

VERIFICATION BY FIGURE PIXEL COMPARISON FOR SECURED AUTHENTICATION ON CLOUD

at

**Sathyabama Institute of Science and Technology
(DEEMED TO BE UNIVERSITY)**

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering Degree in Computer Science and Engineering

By

**PAVANKALYAN MANDALA
(Reg.No.37110556)**



**DEPARTMENT OF COMPUTER SCIENCE AND
ENGINEERING SCHOOL OF COMPUTING
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU**

APRIL 2021



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

(Established under Section 3 of UGC Act, 1956)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI- 600119

www.sathyabamauniversity.ac.in



SCHOOL OF COMPUTING

BONAFIDE CERTIFICATE

This is to certify that the project Report is the bonafide work of **PAVANKALYAN MANDALA (Reg. No. 37110556)** who carried out the project entitled **"VERIFICATION BY FIGURE PIXEL COMPARISON FOR SECURED AUTHENTICATION ON CLOUD"** under our supervision from Dec 2020 to Mar 2021.

Internal Guide

Dr. R. AROUL CANESSANE, M.E., Ph.D.,

Head of the Department

Dr. S.VIGNESHWARI, M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I PAVANKALYAN MANDALA (Reg. No. 37110556), hereby declare that the Report on"VERIFICATION BY FIGURE PIXEL COMPARISON FOR SECURED AUTHENTICATION ON CLOUD" done under the guidance of Dr.M.MAHESWARI, M.E., Ph.D., at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDAT

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my tanks to **Dr. T.SASIKALA, M.E., Ph.D.,Dean, School of Computing** **Dr. S.VIGNESHWARI, M.E., Ph.D.,** and **Dr. L.LAKSHMANAN, M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. M. MAHESWARI, M.E., Ph.D.,** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the Department of **Computer Science and Engineering** who were helpful in many ways For the Completion of the project.

ABSTRACT

E-Banking is a course of movement of agencies given by using a gathering of sorted out bank places of work. Through web user can access their account from anywhere in the world. Recognition of valid client is a major problem in E-banking. The security issue arises due to unavoidable hacking of banking web. Duplicate websites is a kind of online data misrepresentation that expects to take confidential data, like e keeping cash passwords and cash transaction data from user. OPT based verification is a standout amongst the most broadly utilized techniques to verify a client before allowing gets to anchored sites. This type of verification is easy for hacking. Hence we propose a framework having figure pixel comparison for user validation based on blocking chain process. In proposed system for every currency surrendered by the client we produce an ID for each money, when the any sum of amount is transferred the ID of the currencies will only be transferred so we can track the way of the cash going around. The growth of internet storing money and web based business frameworks has prompted a gigantic increment in the quantity of usernames and passwords oversaw by singular clients and The Text based password uses username and password. So recalling of password is necessary which may be a difficult one and easy for hacking. Graphical password are generally easier to be remembered than text; user can set images as their password. Therefore graphical password has been proposed by many researchers as an alternative to text based password. Implementation of Link chain graphical password which uses circular tolerance makes the system more secured than existing.

TABLE OF CONTENTS

Chapter No.	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	viii
	LIST OF ABBREVIATIONS	ix
1	INTRODUCTION	1
	1.1 SCOPE OF THE PROJECT	2
	1.2 NEED OF THE PROJECT	2
	1.3 OBJECTIVE	3
2	LITERATURE SURVEY	4
3	METHODOLOGY	16
	3.1 EXISTING SYSTEM	16
	3.1.1 DISADVANTAGES	16
	3.2 PROPOSED SYSTEM	17
	3.2.1 ADVANTAGES	17
	3.3 SYSTEM REQUIREMENTS	18
	3.3.1 SOFTWARE REQUIREMENTS	18
	3.3.2 HARDWARE REQUIREMENTS	18
	3.4 SYSTEM DESIGN	18
	3.4.1 ARCHITECTURE DIAGRAM	18
	3.4.2 USE CASE DIAGRAM	19
	3.4.3 SEQUENCE DIAGRAM	20
	3.4.4 COLLABORATION DIAGRAM	21
	3.4.5 CLASS DIAGRAM	22
	3.4.6 ACTIVITY DIAGRAM	23
	3.4.7 DATA FLOW DIAGRAM	25
4	SYSTEM IMPLEMENTATION	27
	4.1 MODULE DESCRIPTION	27
	4.1.1 USER AUTHENTICATION	27
	4.1.2 SECURED LOGIN	27
	4.1.3 VARIOUS CURRENCIES	28

	ALLOCATE INITIAL CURRENICES	28
	TRANSFER OF DIGITAL CURRENCY ACROSS INDIVIDUALS	29
5	RESULTS AND DISCUSSION	30
	RESULTS AND DISCUSSION	30
6	FUTURE ENHANCEMENT AND CONCLUSION	33
	FUTURE EHANCEMENT	33
	REFERENCES	34
	APPENDIX	35
	A SOURCE CODE	35
	B PAPER WORK	40

LIST OF FIGURES

FIGURE No.	FIGURE NAME	PAGE No.
3.1	ARCHITECTURE DIAGRAM	19
3.2	USE CASE DIAGRAM	20
3.3	SEQUENCDE DIAGRAM	21
3.4	COLLABORATION DIAGRAM	22
3.5	CLASS DIAGRAM	23
3.6	ACTIVITY DIAGRAM	24

LIST OF ABBREVIATIONS

UML	UNIFIED MODELING LANGUAGE
SysML	SYSTEMS MODELLING LANGUAGE
JSP	JAVA SERVER PAGE
NDB	NEGATIVE DATABASE
PCFG	PROBABALISTIC CONTEXT FREE GRAMMARS

CHAPTER 1

INTRODUCTION

The use of computers and internet has become so pervasive so it influences all the banking sectors. Security has become the most important aspect in today's banking transaction system because banks are committed to provide secure core banking services to their customers. To achieve this goal authenticity of the users is required i.e. only the authorized users can take part in the transaction. Regarding this purpose banks use Biometrics based systems but due to unavoidable malicious activities database of the banking system is no longer secure. Smart hackers can fetch biometric details of customers from the bank's database and later can use it for fake transactions. To avoid all this catastrophic things image processing technique is used. Image processing is an efficient encryption scheme in which information hide inside the images and decrypted only by human visual system. In this paper we propose a secure XOR operation based image processing technique to secure bank authentication transaction. Here we consider the case of joint account operation. Generally, in banking sector Biometrics based authentication is used. Biometrics based authentication system operates by obtaining raw biometric data (e.g., Face image, Fingerprints etc.) from the subject, extracting feature set from the raw data and comparing the feature set against the blueprint stored in the database in order to authenticate the subject or to verify claimed identity. Security of any institute/organization depends on underlying design technology middle-ware and most of on the design of the database. Every transaction spatial or temporal has impact on the database. Therefore hackers always try to hack the database. The banking system while offering web enable core services major issue is authentication of the user. Many techniques are used for this purpose i.e. Password based authentication, Smart card based authentication, Biometric based authentication system. All these techniques are required to maintain database hence vulnerable for hacking. Database contains private information therefore there is possibility of privacy loss. Simplest form of Image processing or visual secret sharing scheme considers binary image as input and deals with each and every pixel independently. To encode a pixel of the secret image, we split the secret pixel into n versions in such a way that if all versions are printed on transparencies and superimposed the original secret pixel is revealed. This process has to be applied for entire secret image. Consequently n shares of original secret image are ready, to reveal the secret print the shares on transparencies and superimpose them. Proposed authentication method uses XOR operation based image processing techniques to ensure authentication as well as security of the information stored in the bank database.

SCOPE OF THE PROJECT

We provide the security in e-banking applications for customers. The access to account created in the account is done with graphical pixel comparison. Hence security is highly ensured and phishing can be eradicated. Use of bit coin helps to do the reduction of black money and transactions are monitored by the block chain concept.

NEED OF THE PROJECT

Individuals running peer-to-peer application are assigned a unique id address based on their computer's public key. It can be stored on an individual's computer in an encrypted "digital wallet." The corresponding private keys are used to send payments to other users. Unique addresses contain no personal information attached to it, and are somewhat anonymous. However, it is still possible to track a user using transaction history, which is public to all users. Users can own multiple addresses, and generate new ones, as generating them is equivalent to generating a public/private key pair. Digital currency is a work in progress, and lacks some features you probably consider important. It also has strange quirks and other issues that should be fixed, but nobody has yet had time to do so (there were always higher priorities). The Wallet code doesn't scale well. All transactions that were ever relevant to the wallet are loaded into memory, all the time, and re-written every time the wallet is saved. This results in a simple on-disk format accessible to many kinds of apps, but has poor performance for heavy users. In time we'll probably switch to a log structured wallet file format to solve this. A lot of these quirks persist because the primary goal of the project has always been to support SPV smartphone wallets, with other use cases being treated as secondary priorities. Hence making the Android wallet perform well has repeatedly evicted other features and refactoring. The strength in digital currency is that it is encrypted and safe regarding that it does not exist in physical form, like cash. The seriousness of Digital Currency has pushed a lot of organizations to create other Digital Currencies that also became popular and used.

