COLLEGE OF ENGINEERING, THALASSERY

KANNUR DT.-670107

A MAJOR PROJECT REPORT ON

CLOUDSEC

Submitted in partial fulfilment of the requirements for the
Award of the degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE & ENGINEERING

By

PREMITH PRADEEP (Register No.:12152017)
JINSHA K (Register No.:12152042)
SWEYA P (Register No.:12152057)
VIDYA VALSALAN (Register No.:12152060)
SHAMNA K V (Register No.:12152064)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MARCH 2018

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COLLEGE OF ENGINEERING, THALASSERY

KANNUR DT.-670107

CERTIFICATE

This is to certify that the major project work entitled

CLOUDSEC

Submitted by

PREMITH PRADEEP (Register No.:12152017)
JINSHA K (Register No.:12152042)
SWEYA P (Register No.:12152057)
VIDYA VALSALAN (Register No.:12152060)
SHAMNA K V (Register No.:12152064)

Is a bonafide record of the work done by them in partial fulfilment of the requirements for the award of B.Tech Degree in Computer Science during the year 2018.

PROJECT CO-ORDINATOR **PROJECT GUIDE** **HEAD OF THE DEPARTMENT**

ACKNOWLEDGEMENT

Before we get into the thick of things we would like to add a few heart full words for the people who gave unending support right from the stage the idea of project was received. We express our deep sense of gratitude and sincere thanks to those who have helped us in developing this project.

Our first and foremost thanks goes to our college principal **Dr.Joseph O A** for being constant source of encouragement during this project period. We are extremely grateful to him for providing opportunity to do our project at this college.

Our sincere thanks to **Mrs. Priya V V** (Assistant Prof. in Computer Science, College Of Engineering Thalassery) and **Ms. Binitha S** (Assistant Prof. in Computer Science, College Of Engineering Thalassery) can't be expressed fully in words. We thank her from the bottom of our heart.

We pay our regards to all our teachers and non-teaching staffs at the college or the knowledge they have imparted to us over the last two years. We are also grateful to our family members and friends for their cooperation and moral support. Above all, we owe my gratitude to God almighty for showering abundant blessings upon us. Above all it is the grace and blessing of God the almighty, which make this endeavour success.

ABSTRACT

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as ”the weakest link” in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability.

