International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Money Transaction Security Using Cloud Computing and Blockchain

[1] Mr R .Vinoth Kumar, [2] A Joseph Raj, [3] C Mohamed Thofith, [4] S Jayaprakash.

[1] Asst. Professor, faculty of Information Technology, Rajiv Gandhi college of Engineering and Technology, Kirumampakam 607403.

[2,3,4] Department of Information Technology, Rajiv Gandhi college of Engineering and Technology, Kirumampakam 607403.

ABSTRACT : This application can be accessed and efficiently used by a server system with proper login enable. This project is based on client server architecture. In the server system some process can be accessed and others may be restricted. If the client login websites that can be accessed then the will be automatically opened. If the client login without using password and OTP and Image the blocklist generated then the process could not allow to access any transaction process and will monitor and send it to server system. As well as the client system will be screen locked and a OTP will be generated in the admin mail id. By using this OTP the clients system can be unlocked. In the server system the number of persons who have used restricted website will be calculated.

INTRODUCTION: Cloud computing, also on-demand computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort.

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently.

Cloud computing: Client–server model—Client–server computing refers broadly to any distributed application that distinguishes between service providers (servers) and service requestors (clients).[36]

- Grid computing—"A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks."

- Fog computing—Distributed computing paradigm that provides data, compute, storage and application services closer to client or near-user edge devices, such as network routers. Furthermore, fog computing handles data at the network level, on smart devices and on the end-user client side (e.g. mobile devices), instead of sending data to a remote location for processing.
- Dew computing—In the existing computing hierarchy, the Dew computing is positioned as the ground level for the cloud and fog computing paradigms. Compared to fog computing, which supports emerging IoT applications that demand real-time and predictable latency and the dynamic network reconfigurability, Dew computing pushes the frontiers to computing applications, data, and low level services away from centralized virtual nodes to the end users.
- Mainframe computer—Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as: census; industry and consumer statistics; police and secret intelligence services; enterprise resource planning; and financial transaction processing.
- Utility computing—The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity.
- Peer-to-peer—A distributed architecture without the need for central coordination. Participants are both suppliers and consumers of resources (in contrast to the traditional client–server model).

Key Characteristics : **Agility** improves with users' ability to re-provision technological infrastructure resources.

- **Cost** reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and need not be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house).[41] The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.
- **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
- **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.
- **Multitenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
  - **centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
  - **peak-load capacity** increases (users need not engineer for highest possible load-levels)
  - **utilisation and efficiency** improvements for systems that are often only 10–20% utilized.
- **Performance** is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Productivity** may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.
- **Reliability** improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, OS and cloud providers), without users having to engineer for peak loads. This gives the ability to

Service Model

Cloud Computing is a process in which nothing but a particular design of computing where everything from processing energy to infrastructure, company applications etc. are offered "as a service".

Cloud computing generally works on three types of architectures. These are: SAAS, PAAS and IAAS.

Software as a Service (SAAS)

Users are provided access to software and data source. Cloud providers handle the systems and facilities that run the programs.

Platform as a service (PAAS)

Cloud vendors provide a platform for computing, which includes the OS, coding language, execution environment, web server and the database. Developers can use the resources to build and run their software without buying expensive hardware.

Infrastructure as a service (IAAS)

Providers of IAAS offer computers – physical or virtual – and other resources. A good example of IAAS is dedicated servers provided by Web Hosting sites such as Bluehost, Hostgator etc.

Cloud computing is making everything simpler and flexible nowadays, but there is another important aspect which is Cloud architecture with robust security implementation is the key to cloud security. Cloud is complex and hence security measures are not simple too. Since it is new, it faces new security issues and challenges as well. Till date, most users don't trust storing their data on SASS-based cloud computing providers such as Dropbox, Skydrive and Google Drive etc. Since the outburst of Cloud Computing in the year 2006, various methods are devised to increase the security of the data being stored over Cloud Servers. Some of which include Encryption, Decryption, Data Partitioning, Digital Signatures etc.