OBJECTIVE

The main aim of the project is to make all the currency of each and every individual to be digitalized, so that we can avoid black money, this is achieved using the creation of digital coin. Every currency transformation will be tracked individually. It provides the secure authentication and identification.

CHAPTER 2

LITERATURE SURVEY

TITLE 1: A STUDY OF PROBABILISTIC PASSWORD MODELS

AUTHOR: Jerry Ma, Weining Yang, Min Luo, Ninghui Li

YEAR: 2014

DISCRIPTION:

A probabilistic password model assigns a probability value to each string. Such models are useful for research into understanding what makes users choose more (or less) secure passwords, and for constructing password strength meters and password cracking utilities. Guess number graphs generated from password models are a widely used method in password research. In this paper, we show that probability-threshold graphs have important advantages over guess-number graphs. They are much faster to compute, and at the same time provide information beyond what is feasible in guess-number graphs. We also observe that research in password modeling can benefit from the extensive literature in statistical language modeling. We conduct a systematic evaluation of a large number of probabilistic password models, including Markov models using different normalization and smoothing methods, and found that, among other things, Markov models, when done correctly, perform significantly better than the Probabilistic Context-Free Grammar model proposed in Weir et al. [25], which has been used as the state-of-the-art password model in recent research.

ADVANTAGES:

- Introduce probability-threshold graphs for evaluating password datasets.
- Introduce knowledge and techniques from the rich literature of statistical language modeling into password modeling.

DISADVANTAGES:

- Password-based authentication is that many users tend to choose weak passwords that are easy to guess.

TITLE 2: PERSONAL INFORMATION IN PASSWORDS AND ITS SECURITY IMPLICATIONS

AUTHOR: Yue Li, College of William & Mary, Haining Wang, University of Delaware, Kun Sun

YEAR: 2016

DISCRIPTION:

While it is not recommended, Internet users tend to include personal information in their

passwords for easy memorization. However, the use of personal information in passwords and its security implications have yet to be studied. In this paper, we dissect user passwords from several leaked datasets to investigate the extent to which a user's personal information resides in a password. Then we introduce a new metric called Coverage to quantify the correlation between passwords and personal information. Afterward, based on our analysis, we extend the Probabilistic Context-Free Grammars (PCFG) method to be semantics-rich and propose PersonalPCFG to crack passwords by generating personalized guesses. Through offline and online attack scenarios, we demonstrate that Personal-PCFG cracks passwords much faster than PCFG and makes online attacks much more likely to succeed. To defend against such semantics-aware attacks, we examine the use of simple distortion functions that are chosen by users to mitigate unwanted correlation between personal information and passwords.

ADVANTAGES:

- Introduce a new metric, Coverage, to accurately quantify the correlation between personal information and a password.
- Distortion functions are effective in defending against personal-information-related and semantics aware attacks.
- Personal-PCFG is significantly faster than PCFG in password cracking and eases the feasibility of mounting online attacks.

DISADVANTAGES:

- Human users are prone to choose weak passwords simply because they are easier to remember. As a result, most passwords are chosen within a small portion of the entire password space, leaving them vulnerable to bruteforce or dictionary attacks.
- Personal-PCFG generates personalized password guesses by integrating personal information in the guesses.

TITLE 3: OPASS: A USER AUTHENTICATION PROTOCOL RESISTANT TO PASSWORD STEALING AND PASSWORD REUSE ATTACKS

AUTHOR: Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin

YEAR: 2012

DISCRIPTION:

Text password is the most popular form of user authentication on websites due to its convenience and simplicity. However, users' passwords are prone to be stolen and compromised under different threats and vulnerabilities. Firstly, users often select weak passwords and reuse

the same passwords across different websites. Routinely reusing passwords causes a domino effect; when an adversary compromises one password, she will exploit it to gain access to more websites. Second, typing passwords into untrusted computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, keyloggers and malware. In this paper, we design a user authentication protocol named oPass which leverages a user's cellphone and short message service to thwart password stealing and password reuse attacks. oPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through oPass, users only need to remember a long-term password for login on all websites. After evaluating the oPass prototype, we believe oPass is efficient and affordable compared with the conventional web authentication mechanisms.

ADVANTAGES:

- A user authentication protocol named oPass which leverages cellphones and SMS to thwart password stealing and password reuse attacks.
- Users are free from typing any passwords into untrusted computers for login on all websites. Compared with previous schemes, oPass is the first user authentication protocol to prevent password stealing (i.e., phishing, keylogger, and malware) and password reuse attacks simultaneously.

DISADVANTAGES:

- Password-based user authentication has a major problem that humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe.
- Users tend to reuse passwords across various websites. Password reuse causes users to lose sensitive information stored in different websites if a hacker compromises one of their passwords. This attack is referred to as the password reuse attack.

TITLE 4: ARGON2: NEW GENERATION OF MEMORY-HARD FUNCTIONS FOR PASSWORD HASHING AND OTHER APPLICATIONS

AUTHOR: Alex Biryukov, Daniel Dinu, Dmitry Khovratovich

YEAR: 2016

DISCRIPTION:

We present a new hash function Argon2, which is oriented at protection of low-entropy secrets without secret keys. It requires a certain (but tunable) amount of memory, imposes prohibitive

time-memory and computation-memory tradeoffs on memory-saving users, and is exceptionally fast on regular PC. Overall, it can provide ASIC- and botnet-resistance by filling the memory in 0.6 cycles per byte in the non-compressible way.

ADVANTAGES:

- Make the design clear and compact, so that any feature and operation has certain rationale
- The clarity and brevity of the Argon2 design has been confirmed by its eventual selection as the PHC winner.

DISADVANTAGES:

- Remain the primary form of authentication on various web-services. Passwords are usually stored in a hashed form in a server's database. These databases are quite often captured by the adversaries, who then apply dictionary attacks since passwords tend to have low entropy.
- In the meanwhile, the password crackers migrated to new architectures, such as FPGAs, multiple-core GPUs and dedicated ASIC modules, where the amortized cost of a multiple-iterated hash function is much lower. It was quickly noted that these new environments are great when the computation is almost memoryless, but they experience difficulties when operating on a large amount of memory.

TITLE 5: NEGATIVE IRIS RECOGNITION

AUTHOR: Dongdong Zhao, Wenjian Luo, Senior Member, IEEE, Ran Liu, and Lihua Yue

YEAR: 2015

DISCRIPTION:

Elements of a person's biometrics are typically stable over the duration of a lifetime, and thus, it is highly important to protect biometric data while supporting recognition (it is also called secure biometric recognition). However, the biometric data that are derived from a person usually vary slightly due to a variety of reasons, such as distortion during picture capture, and it is difficult to use traditional techniques, such as classical encryption algorithms, in secure biometric recognition. The negative database (ndb) is a new technique for privacy preservation. Reversing the ndb has been demonstrated to be an np-hard problem, and several algorithms for generating hard-to-reverse ndbs have been proposed. In this paper, first, we propose negative iris recognition, which is a novel secure iris recognition scheme that is based on the ndb. We show that negative iris recognition supports several important strategies in iris recognition, e.g., shifting and masking. Next, we analyze the security and efficiency of negative iris recognition. Experimental results show that negative iris recognition is an effective and secure iris recognition scheme. Specifically, negative iris recognition can achieve a highly promising recognition

performance (i.e., gar=98.94% at far=0.01%, eer=0.60%) on the typical database casia-irisev3-interval.

ADVANTAGES:

- Negative iris recognition possesses the properties of irreversibility, revocability and renewability, and unlinkability.
- Several experiments are conducted, and the results show the effectiveness of negative iris recognition. Specifically, negative iris recognition achieves very good performance on a typical database

DISADVANTAGES:

- If biometric data are stored in plain-text, then once attackers break into those systems, they can obtain users' biometric data.
- An attacker could impersonate a valid user to access internal resources. Moreover, the attacker could use biometric data to break into other systems that the user has registered in, and he could damage the benefits to the valid users.

TITLE 6: A HYBRID OF THE PREFIX ALGORITHM AND THE 1-HIDDEN NDB ALGORITHM FOR GENERATING SINGLE NEGATIVE DATABASES

AUTHOR: Ran Liu, Wenjian Luo, Xufa Wang

YEAR: 2011

DISCRIPTION:

The negative database (NDB) is a complement of the corresponding database. The NDB cloud protect the privacy of the data, but it should be complete and hard-to-reverse. However, existent techniques cannot generate the complete and hard-to-reverse negative database. In this paper, a hybrid method is proposed to generate single negative databases. The proposed hybrid method includes two phases. Firstly, a complete negative database with a small size is generated by the transformation of the prefix algorithm. Secondly, a hard-to-reverse negative database, which is generated with the q-hidden method, is added into the small complete negative database. Therefore, the hybrid negative database is both complete and hard-to-reverse. Experiment results show that the NDB generated by the hybrid method is better than the NDB generated by the typical q-hidden method. Especially, the NDB generated by the q-hidden method can be reversed on average when the string length is 300. However, the NDB generated by the hybrid method cannot be reversed on average when the string length is 150.

