International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

Neo Banking using Containerized Application

Subramanian. E, Fayaz Ahamed. D, Niteesh. N, Mohammed Arish Rahuman. A

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 an Elastic Cloud Computing (EC2) Server on Amazon Web Service (AWS), which can be obtained by implemented by Web Socket using Application programming Interface (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 Representational State Transfer (REST), Hyper Text Transfer Protocol (HTTP), and Web Socket 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.

Keywords: AWS, Container, EC2, REST

I. INTRODUCTION

This 'Neo Banking' Project is a model Internet Banking. This enables the customers to perform the basic banking transactions by sitting at their office or at homes through PC or laptop or Mobile Phone. The customers can access the banks website for viewing their Account details and perform the transactions on account as per their requirements. With Internet Banking, the brick and mortar structure of the traditional banking gets converted into a click and portal model, thereby giving a concept of virtual banking a real shape. Thus, today's banking is no longer confined to branches. Neo banking facilitates banking transactions by customers round the clock globally.

The primary aim of this application is to provide an improved design methodology, which envisages the future expansion, and modification, which is necessary for a core sector like banking. This necessitates the design to be expandable and modifiable and so a modular approach is used in developing the application. Anybody who is an Account holder in this bank can become a member of online banking. He has to fill a form with his personal details and Account Number. All transactions are carried out online by transferring from accounts in the same Bank [4]. The application is meant to overcome the drawbacks of the manual system. The application has been developed using the most powerful and secure backend MS SQL Server and the most widely accepted web oriented as well as application oriented .PHP which is being deployed.

II. LITERATURE SURVEY

Although cloud computing models are ready to assist the banking sector in numerous ways, but the banking industry has serious concerns about their sustainability. Some of their integral and prominent concerns are security, privacy, confidentiality, data integrity, and authentication requirements, along with location of data, availability, and recoverability [2]. When a bank moves into cloud computing, there are two primary challenges that must be addressed. Security: The confidentiality and security of financial and personal data and mission-critical applications is paramount. Banks cannot afford the risk of a security breach. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions", according to Gartner. Many banking regulators require that financial data for banking customers stay in their home country. Certain compliance regulations require that data not be intermixed with other data, such as on shared servers or databases. As a result, banks must have a clear understanding of where their data resides in the cloud.

III. SYSTEM DESIGN

The first module is account creation for a new user. 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. 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. The withdrawal will be controlled by the rules of the account

The module also helps the account holders in transferring a particular sum of money from one particular account to another one through online facility. Here also, the amount transferred will be controlled by the rules of the account. The provides administrator to view all the details till to-date. It also contains money transaction details. authentication will be provided and deals with all the alerts to the bank through the message and e-mail once it is unverified. Web service is arguably the most exciting and innovate features of Microsoft's. NET initiative and they are likely to profoundly affect the way business interact using computer application. List of possible Web services is as varies as the list of possible business opportunities. Web service would typically perform a core business service such as user authentication, credit card validation, pricing a derivates security, placing a purchase order for a stock or pricing a same-day shipment well-defined interface.

Gartner's seven security issues which cloud clients should advert as mentioned below [5]:

1) **Regulatory Compliance**: Customers are responsible for the security of their data. Traditional service providers are subjected to external audits and security certifications,
2) **Privileged User Access**: There resides sensitive data that is processed outside the organization inherent risk of security of data because outsourced services bypass the "physical and logical IT controls",
3) **Data Location**: When users use the cloud, they have no knowledge about the hosted data. Distributed data storage is a main reason of cloud providers that can cause lack of control and that is risky for customers,
4) **Data Segregation**: As cloud is typically in a shared environment in that data can be shared. So there is the risk for data loss. Is encryption available at all stages, and were these encryption schemes designed and tested by experienced professionals?
5) **Recovery**: It is very essential to recover the data when some problem occurs and creates failure. So the main question arises here is that can cloud provider restore data completely or not? This issue can cause a stalemate in security,
6) **Investigative Support**: Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers,
7) **Long-term Viability**: Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available even after such an event.

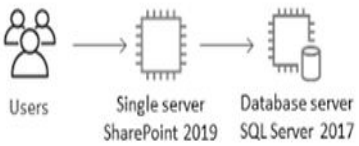
The following Fig.A.1depicts about the uses of single server by single user as follows,

Fig. A.1. Single user uses single server

IV. SYSTEM IMPLEMENTATION

Architecture of secure cloud for banking application authentication protocol that works on ticket basis and provides identity for secure authentication by which identity is proved by this protocol. EC2 uses symmetric key cryptography and requires a trusted third party during certain phases of authentication. Dynamic Firewall is used to protect the outsider attacks. Honey Pot is used to detect unauthorized use of data. These honey pots do not add direct value to a particular organization; instead, they are used to research the attacks for the organizations and used to protect against those attacks.

IDS i.e., intrusion detection system is used to monitor the network or policy violations and provide reports to management station. Some systems may attempt to stop an intrusion attempt but this is not required for monitoring a system.