EXISTING SYSTEM: This problem of this existing work, that we have analyzed the banking cloud server based storage services and its components .We have tried to find out the behavior of these mitigate attackers provide and challenges that they are facing.

ISSUES IN EXISTING SYSTEM : Lack of security of data,More man power,Time consuming,Consumes large volume of pare work,Needs manual calculations,No direct role for the higher officials,

Damage of machines due to lack of attention

PROPOSED SYSTEM : The rapid growth of security incidents and data breaches recently had risen concerns on Internet banking security issues. Existing Internet banking authentication mechanism that primarily relies on the conventional password-only authentication cannot efficiently resist to recent password guessing and password cracking attacks. To address this problem, this paper proposed an extended Honey Encryption (XHE) scheme by adding an additional protection mechanism on the existing user authentication mechanism. When the malicious user attempts to unauthorized access to online bank account by entering his guessed password, instead of rejecting the access and preventing them from using the application and keeping the information secured.

.

BENEFITS OF PROPOSED SYSTEM :

- Error detection and correction is very low and their resistance to fault attacks.
- SK(Secret key) and Common Randomness protocol may eventually become one of the most effective technologies for the development of various innovations in the field of network security.
- Easily to find the fault attackers and bug is free to verify it.

SYSTEM REQUIREMENTS

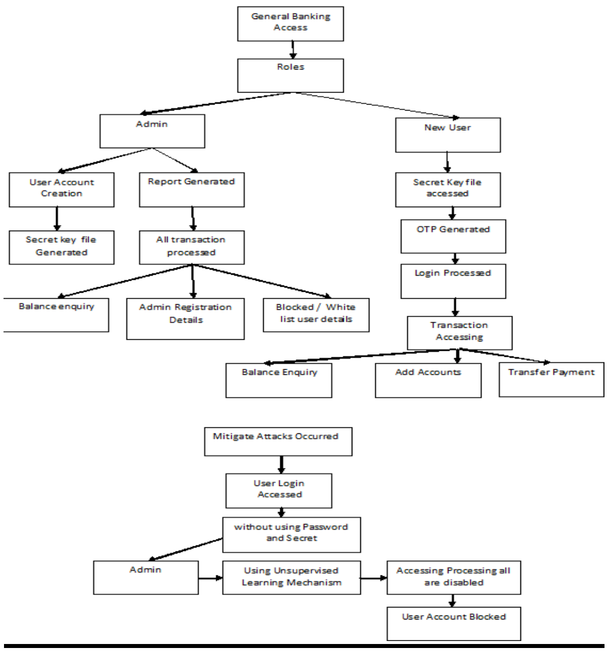
HARDWARE REQUIREMENTS :

Processor	-I3 Processor
Speed	-2.0 GHz
RAM capacity	-4 GB
Hard Disk	-500 GB

SOFTWARE REQUIREMENTS :

Operating System :	Windows '07
Back End :	My SQL 5. 0
Front End:	PHP MVC Framework
Cloud Hosting :	Gsuite Server (Google Cloud)

SYSTEM DESIGN :



MODULE DESCRIPTION

Admin and User Module:

The admin module will be used by the administrator of this portal, admin can access the customer registration. This module is having following functionalities.

Create New Account:

By using this functionality user can create a new account in any bank by selecting bank name option.

View Account Information:

By using this functionality user view all his account details, this can be viewed by users who are having account in any bank.

Transfer Amount:

By using this functionality user can transfer money from his account to other accounts of same bank or other banks.

Transaction Reports:

By using this functionality user can get all his transaction reports like accepted transactions, rejected transactions and pending transactions.

List of Customers:

By using this functionality Bank admin can get their entire customers list and their details.

List of Accounts:

By using this functionality Bank admin can get their entire customers list based on selected account type like saving account, current account etc.