ADVANTAGES:

- The technique can detect all illegitimate users without leaking out the passwords.

- The hybrid method makes sure that the hybrid-NDB is complete with the transformation of the prefix algorithm. Prefix algorithm is efficient in terms of time and space complexity, the NDB generated is easy to reverse.

DISADVANTAGES:

- The q-hidden-NDB is not complete, and it needs extra techniques (e.g. the error correcting code or encryption to get rid of superfluous strings not in original DB.
- The encryption and the decryption are not appropriate for some applications.

TITLE 7: THE SCIENCE OF GUESSING: ANALYZING AN ANONYMIZED CORPUS OF 70 MILLION PASSWORDS

AUTHOR: Joseph Bonneau

YEAR: 2012

DISCRIPTION:

We report on the largest corpus of user-chosen passwords ever studied, consisting of anonymized password histograms representing almost 70 million Yahoo! users, mitigating privacy concerns while enabling analysis of dozens of subpopulations based on demographic factors and site usage characteristics. This large data set motivates a thorough statistical treatment of estimating guessing difficulty by sampling from a secret distribution. In place of previously used metrics such as Shannon entropy and guessing entropy, which cannot be estimated with any realistically sized sample, we develop partial guessing metrics including a new variant of guesswork parameterized by an attacker's desired success rate. Our new metric is comparatively easy to approximate and directly relevant for security engineering. By comparing password distributions with a uniform distribution which would provide equivalent security against different forms of guessing attack, we estimate that passwords provide fewer than 10 bits of security against an online, trawling attack, and only about 20 bits of security against an optimal offline dictionary attack. We find surprisingly little variation in guessing difficulty; every identifiable group of users generated a comparably weak password distribution. Security motivations such as the registration of a payment card have no greater impact than demographic factors such as age and nationality. Even proactive efforts to nudge users towards better password choices with graphical feedback make little difference. More surprisingly, even seemingly distant language communities choose the same weak passwords and an attacker never gains more than a factor of 2 efficiency gain by switching from the globally optimal dictionary to a population-specific lists.

ADVANTAGES:

- A stricter password selection policy might produce distributions with significantly higher resistance to guessing.
- No practical amount of iterated hashing can prevent an adversary from breaking a large number of accounts given the opportunity for offline search.

DISADVANTAGES:

- Text passwords have been derided by security researchers ever since, with Multics evaluators singling passwords out as a weak point
- Which passwords are weak due to a lack of motivation or inherent user limitations

TITLE 8: CLEARSHOT: EAVESDROPPING ON KEYBOARD INPUT FROM VIDEO

AUTHOR: Davide Balzarotti, Marco Cova, and Giovanni Vigna

YEAR: 2008

DISCRIPTION:

Eavesdropping on electronic communication is usually prevented by using cryptography-based mechanisms. However, these mechanisms do not prevent one from obtaining private information through side channels, such as the electromagnetic emissions of monitors or the sound produced by keyboards. While extracting the same information by watching somebody typing on a keyboard might seem to be an easy task, it becomes extremely challenging if it has to be automated. However, an automated tool is needed in the case of long-lasting surveillance procedures or long user activity, as a human being is able to reconstruct only a few characters per minute. This paper presents a novel approach to automatically recovering the text being typed on a keyboard, based solely on a video of the user typing. As part of the approach, we developed a number of novel techniques for motion tracking, sentence reconstruction, and error correction. The approach has been implemented in a tool, called ClearShot, which has been tested in a number of realistic settings where it was able to reconstruct a substantial part of the typed information.

ADVANTAGES:

- The automatic recognition of the keys pressed by a person based on video information only is a very complex and challenging task, preventing this attack is easy.
- Text from a typing video could be reused and adapted to other fields, such as computer vision and augmented reality.

DISADVANTAGES:

- Encrypting the communication does not help in protecting one's physical environment, that is, the room the person is sitting in and sometimes the devices attached to one's computer
- In the past it has been a corpus of research devoted to exploring how to pry into someone's communication by exploiting the side effects of communication and the devices attached to someone's computer

TITLE 9: THE QUEST TO REPLACE PASSWORDS: A FRAMEWORK FOR COMPARATIVE EVALUATION OF WEB AUTHENTICATION SCHEMES

AUTHOR: Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano

YEAR: 2012

DISCRIPTION:

We evaluate two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deployability and security benefits that an ideal scheme might provide. The scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Our comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desired benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use. We conclude that many academic proposals have failed to gain traction because researchers rarely consider a sufficiently wide range of real-world constraints. Beyond our analysis of current schemes, our framework provides an evaluation methodology and benchmark for future web authentication proposals.

ADVANTAGES:

- It reflects the reality of a decentralized system like the Internet.
- Marginal gains are often not sufficient to reach the activation energy necessary to overcome significant transition costs.

DISADVANTAGES:

- Passwords are plagued by security problems and openly hated by users
- Other one is unbiased evaluation of password replacement schemes is complicated by the diverse

TITLE 10: THE PSYCHOLOGY OF SECURITY FOR THE HOME COMPUTER USER

AUTHOR: Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska , Zinta Byrne

YEAR: 2016

DISCRIPTION:

The home computer user is often said to be the weakest link in computer security. They do not always follow security advice, and they take actions, as in phishing, that compromise themselves. In general, we do not understand why users do not always behave safely, which would seem to be in their best interest. This paper reviews the literature of surveys and studies of factors that influence security decisions for home computer users. We organize the review in four sections: understanding of threats, perceptions of risky behavior, efforts to avoid security breaches and attitudes to security interventions. We find that these studies reveal a lot of reasons why current security measures may not match the needs or abilities of home computer users and suggest future work needed to inform how security is delivered to this user group.

ADVANTAGES:

- Costs are carefully assessed.
- Armed with such information, approaches to security can be more automated and personalizable: suited to the perceptions and capabilities of the person at the keyboard as well as giving them alternatives when their desired action

DISADVANTAGES:

- Worms and viruses have shown, even systems administrators are not diligent enough in applying patches to improve security
- Many home computer users do not adequately maintain their home systems to support security and often ignore or simply do not act in ways that would keep them secure.

CHAPTER 3

METHODOLOGY

EXISTING SYSTEM

- In existing framework, same clients have the various online records they are utilizing comparable passwords for that records.
- In that time the programmers where an enemy may assault a record of a client utilizing the same or comparable passwords of his/her different less delicate records.
- It is secure against secret word related assaults, as well as can oppose replay assaults, bear surfing assaults, phishing assaults, and information break episodes.
- The existing framework is simply cash exchange will be kept up in such a way like the aggregate sum to be exchanged and check of the rupees will be kept up.
- The above process is just used to keep up the amount of sum is exchanged from every single record this idea will be commendable if there should arise an occurrence of client see yet not to lessen the dark cash in the perspective of government.
- Different from existing works, we misuse dynamic verification accreditations alongside client driven access control to tackle the static qualification issue.
- In ordinary strategy in the event that you need to open one record implies we will give the username and give the watchword. So if it's conceivable someone else might be track our record detail.

DISADVANTAGES

- The security level of the current framework is low, so there might be shot of programmers may hacked our keeping money framework and gather the information.
- Difficult to keep up private subtle elements from programmer.
- Black cash exchange can't be distinguished.
- And they can't keep up exchange serial codes.

PROPOSED SYSTEM

- In proposed each and every trade out our application surrendered by the customer we will make the fascinating id for every cash.
- When the aggregate is traded from source to objective not only the entirety and count of the money will be taken despite that fascinating id will moreover be traded with the objective that we can track the method for the cash going around.
- If the outstanding id isn't in an upset then we can separate which is the last record it has entered and from that record it is subtle thusly we can keep up the inspecting.

- In this system we have displayed username, mystery word and give the precisely picked picture pixels. In case we are not picked alter motivation behind the photo pixels infers the photo is changed determinedly.
- Using this cryptographic systems the course for customer driven access control that restrains the risks of various ambushes.
- It design gives protection against various mystery word related strikes, for instance, bear surfing ambushes and direct observation attacks. The client is directly kept from using static usernames and passwords that can be seen by using warm imaging, or by recognizing the pressed keys using a mechanical vibration examination.

ADVANTAGES

- Here, we utilize progressed graphical verification strategy so it is exceptionally troublesome for other client to hacking.
- Data will be put away in encoded design so the security level turned out to be high.
- In the present framework, we keep up one of a kind code for each exchange.