A. Salt Algorithm:

In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard

passwords in storage. Historically a password was stored in plaintext on a system, but over time, additional safeguards were developed to protect a user's password against being read from the system. A salt is one such method. A new salt is randomly generated for each password. Typically, the salt and the password are concatenated and fed to a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password if the authentication data store is compromised. Note that due to this, salts don't need to be encrypted or stored separately from the hashed password itself, because even if an attacker has access to the database with the hash values and the salts, the correct use of said salts will hinder any effective attempt to crack the passwords. The following Fig.A.2 depicts about the salting password used for both encryption and decryption as follows,

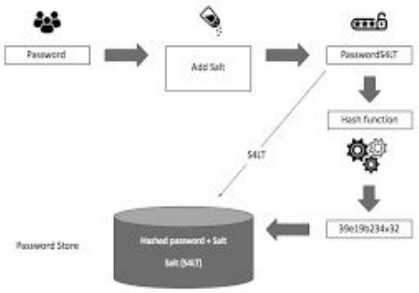


Fig.A.2. Salting Password (Encryption & Decryption)

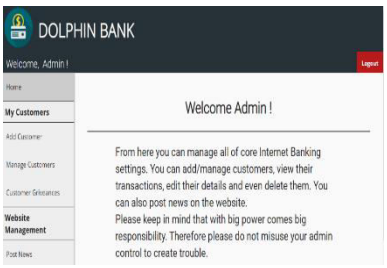
- **Containers**: Virtualization is an expanding technology in all areas of research and development. It has been widely accepted because of characteristics such as elasticity and flexibility in delivering on-demand resources. Nowadays, containers are a new form of virtualization and they have been highlighted as large technology companies are giving more support to them. Containers are a type of OS-level virtualization, in which the kernel allows the existence of multiple isolated instances.

- **EC2:** Explore the AWS Cloud for Free. 350+ Instance Types to Optimize Apps and Websites on EC2. Deploy Secure, Reliable, & Scalable Websites, Apps or Processes with Amazon EC2 for Free. Virtual Private Cloud. In-Memory Caching. Durable, Safe & Secure. Easy to Start.

- **Web Socket:** Using a Web Socket client attempt to connect to the remote Web Socket server. If the connection is allowed the Web Socket server may not be checking the Web Socket handshake's origin header. Attempt to replay requests previously intercepted to verify that cross-domain Web Socket communication is possible.

V. RESULTS AND DISCUSSIONS

The system study is the first phase in the system life cycle. It involves studying the ways an organization currently retrieves and process data to produce information with the goal of determining how to make it better. For this, system analyst should develop alternative system and evaluate each term of cost, benefit and feasibility. The term analysis, design and development are used in sequence, because in practice this sequence of steps used to construct computer-based information system. System analysis



includes the investigation and possible changes to the existing system. Analysis is used to gain an understanding of the existing system description and set of requirements for a new system. If there is no existing system, then analysis only defines the requirements. Development begins by defining a model of the new system and continues this model to a working system. The module of the system shows what the system must do to satisfy these' requirements. Finally, the data models are to a database and processed to user procedures and computer programs. These are depicted under Fig.A.3 as customer section as follows,

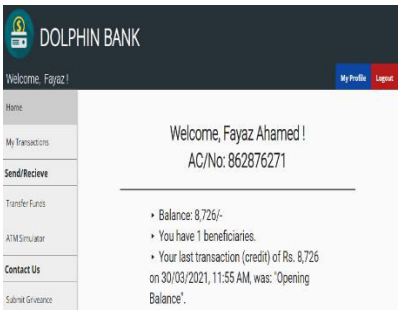


Fig.A.3. Customer Section

The present system consists of networking environment wherein regular activities are automated. However, activities like Demand Draft issues, Pay Order issues are done manually and corresponding registers updated manually. Further the status of a pay order whether the same has been honored or not cannot be accessed, in case, if required. Above all in manual system, only the man responsible for DD/Pay issue is aware of the various records to be updated on each transaction. Readability of the records, which are maintained manually, is also constrained in the present system. Since record are kept on a paper registers, again is also a problem. Further retrieving information from such records for a period is tedious, as the storage place restricts, old records will be kept off the disk. Also report generation of the various areas is done manually using great amount of manpower and time. These are depicted under Fig.A.4 as admin section as follows,

Fig A.4. Admin Section

VII. CONCLUSION AND FUTURE WORK

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. Corporate 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.

This research can be enhanced by improving the higher level by using Server less architecture and manages the large number of translations using Load Balancer with Payment Gateway. Improve the Business logics with higher level of the algorithms by modifying the existing algorithms on multiple containers by using the light weight instance of docker in REST API's.

REFERENCES

[1] Daniel Benton and Walid Negm, "Banking on Cloud", 2010.
[2] Farzad Sabahi, "Cloud Computing Security Threats and Responses", Faculty of Computer Engineering Azad University, 2001 IEEE.
[3] Chang-Lung Tsai Uei-Chin Lint, "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, "Gartner Seven Cloud-computing Security Risks", Reside at: http://www.networkworld.com/ news/200S! 07020Scloud.html.
[6] Gartner Incorporation, http://www.gartner.com/.
[7] Cong Wang, Qian Wang, and Kui Ren, "Towards Secure and Effective Utilization over Encrypted Cloud Data", 2011 31st IEEE International Conference on Distributed Computing Systems Workshops, 2011.
[8] L. Zhu "Microsoft Corporation", B. Tung "Aerospace Corporation", "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)" June 2006.
[9] Lance Spitzner, "Honey pots Tracking Hackers". Addison-Wesley. pp. 68-70. ISBN 0321108957.
[10] Scarfone, Karen; Mell, Peter, "Guide to Intrusion Detection and Prevention Systems (IDPS)", Computer Security Resource Center Retrieved 1 January 2010.