TABLE OF CONTENTS

1. INTRODUCTION……... 1

1.1. OBJECTIVES……. 5

1.2. MOTIVATION..... 6

1.3. APPLICATION……... 6

2. LITERATURE REVIEW..... 7

3. SYSTEM STUDY AND ANALYSIS..... 19

31. EXISTING SYSTEM..... 19

3.2. PROPOSED SYSTEM..... 22

4. DEVELOPING TOOLS..... 24

4.1. HARDWARE SPECIFICATION..... 24

4.2. SOFTWARE SPECIFICATION..... 24

4.2.1 FRONT END..... 24

4.2.2 BACK END..... 27

4.3 IDE..... 30

4.4 WEBSERVER..... 31

5. SYSTEM DESIGN..... 32

5.1 MODULES..... 32

5.1.1 USER MODULE..... 32

5.1.1.1 REGISTRATION MODULE..... 32

5.1.1.2. QR CODE GENERATOR MODULE……..... 32

5.1.1.3 LOG IN MODULE..... 33

5.1.1.4. WATER MARKING MODULE..... 33

5.2. DATA FLOW DIAGRAM..... 33

6. DATABASE DESIGN..... 38

7. COST ESTIMATION..... 42

8. SCREEN SHOTS..... 43

9. SYSTEM TESTING..... 45

9.1. TESTING STRATEGIES……..... 47

9.1.1. UNIT TESTING..... 48

9.1.2. INTEGRATION TESTING..... 48

9.1.3. SYSTEM TESTING..... 49

9.1.4. OUTPUT TESTING..... 49

9.1.5. ACCEPTANCE TESTING..... 49

9.2. MAINTENANCE..... 49

10. CONCLUSION..... 51

11. FUTURE ENHANCEMENT..... 52

12. REFERENCES..... 53

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO.
1.	Computer Network of Cloud Computing	1
2.1.	Pixel Squares Selected By Users……..……	9
2.2.	Fake Pointer…….	10
2.3.	Color Rings method and Convex Hull method….	11
5.2.1.	Level 0 DFD……	35
5.2.2.	Level 1 DFD……..	35
5.2.2.1.	Level 1.1 DFD……...……	36
5.2.2.2.	Level 1.2 DFD……...	36
5.2.2.3.	Level 1.3 DFD……	37
6.1.	User Table……	40
6.2.	Log in Table…….	40
6.3.	Pass_file Table…….	40
8.1.	Home Page……...	43
8.2.	Registration Form……	43
8.3.	Log in Page……..	43

1. INTRODUCTION

As a newfound service grown in IT in recent decades, cloud computing has emerged as a new technology to tackle the access to sharing computing resources such as computer networks, storage, servers, services, and applications. Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data centre from a capital-intensive set up to a variable priced environment.

The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Based on various models, the services provided by the cloud computing system include (IAAS), (SAAS), and (PAAS), that indicates infrastructure, software, and platform as service, respectively, together with virtualization.

1. Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

2. Platform as a Service (Paas): Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE and Ruby. Google's App Engine, Force.com are some of the popular PaaS examples.