SYSTEM REQUIREMENTS

Software Requirements:

Operating System	:	Windows 7 or Higher
Languages used	:	Java (JSP, Servlet), HTML
Tools	:	JDK 1.7, Net Beans 7.3.1, SQLyog
Backend	:	MySQL

Hardware Requirements:

Processor	:	Pentium Dual Core 2.3 GHz
Hard Disk	:	250 GB or Higher
Ram	:	2 GB

SYSTEM DESIGN

ARCHITECTURE DIAGRAM:

Here we have provided a clear architecture for our proposed system. Here the system works on two phase one is admin part and the user part. Admin can check the transaction, customer details and cash details. In the user part we stats with the creation of an individual bank account user data will be encrypted for security and before logging in the blocking chain is implemented for pixel comparisons. If the selected pixel matched then used is allowed to login. User can do transaction and while making money transfer an E-coin is generated randomly according to the note and amount is deposited to the account in the form of that e-coin key.

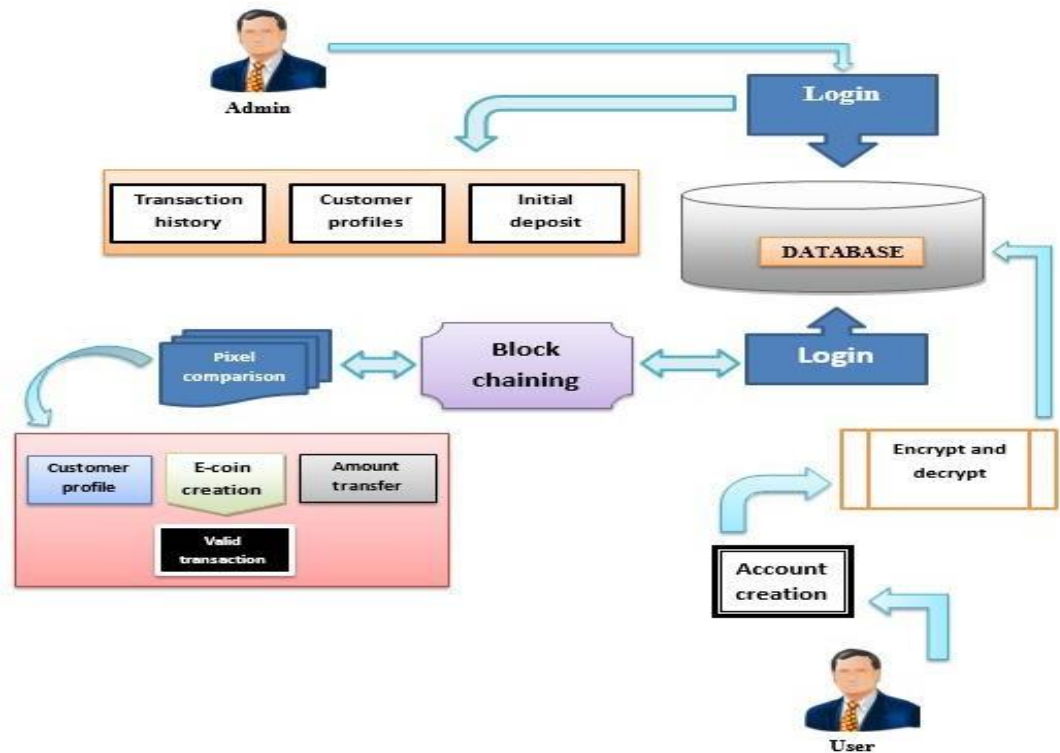


Fig : 3.1 ARCHITECTURE DIAGRAM

Use case diagram

In software and systems engineering, a **use case** is a list of steps, typically defining interactions between a role (known in UML as an "actor") and a system, to achieve a goal. The actor can be a human or an external system. In systems engineering, use cases are used at a higher level than within software engineering, often representing missions or stakeholder goals. The detailed requirements may then be captured in SysML or as contractual statements.