New Accounts creation:

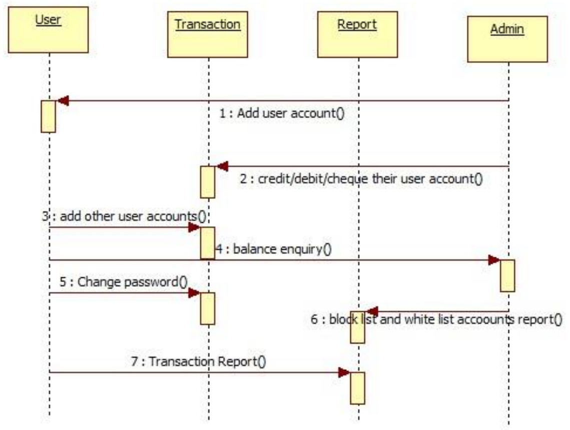
By using this functionality Bank admin can maintain entire user details who are requesting for new account in that bank.

Reports Module:

In this module administrator will get different types of reports regarding customers like Number of customers of this portal and banks registered in this portal. This module is controlled by administrator only.

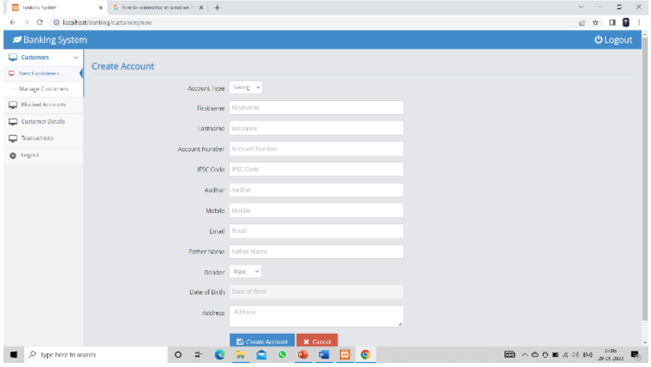
IMPLEMENTATION

Testing : The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.


User
Transaction
Report
Admin
1 : Add user account()
2 : credit/debit/cheque their user account()
3 : add other user accounts()
4 : balance enquiry()
5 : Change password()
6 : block list and white list accoounts report()
7 : Transaction Report()

SCREENSHOTS

Create New Account :

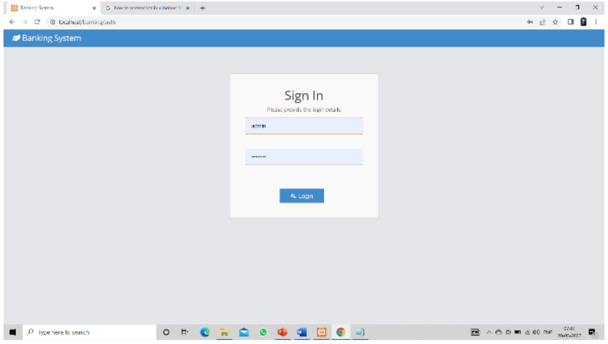

localhost/banking/customers/new

Banking System

Create Account

Account Type: Saving
Firstname
Lastname
Account Number
IFSC Code
Aadhar
Mobile
Email
Father Name
Gender: Male
Date of Birth
Address

Admin and User Module :


localhost/banking/auth

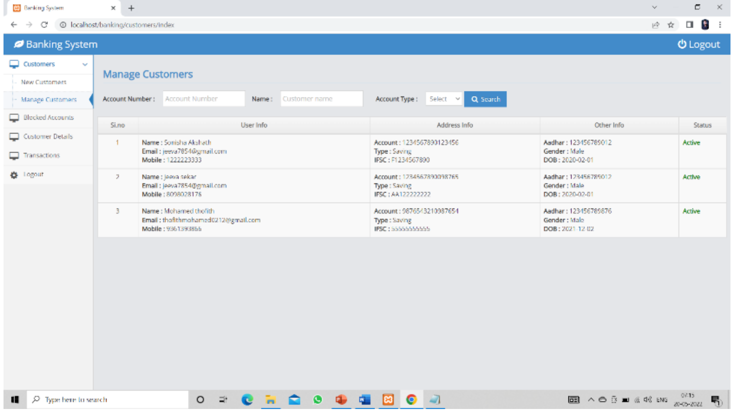
Banking System

Sign In

Please provide the login details

admin

View Account Information :


