5]. J. Brodkin. (2008). “Gartner Seven Cloud-computing Security Risks”. Resideat: http://www.networkworld.com/ news/200S! 07020Scloud.html.Gartner Incorporation, http://www.gartner.com/.

[6]. Ramgovind S., Eloff M.M., Smith E., “The Management of Security in Cloud Computing”, 978-1-4244-5495-2/10/ $26.00 ©2010 IEEE.

[7]. Cong Wang, Qian Wang, and Kui Ren, “Towards Secure and Effective Utilization over Encrypted Cloud Data”, 2011 31st International Conferenc e on Distributed Computing Systems Workshops, 2011 IEEE.

[8]. L. Zhu “Microsoft Corporation”, B. Tung “Aerospace Corporation”, “Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)” June 2006.

Lance Spitzner (2002). “Honeypots Tracking Hackers”. Addison-Wesley. pp. 68-70. ISBN 0321108957.

[9]. Scarfone, Karen; Mell, Peter (February 2007). “Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center <marque> (National Institute of Standards and Technology) (800-94</marque>). Retrieved 1 January 2010.

[10]. Chang-Lung Tsai Uei-Chin Lin et, “Information Security Issue of Enterprises Adopting the Application of Cloud Computing”, Chinese Culture University, 2011 IEEE.