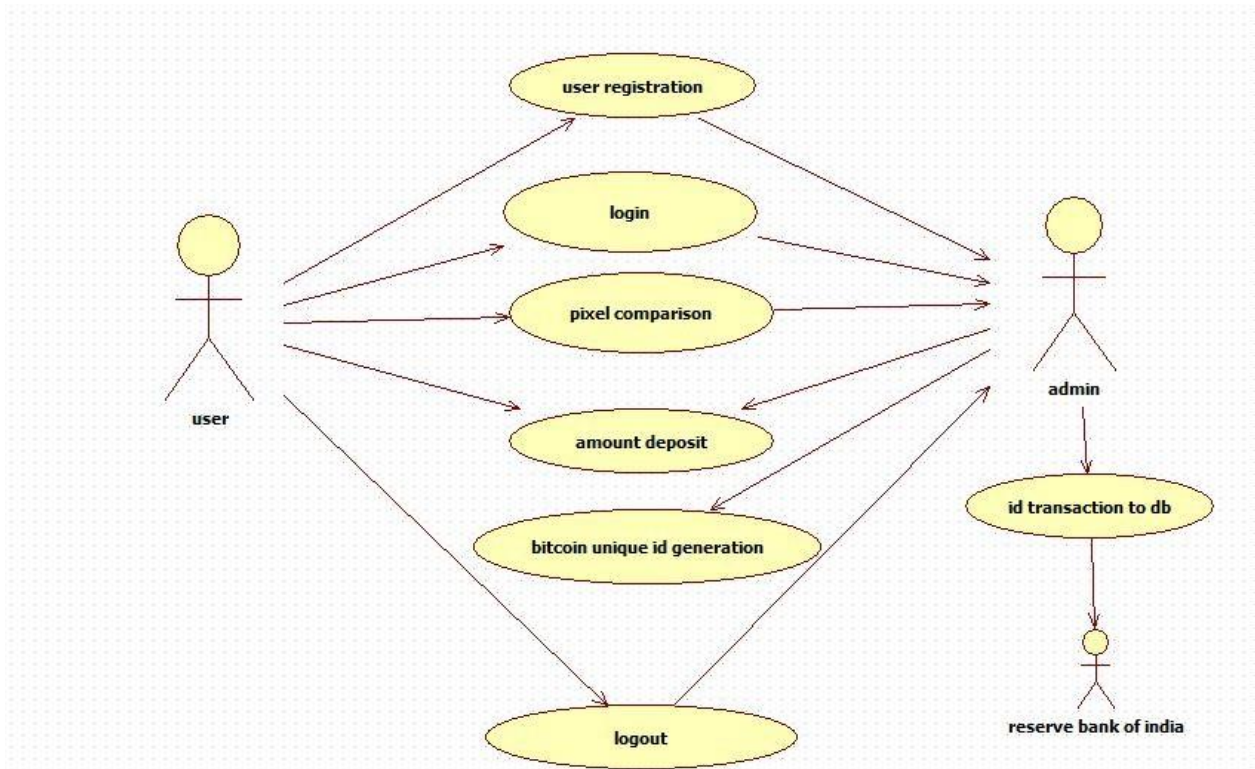


Fig : 3.2 Use case diagram

Sequence Diagram

A sequence diagram in a Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

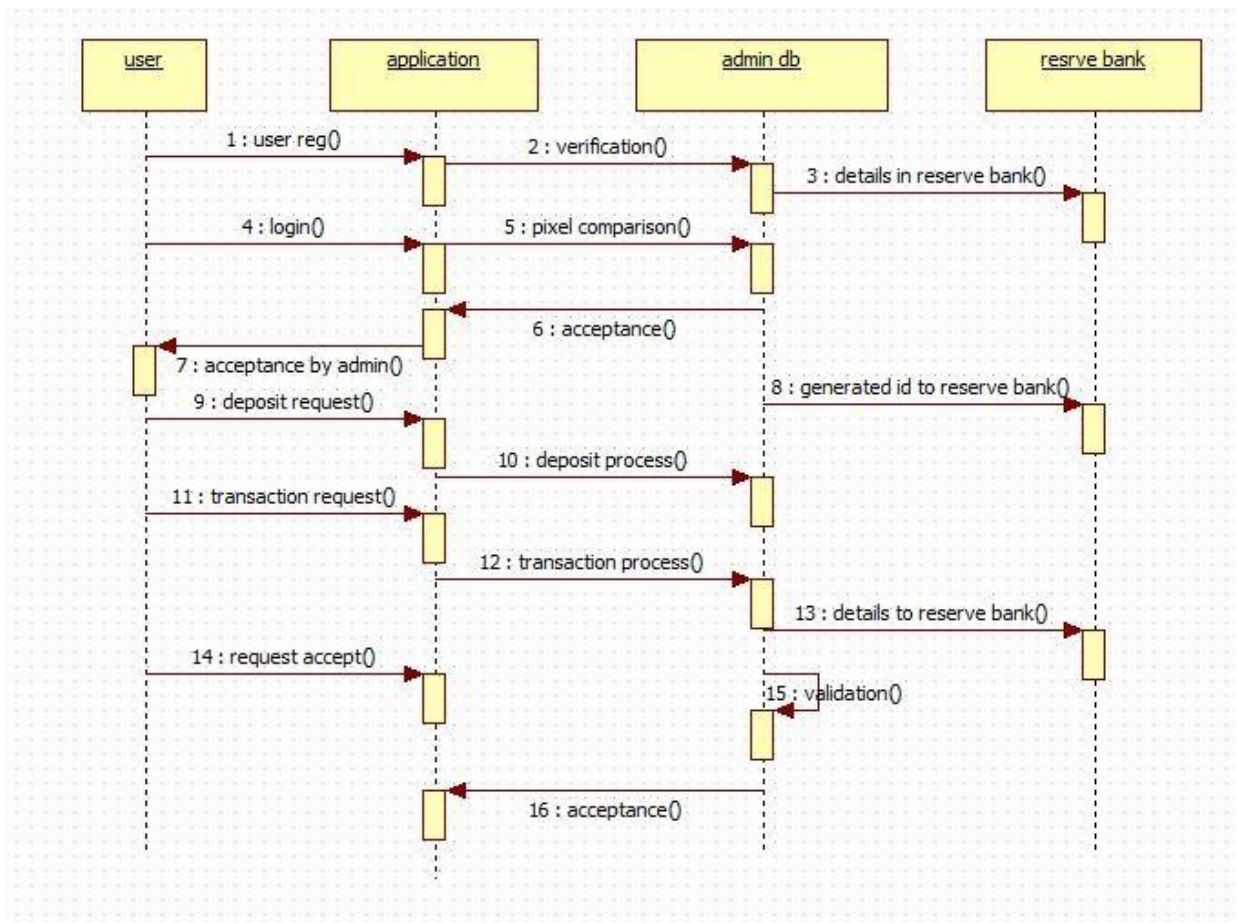


Fig : 3.3 Sequence Diagram

COLLABORATION DIAGRAM

A collaboration diagram, also called a communication diagram or interaction diagram, is an illustration of the relationships and interactions among software objects in the Unified Modeling Language (UML). The concept is more than a decade old although it has been refined as modeling paradigms have evolved. A collaboration diagram resembles a flowchart that portrays the roles, functionality and behavior of individual objects as well as the overall operation of the system in real time. Objects are shown as rectangles with naming labels inside. These labels are preceded by colons and may be underlined. The relationships between the objects are shown as lines connecting the rectangles.

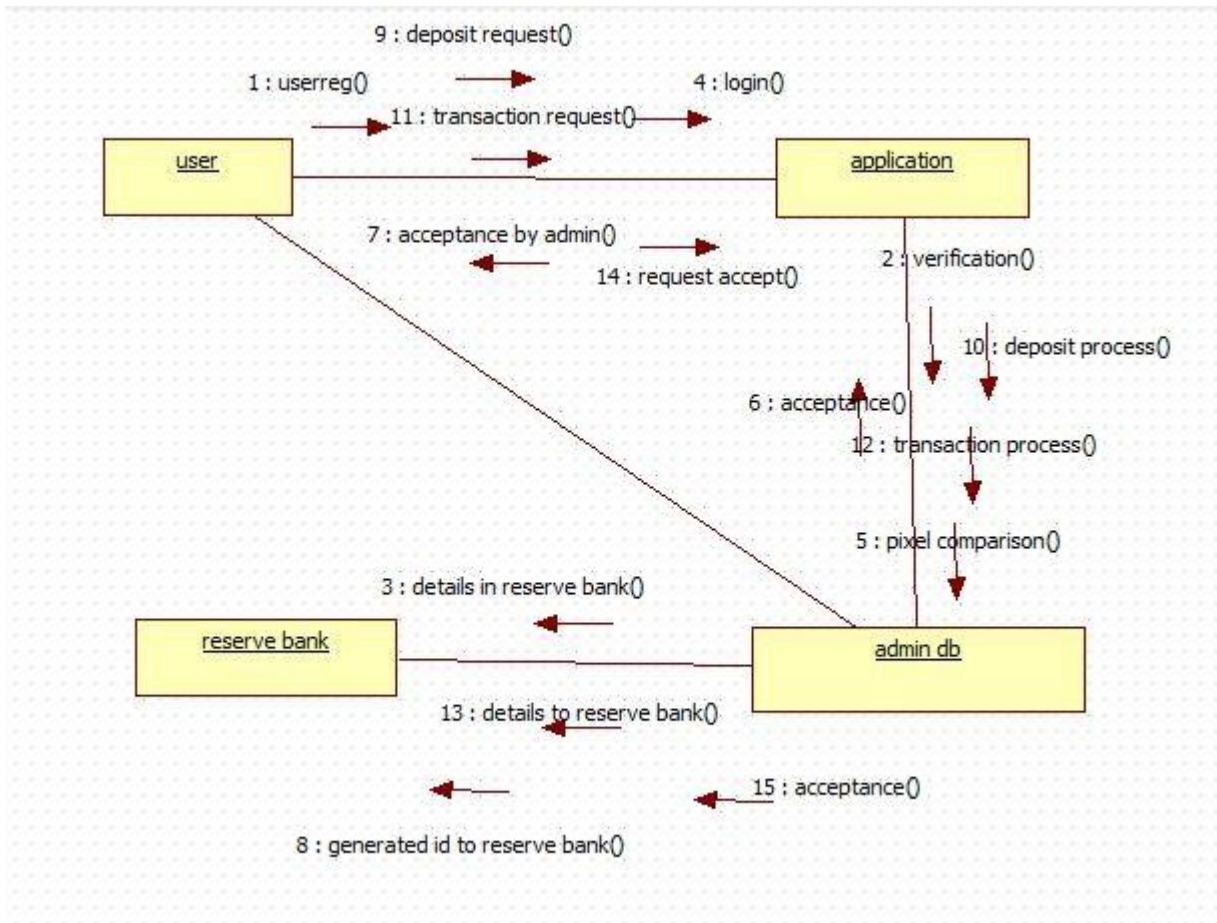


Fig : 3.4 COLLABORATION DIAGRAM

Class diagram

The class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing and documenting different aspects of a system but also for constructing executable code of the software application. The class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modelling of object oriented systems because they are the only UML diagrams which can be mapped directly with object oriented languages. The class diagram shows a collection of classes, interfaces, associations, collaborations and constraints. It is also known as a structural diagram. The purpose of the class diagram is to model the static view of an application. The class diagrams are the only diagrams which can be directly mapped with object oriented languages and thus widely used at the time of construction. The UML diagrams like activity diagram, sequence diagram can only give the sequence flow of the application but class diagram is a bit different. So it is the most popular UML diagram in the coder community.

So the purpose of the class diagram can be summarized as:

- Analysis and design of the static view of an application.
- Describe responsibilities of a system.

- Base for component and deployment diagrams.
- Forward and reverse engineering.