localhost/banking/customers/index

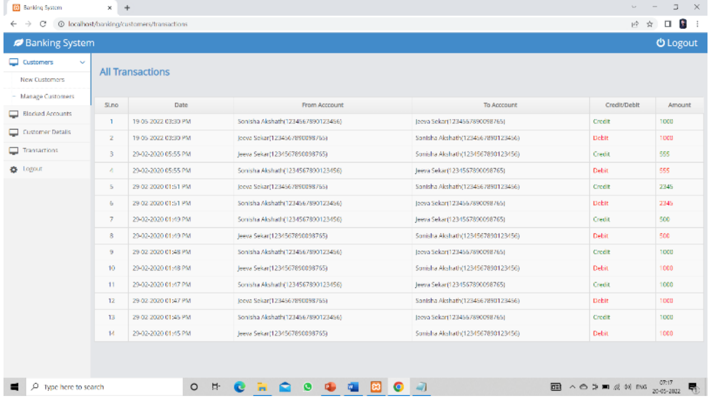
Banking System

Manage Customers

Account Number : Name : Account Type : Select

Si.no	User Info	Address Info	Other Info	Status
1	Name : Sonisha Akshath Email : jeeva7854@gmail.com Mobile : 1222223333	Account : 1234567890123456 Type : Saving IFSC : F1234567890	Aadhar : 123456789012 Gender : Male DOB : 2020-02-01	Active
2	Name : Jeeva sekar Email : jeeva7854@gmail.com Mobile : 8098028176	Account : 1234567890098765 Type : Saving IFSC : AA122222222	Aadhar : 123456789012 Gender : Male DOB : 2020-02-01	Active
3	Name : Mohamed thofith Email : thofithmohamed0212@gmail.com Mobile : 9361393866	Account : 9876543210987654 Type : Saving IFSC : 55555555555	Aadhar : 123456789876 Gender : Male DOB : 2021-12-02	Active

Transaction Reports :

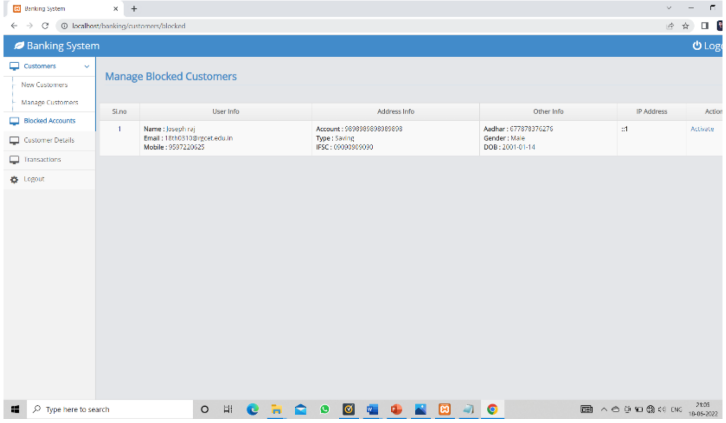

localhost/banking/customers/transactions

Banking System

All Transactions

Sl.no	Date	From Account	To Account	Credit/Debit	Amount
1	19-05-2022 03:30 PM	Sonisha Akshath(1234567890123456)	Jeeva Sekar(1234567890098765)	Credit	1000
2	19-05-2022 03:30 PM	Jeeva Sekar(1234567890098765)	Sonisha Akshath(1234567890123456)	Debit	1000
3	29-02-2020 05:55 PM	Jeeva Sekar(1234567890098765)	Sonisha Akshath(1234567890123456)	Credit	555
4	29-02-2020 05:55 PM	Sonisha Akshath(1234567890123456)	Jeeva Sekar(1234567890098765)	Debit	555
5	29-02-2020 01:51 PM	Jeeva Sekar(1234567890098765)	Sonisha Akshath(1234567890123456)	Credit	2345
6	29-02-2020 01:51 PM	Sonisha Akshath(1234567890123456)	Jeeva Sekar(1234567890098765)	Debit	2345
7	29-02-2020 01:49 PM	Sonisha Akshath(1234567890123456)	Jeeva Sekar(1234567890098765)	Credit	500
8	29-02-2020 01:49 PM	Jeeva Sekar(1234567890098765)	Sonisha Akshath(1234567890123456)	Debit	500
9	29-02-2020 01:48 PM	Sonisha Akshath(1234567890123456)	Jeeva Sekar(1234567890098765)	Credit	1000
10	29-02-2020 01:48 PM	Jeeva Sekar(1234567890098765)	Sonisha Akshath(1234567890123456)	Debit	1000
11	29-02-2020 01:47 PM	Sonisha Akshath(1234567890123456)	Jeeva Sekar(1234567890098765)	Credit	1000
12	29-02-2020 01:47 PM	Jeeva Sekar(1234567890098765)	Sonisha Akshath(1234567890123456)	Debit	1000
13	29-02-2020 01:45 PM	Sonisha Akshath(1234567890123456)	Jeeva Sekar(1234567890098765)	Credit	1000
14	29-02-2020 01:45 PM	Jeeva Sekar(1234567890098765)	Sonisha Akshath(1234567890123456)	Debit	1000