3. Infrastructure as a Service (Iaas): IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.

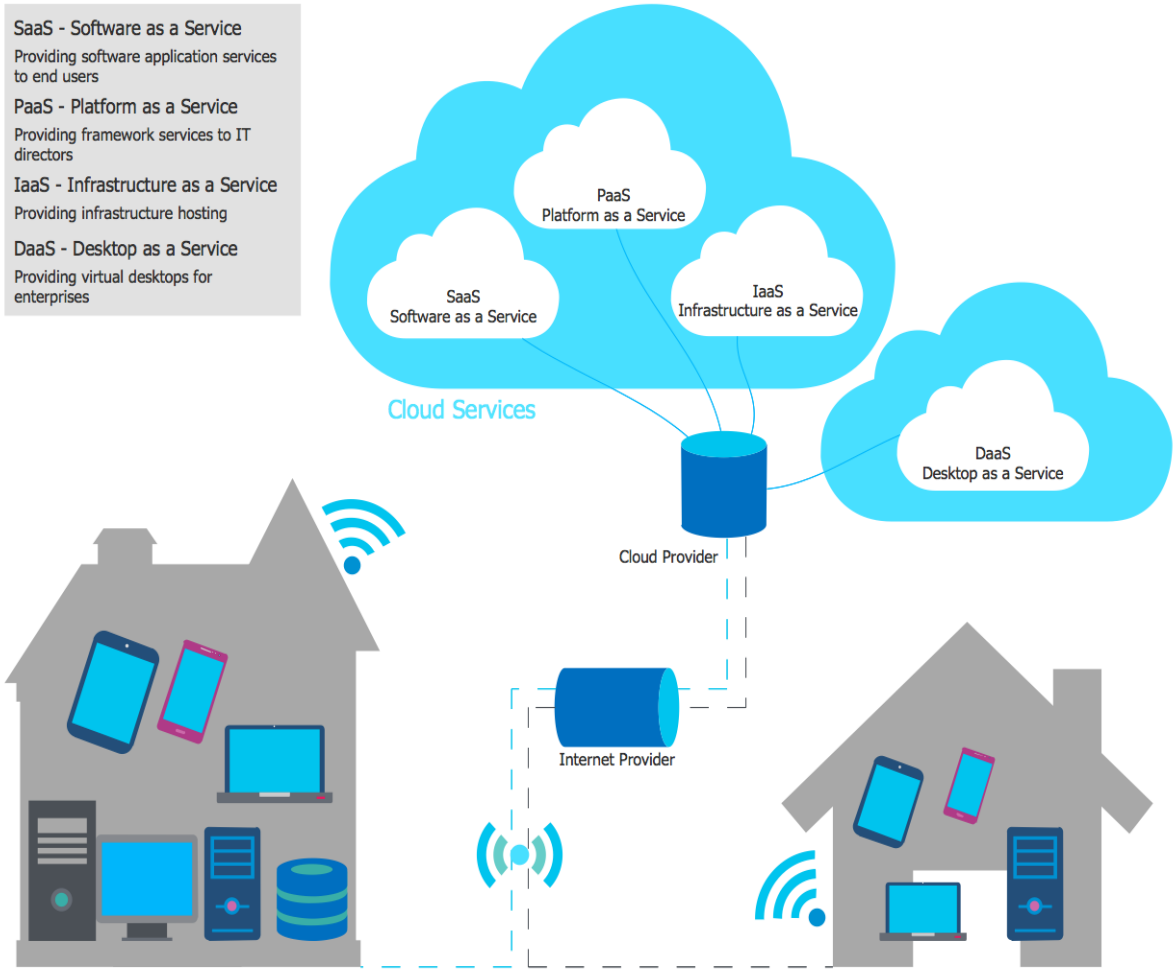


Fig 1. Computer Network of Cloud Computing

Under this new technology, the users are provided with vast flexibility not only to process and store their data in the cloud server but also to get into it anywhere and anytime via the channel of internet. Some typical benefits of cloud computing are:

(a) Reduced Cost -There are a number of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased

thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing.

(b) Increased Storage -With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically.

(c) Flexibility - This is an extremely important characteristic. With enterprises having to adapt even more rapidly to changing business conditions speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

Cloud computing has many advantages including information shared in the virtual environment, dynamic scalability, utility of storage and utilization of software, platform and infrastructure, managed distributed computing power, and so on.

The global market for the cloud will grow to $95million and some percentage of software will also move within next five years. This requires the tremendous change in the privacy and security requirements of cloud. This attribute raises many new security challenges. The hackers of cloud storage in the cloud as a honey pot, because of the lack of security and privacy. The main aim of the cloud is to provide better utilization of resources using virtualization.

In spite of these features mentioned above, the reliability of these models is greatly influenced by some security issues such as user authentication. The user authentication is said to be the most important security issue and challenge to be searched, debated and addressed, for it is considered as a core requirement for cloud computing. In this sense, it has received great attention by so many researchers and scholars who try to propose new strong user authentication techniques to protect the cloud users' personal authenticating data. According to them, strong authentication is nothing, but a promising solution not only to identify and prove the legal cloud user's identity and authenticity but also to prevent illegal user's access to the authorized user's data.

Despite its growing influence, concerns regarding cloud computing still remain. Some other common challenges faced in cloud are:

1. Data Protection: Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centres (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

2. Data Recovery and Availability: All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support. Appropriate clustering and Fail over Data Replication System monitoring (Transactions monitoring, logs monitoring and others), Maintenance (Runtime Governance), Disaster recovery Capacity and performance management. If any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.

3. Management Capabilities: Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like, Auto-scaling for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

4. Regulatory and Compliance Restrictions: In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data centre or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

With cloud computing, the action moves to the interface — that is, to the interface between service suppliers and multiple groups of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment and service negotiation — areas that many enterprises are only modestly equipped to handle.

Generally speaking, an attractive authentication scheme for users in services of cloud environment should meet the following benefits.

(1) It based on some effective cryptosystems to support authentication mutuality and user pseudonym without using SSL.

(2) It should require a trusted third party for user and service provider registration, but it is not required in upcoming user authentication session.

(3) A user has to use only one private key to access services from multiple service providers.

(4) It does not require hard computation operations on users' side.

In focus on the problem of auditing when an untrusted server stores client's data. The authors introduce the model for provable data possession. This software overcomes the vulnerabilities of like eves dropping, dictionary attack, social engineering, key-logger and shoulder surfing which are well known. Secure cloud is a software which uses key-logger resistance protocols in login phase and PassMatrix authentication system is used while modifying data in user's cloud storage.