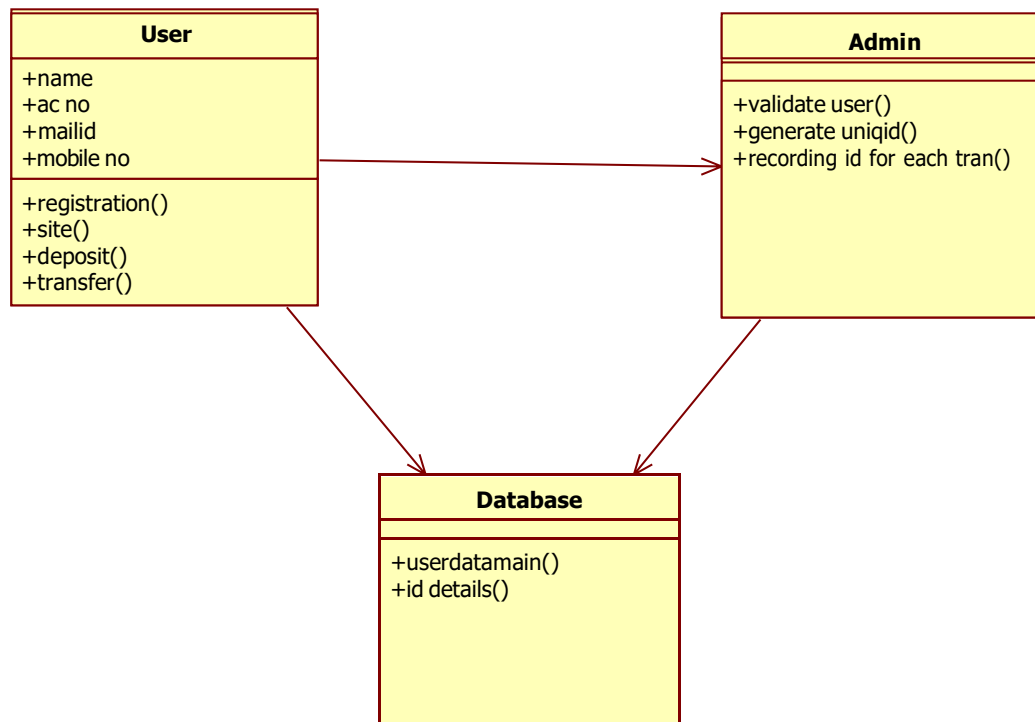


Fig : 3.5 Class diagram

Activity Diagram

Activity diagram is another important diagram in UML to describe dynamic aspects of the system. Activity diagram is basically a flow chart to represent the flow from one activity to another activity. The activity can be described as an operation of the system. So the control flow is drawn from one operation to another. This flow can be sequential, branched or concurrent. Activity diagrams deal with all types of flow control by using different elements like fork, join etc. The basic purposes of activity diagrams are similar to other four diagrams. It captures the dynamic behavior of the system. Other four diagrams are used to show the message flow from one object to another but activity diagram is used to show message flow from one activity to another. Activity is a particular operation of the system. Activity diagrams are not only used for visualizing dynamic nature of a system but they are also used to construct the executable system by using forward and reverse engineering techniques. The only missing thing in activity diagram is the message part. It does not show any message flow from one activity to another. Activity diagram is sometimes considered as the flow chart. Although the diagram looks like a flow chart but it is not.

So the purposes can be described as:

- Draw the activity flow of a system.

- Describe the sequence from one activity to another.
- Describe the parallel, branched and concurrent flow of the system.

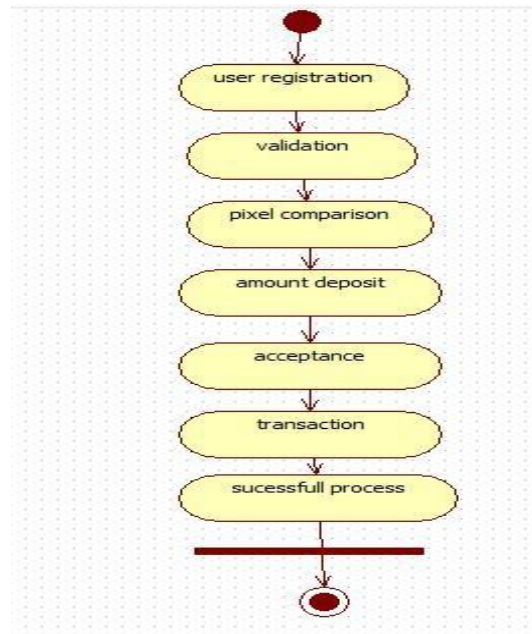
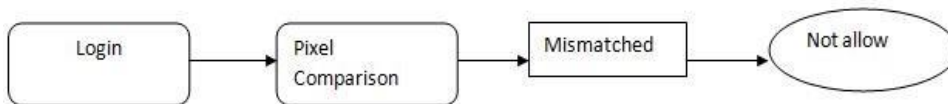


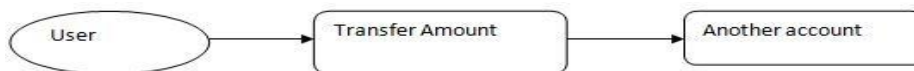
Fig : 3.6 Activity Diagram

DATA FLOW DIAGRAM:

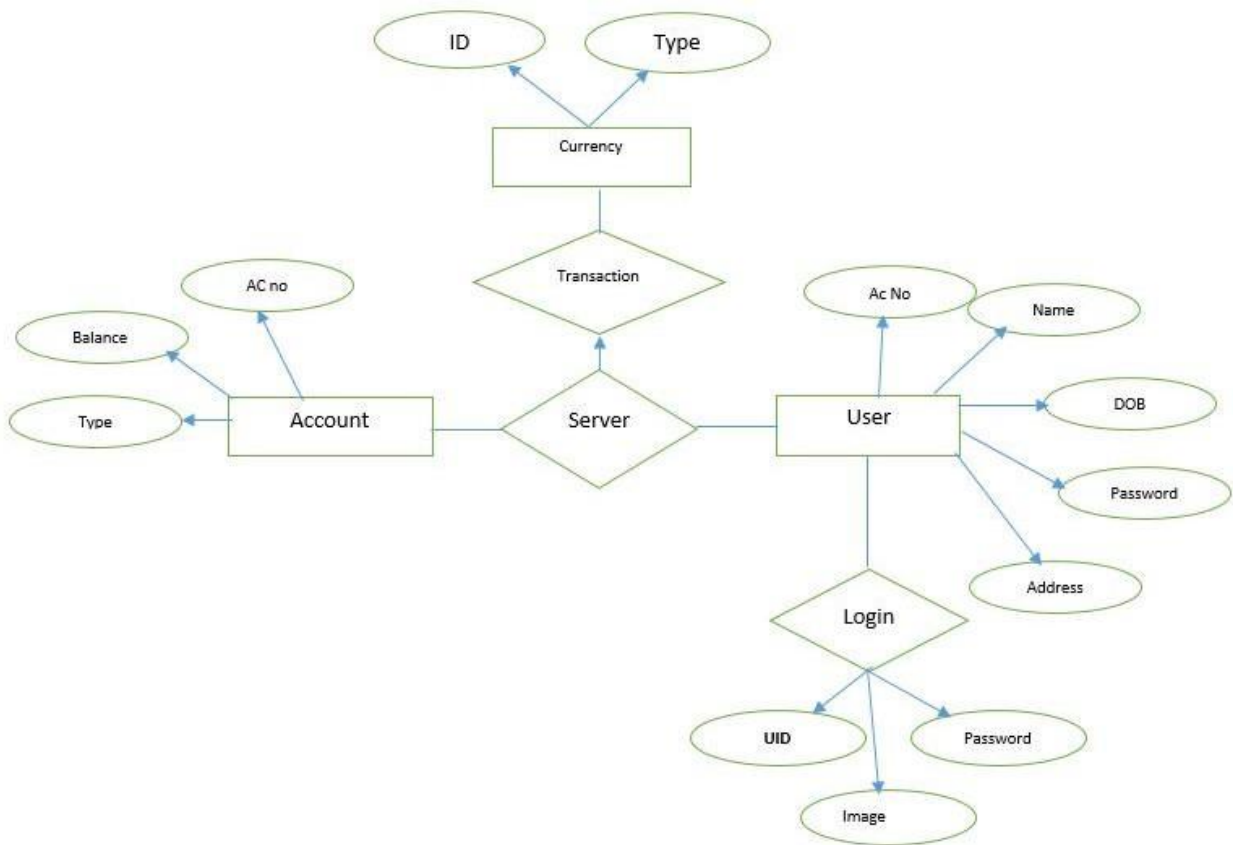
- **Level 0**



- **Level 1**



ER diagram



CHAPTER 4

SYSTEM IMPLEMENTATION

MODULES:

- User Authentication
- Secured login
- Various Currencies
- Allocate initial currencies to the individual
- Transfer of digital currency across individuals
- Tracking of currencies

MODULE DESCRIPTION

User Authentication:

Every last client login the page at that point makes the exchange and utilize this application. Validness is confirmation that a message, exchange, or other trade of data is from the source it cases to be from. Validness includes verification of character. We can check validness through confirmation. Enroll and login choice in landing page. Every single client needs to enlist as the new client for login. Client need to Fill the all prerequisite for security reason just, so fill the all subtle elements unique points of interest. Every one of the subtle elements spared in various ways. Make new table for every client and spare points of interest in like manner table. Those qualities utilized standardize and check for cash transmission preparing. Here to confirm the client points of interest for one time secret key sent to your enlisted mail id. At that point enter the way to confirm your subtle elements and can get to the page. Client accessible to see the adjust, see exchange history and make exchange of its own and client likewise see what number of cash they have.

Secured login

An effective and handy client confirmation conspire utilizing individual gadgets that use distinctive cryptographic natives, for example, encryption, advanced mark, pixel determination. The strategy profits by the broad utilization of figuring and different smart convenient gadgets that can empower clients to execute a safe verification convention. It keep up static username and secret key tables for distinguishing and confirming the authenticity of the login clients. Furthermore the picture pixel utilizing for to open the record. In the event that we are not pick

amend point picture implies the record won't open. It is secure technique.

Various Currencies:

That currencies concept one of the security layer for reduce the black money propagation. There are three various currencies model,

1. Two Thousand Currencies
2. Five Hundred Currencies
3. Hundred Currencies

That way isolates money in the E-Coin Application. The different cash demonstrate utilized special incentive for every rupee note and simple to recognize the rupees. That one of a kind esteem used to maintain a strategic distance from counterfeit cash in the cash transmission and furthermore simple to discover every rupee note is the place it now. That one of a kind esteem created naturally so every cash transmission is extremely secure. That extraordinary esteem is essential key so exceptional esteem can't produce same esteem. Every single client has part of cash and every single cash or money have unique id.