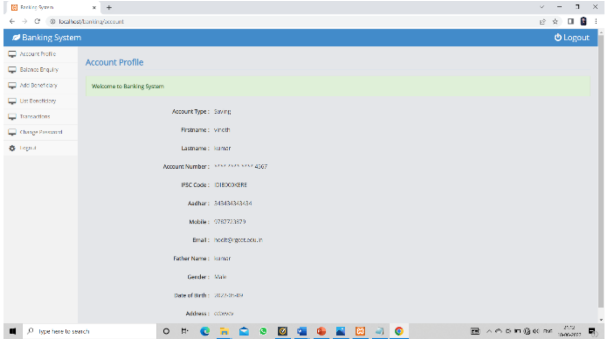
Reports Module:



Manage Blocked Customers

Si.no	User Info	Address Info	Other Info	IP Address	Action
1	Name : Joseph raj Email : 18th0310@rgcet.edu.in Mobile : 9597220625	Account : 9898989898989898 Type : Saving IFSC : 09090909090	Aadhar : 677878376276 Gender : Male DOB : 2001-01-14	::1	Activate

View Account Information :



Account Profile

Welcome to Banking System

Account Type : Saving
Firstname : vinoth
Lastname : kumar
Account Number : XXXX XXXX XXXX 4567
IFSC Code : IDIB000KERE
Aadhar : 343434343434
Mobile : 9787723879
Email : hodit@rgcet.edu.in
Father Name : kumar
Gender : Male
Date of Birth : 2022-05-09
Address : cdcwcv

CONCLUSION : The SK generation protocol which is introduced in this work uses a two phase approach to achieve the given SK rate. In the first step, the user estimates her state and sends this along with other information which is obtained from her observation to Admin. Although, this information is also received by Admin it is shown that the strong secrecy and uniformity of the generated SK is still guaranteed. In the second step, user uses this information including the estimated state of the owner to generate the SK. A Secret key is a capacity of a finite compound source is derived as a function of the communication rate parameter between user and admin. This result is further extended to a multi-letter SK capacity formula by discarding the public communication rate constraint. As the final result, a single-letter SK capacity formula is derived for degraded compound sources with no communication constraint and an arbitrary (possibly infinite) set of source states. It is shown that for any infinite compound source, with finite marginal set of states, there exists an approximating finite source whose SK generation protocol also guarantees the achievability of the given rates for the infinite source**.**

REFERENCE :

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, “Simultaneous hardcore bits and cryptography against memory attacks,” in Proc. 6th Theory Cryptography Conf., 2009, pp. 474–495.

[2] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in Proc. 9th Int. Conf. Theory Appl. Cryptol., 2003, pp. 452–473.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, “Certificate based (linkable) ring signature,” in Proc. Inf. Security Practice Experience Conf., 2007, pp. 79–92.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, “Malicious KGC attacks in certificateless cryptography,” in Proc. 2nd ACM Symp. Inf., Comput. Commun. Security, 2007, pp. 302–311.

[5] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1998, pp. 127–144.

[6] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.