Allocate initial currencies to the individual:

This allots beginning monetary standards to the individual model just access consent to Admin. The Admin get to all procedure after the login with administrator validation subtle elements, generally can't get to the E-coin application. That administrator is put the underlying cash an incentive for every client. The Customer store cash in account implies at the time Admin produce the exceptional incentive for every money note. That one of a kind esteem warehouses on rupee note number and the amount of rupee note for instance two thousand or five hundred or hundred. After that store cash in client account. Administrator have an opportunity to check every single client's exchange points of interest and furthermore check the id of those monetary standards.

Transfer of digital currency across individuals:

Every single exchange made by client as it were. Client need to enter the right outsider record number and right name of payee. After that client needs to pick how much sum will exchange to the others and they pick what number of monetary standards have send from various kind of monetary standards like from Thousand Currencies, Five Hundred Currencies, and Hundred Currencies. At that point include the exchange date and time. Sum will be exchanged to the one client to other. The Currencies id will xchange or moved from one client table to payee account table. So we can without much of a stretch recognize the cash, which

client has those monetary forms. So we have recognized the dark cash and we can without much of a stretch diminish the dark cash populace. Advanced monetary forms will dependably be a less expensive fiscal frameworks to keep up and use than a fiat cash, in part when we think about the cost of scaling and security over the long haul, and on a worldwide scale. Because of the interesting development of computerized monetary standards from a security viewpoint, advanced monetary standards make almost flawlessly secure cash frameworks very still. Out of the crate, through cryptographic functionalities incorporated specifically with advanced cash conventions; they are extents more secure, proficient, and adaptable than fiat cash. Fiat cash must be guarded from counter-fitting, keeping money misrepresentation, note decimation, and physical robbery. Fiat cash will dependably be more costly to administration, utilize, and keep up in general money related framework than any sort of computerized money framework in light of those shortcomings and imperfections. Computerized monetary forms have more noteworthy security and versatility than their fiat partners also.

CHAPTER 5

RESULTS AND DISCUSSION

5.1 RESULTS AND DISCUSSION



Fig : 5.1 THIS PAGE OPENS WHEN THE PROJECT RUNS.

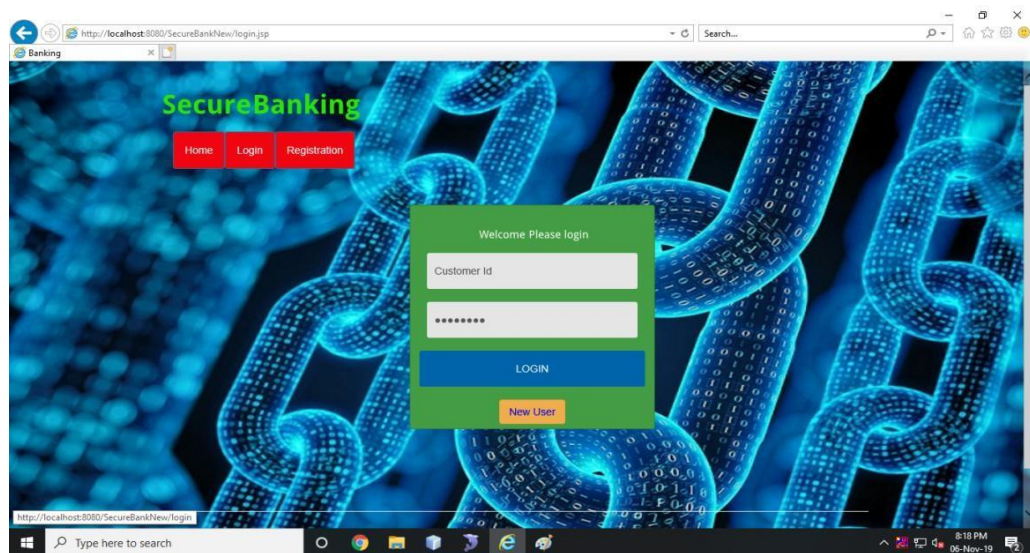


Fig : 5.2 USER CAN LOGIN USING THIS PAGE AFTER THE REGISTRATION COMPLETES.

The screenshot shows a web browser window with the URL `localhost:8080/SecureBankNew/registration.jsp`. The page features a navigation bar with 'Home', 'Login', and 'Registration' links. The main content area is a registration form titled 'Registration Form'. The form includes the following fields:

- First Name:** Input field with placeholder 'First Name'
- Last Name:** Input field with placeholder 'Last Name'
- Age:** Input field with placeholder 'Age'
- Date Of Birth:** Input field with placeholder 'dd-----y'
- Phone:** Input field with placeholder 'Phone'
- Branch Name:** Input field with placeholder 'Branch Name'
- Account NO:** Input field with placeholder 'Account Number'
- Email-id:** Input field with placeholder 'Email-id'
- Password:** Input field with placeholder 'Password'
- Confirm Password:** Input field with placeholder 'Confirm password'

The browser's taskbar at the bottom shows the Windows search bar and several application icons. The system clock indicates 8:21 PM on 06-Nov-19.

Fig : 5.3 NEW USER TO THIS BANK WILL REGISTER ALL THEIR DETAILS HERE.

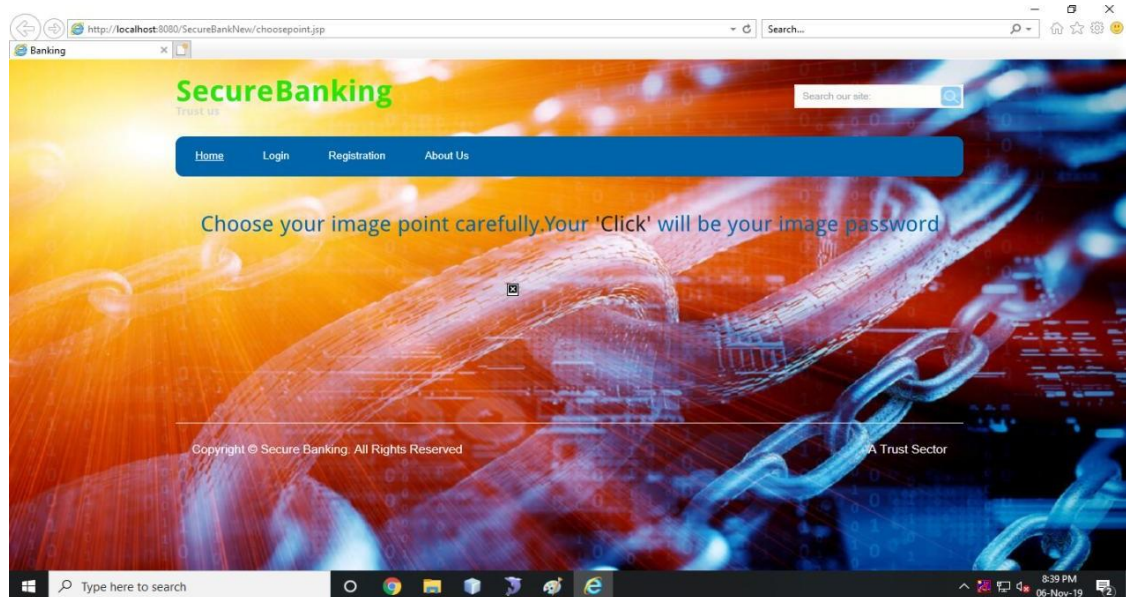


Fig : 5.4 HERE THE USER CAN SELECT THEIR PIXEL POINT TO GET LOGIN INTO THEIR ACCOUNT

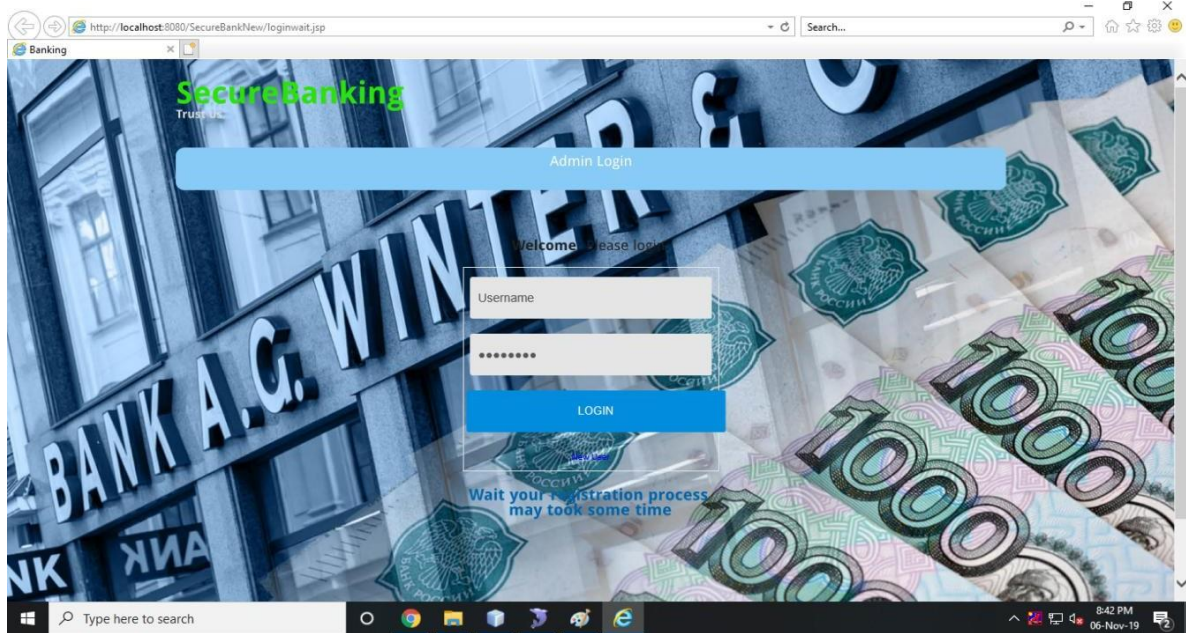


Fig : 5.5 THIS PICTURE REPRESENTS THAT ONLY THE ADMIN CAN LOGIN HERE WITH A PASSWORD.

Sender Account Number	Receiver Account Number	Sender Name	Receiver Name	Amount	Thousand	Five Hundred	
12345123451	12345678902	kumar	12345678902	3600	1	3	1
12345123451	12345678902	kumar	12345678902	3600	1	3	1
12345123451	12345678902	kumar	12345678902	3600	1	3	1
12345123451	12345678902	kumar	12345678902	3600	1	3	1
12345123451	12345678902	kumar	12345678902	3600	1	3	1
12345123451	12345678902	kumar	12345678902	3600	1	3	1
12345123451	12345678902	kumar	12345678902	3600	1	3	1
12345123451	12345678902	kumar	vignesh	3600	1	3	1
88088088001	12345123451	kj	kumar	3300	1	2	3

Fig : 5.6 COMPLETE TRANSACTIONS ALONG WITH THEIR DETAILS AND THE AMOUNT TRANSFERED CAN BE PROVIDED HERE

CHAPTER 6

FUTURE ENHANCEMENT AND CONCLUSION

CONCLUSION

This is the undertaking which can change the fiscal status of our country if it is executed by the hold bank and the significant research is going in light of the bit coin so our thought will be important for the pros. As an issue of first significance, we should need to inspect using lightweight cryptographic frameworks in our diagram. Second, we plan to analyze the blueprint of different customer driven access control models. Our proposed plan is definitely not hard to-learn and easy to-use since customers do nothing past entering one time username and affirmation code. By then select the pixel of picture, in case it is correct entering account for the most part pixels change reliably. The username, watchword is memory canny simple because customers of our arrangement don't have to review any secret at all. In perspective of the structure, our answer is versatile for customers since it diminishes the threat of username/mystery word reuse transversely finished various regions and organizations. Note that we are utilizing an individual contraption that is passed on by the customer as a general rule and the customer does not need to pass on an additional hardware or any physical inquiry for approval. This thought will be to a great degree profitable wherever all through the world in light of its extraordinary id age for each and every single note submitted to the system.

FUTURE ENHANCEMENT

Further enhancement can be done by making this system secure with the use of certificates for both merchant and customer and as technology changes new checks can be added to understand the pattern of fraudulent transactions and to alert the respective account holders and bankers when fraud activity is identified. The dataset available on day to day processing may become outdated, it is necessary to have updated data for effective fraud behavior identification.

REFERENCE:

1. J. Ma, W. Yang, M. Luo, and N. Li, "A study of probabilistic password models," in Proceedings of 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 689–704.
2. Y. Li, H. Wang, and K. Sun, "Personal information in passwords and its security implications," IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2320–2333, Oct. 2017.
3. H. M. Sun, Y. H. Chen, and Y. H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, Apr. 2012.
4. A. Biryukov, D. Dinu, and D. Khovratovich, "Argon2: New generation of memory-hard functions for password hashing and other applications," in Proceedings of 2016 IEEE European Symposium on Security and Privacy, Mar. 2016, pp. 292–302.
5. D. Zhao, W. Luo, R. Liu, and L. Yue, "Negative iris recognition," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 112–125, Jan. 2018.
6. R. Liu, W. Luo, and X. Wang, "A hybrid of the prefix algorithm and the q-hidden algorithm for generating single negative databases," in Proceedings of 2011 IEEE Symposium on Computational Intelligence in Cyber Security, Apr. 2011, pp. 31–38.
7. J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In Proceedings of IEEE Symposium on Security and Privacy, pages 538–552. IEEE, 2012
8. D. Balzarotti, M. Cova, and G. Vigna. Clearshot: Eavesdropping on keyboard input from video. In IEEE Security & Privacy, 2008.
9. J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In IEEE Security & Privacy, 2012.
10. A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In IEEE Security & Privacy, 2012.

APPENDIX

A. SOURCE CODE

```
package newpackage;

import DbConnection.DbConnection;
import java.io.IOException;
import java.io.InputStream;
import java.io.PrintWriter;
import static java.lang.System.out;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;
import java.sql.SQLException;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.HttpSession;
import javax.servlet.http.Part;

@WebServlet("/uploadServlet")
@MultipartConfig(maxFileSize = 16177215) // upload file's size up to 16MB
public class registration extends HttpServlet {
    private String dbURL = "jdbc:mysql://localhost:3306/bank";
    private String dbUser = "root";
    private String dbPass = "admin";

    protected void doPost(HttpServletRequest request,
        HttpServletResponse response) throws ServletException, IOException {
        String Name = request.getParameter("name");
        String last = request.getParameter("last");
        String age = request.getParameter("age");
        String sex = request.getParameter("sex");
```

```

String secondhold = request.getParameter("sec");
System.out.println(Name + " " + last);

InputStream photo = null;
InputStream photo1 = null;
Part profile = request.getPart("photo");
Part profile1 = request.getPart("photo1");
/*Part exper=request.getPart("experiencecert");
Part deg = request.getPart("degreecert");
Part pgc=request.getPart("pgcert");
Part ugc = request.getPart("ugcert");
Part dipc=request.getPart("diplomacert");
Part hsc = request.getPart("hscert");
Part sslcc=request.getPart("sslccert");
*/

if (profile != null) {
    System.out.println(profile.getName());
    System.out.println(profile.getSize());
    System.out.println(profile.getContentType());
    photo = profile.getInputStream();
}

if (profile1 != null) {
    System.out.println(profile1.getName());
    System.out.println(profile1.getSize());
    System.out.println(profile1.getContentType());
    photo1 = profile1.getInputStream();
}

Connection conn = null; // connection to the database
String message = null; // message will be sent back to client

try {

```

```

DriverManager.registerDriver(new com.mysql.jdbc.Driver());
conn = DriverManager.getConnection(dbURL, dbUser, dbPass);
Statement st = conn.createStatement();
ResultSet rs = st.executeQuery("select * from user where accountno=" + acc + "");
    if (photo != null) {

        statement.setString(2, last);
        statement.setString(3, password);
        statement.setString(4, cpass);
        statement.setString(5, dob);
        statement.setString(6, age);
        statement.setString(7, sex);
        statement.setString(8, email);
        statement.setString(9, addr);
        statement.setString(10, acc);
    }
    HttpSession hs = request.getSession();
    hs.setAttribute("accountno", acc);
    int row = statement.executeUpdate();
    int initail = 0;
    if (row > 0) {
        Statement smt = DbConnection.getConnection();
        smt.executeUpdate("insert into credit(accountnumber,creditamount,username)
values(" + acc + "," + initail + "," + Name + ")");
        String query1 = "CREATE TABLE IF NOT EXISTS " + acc + Name + " " +
"(Thousand varchar(100),FiveHundred varchar(100),Hundred varchar(100))";
        // String query2="CREATE TABLE IF NOT EXISTS "+s+uname+" " + "(Thousand
varchar(100),FiveHundred varchar(100),Hundred varchar(100))";
        smt.executeUpdate(query1);
        System.out.println("aaaaaaaaaaaaaaaaaaaaaaaaaaaaa" + query1);
    }
    if (row > 0) {
        message = "File uploaded uploadedand saved into database";
        RequestDispatcher rd = request.getRequestDispatcher("choosepoint.jsp");
    }

```

```

        rd.forward(request, response);
    }
}
} catch (SQLException ex) {
    message = "ERROR: " + ex.getMessage();
    ex.printStackTrace();
    out.print(ex);
} finally {
    if (conn != null) {

        try {
            conn.close();
        } catch (SQLException ex) {
            ex.printStackTrace();
        }
    }
}
}
}
}

```