This project has two visual authentication protocols using QR code: one is used during login phase using virtual keyboard, and the other is a visual -based authentication protocol for file modifications. For the implementation of this virtual keyboard approach, a colour password authentication scheme is used. Colour passwords can be used only once and every time a new password is generated. Two techniques are used to generate colour passwords. One of these two use text and the other use colours. PassMatrix system is used mainly during file upload or download and uses a login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder-surfing attacks.

1.1 OBJECTIVES

The main objective of the project is to protect user data stored in the cloud storage. It should also prevent attackers from accessing the authorized users' data.

This software will also provide security for the data stored in the cloud and also provide authentication for user login. It prevents data from being hacked which leads to data loss.

The implementation of the project ensures better user privacy and prevents datas being upload or download in the client's storage in cloud.

1.2 MOTIVATION

The usage of cloud storage has enabled the users to store their data and access them from anywhere seamlessly. The facilities and services provided by cloud storage is accompanied by the numerous security issues related to privacy and authentication. Moreover, the data in the cloud may be lost or modified due to some breaches in the security. This motivated our team to develop a software that prevents an attacker from accessing an authorized user's data in cloud storage and also prevents the client's data from being modified by the attacker.

1.3 APPLICATION

Some of the applications of the software is as follows:

- It can be used for security and authentication for accessing the data in the cloud.
- It can be used as authentication scheme for other services in cloud.
- Provides better security for sensitive data such as the details regarding the user's banking transactions, information about the user, or any other information that the user wants to keep secret in the cloud.
- It can also be used for protecting other applications apart from the cloud.

2. LITERATURE REVIEW

The strength user authentication has gained its importance from its promising solution for protection the cloud users' personal authenticating data against attackers and unauthorized access. As a result, a lot of scholars and specialists in the cloud computing security field have devoted their time to address such an issue, making good achievements in protecting the cloud user's identification. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems and digital watermarking methods for images.

Choudhury [4] proposed a framework for cloud computing authentication by using a smart card. Their scheme provides management of identity, session key launching, and mutual authentication between the user and the cloud server. Yet, it is not quite efficient because of using the OOB that requires the user to login to the cloud every time. Moreover, the last verification for the login is done not at the server but at the user's device. In addition, it does not give any solution in the case of the smart card loss.

Jiang [5] proposed a simple scheme for cloud storage by using the USB token. In this scheme, both the secret number of the server as well as the user identifier is kept in the server to be used in the identity authentication phase. Accordingly, the method sustains from the modification attack; if the attacker knows the user identifier, he or she can easily get the secret number of the server. In addition, the scheme is dependent on the password to protect the USB Token and in the case of losing the USB, this may be attacked by the password guessing attack. Moreover, Hong [6] proposed a two-channel authentication of user technique by using USB. Yet, the user's authenticating data is still vulnerable to many attacks.

The [7,8] proposed an efficient and practical smart-cardbased scheme on the base of secure one-way hash function. It have eliminated the needing of verification table on the server, and solved the problem of replay attack. However, in [8], the mutual authentication cannot be achieved. And in [7], the passwords of users cannot freely be changed.

In addition, Abdellaoui [9] proposed an authentication scheme in the cloud environment. The idea behind this scheme is on the base of the using of pixels of images to create an OTP as a third factor of authentication. However, the scheme involves a verification table as the password and the user identifier are sent to the server, and the session key is not established.

Thus, the user privacy cannot be achieved. In addition, it is not resistant to the DOS attack and the inside attack.

Furthermore, Chun-Ta Li [10] to provide the user anonymity, extended his advanced password authentication scheme which updated by using a smart card. However, the proposed scheme has a verification table, and cannot achieve the user privacy. It also suffers from the DOS attack and Man in the middle attack. In addition, it does not offer any solution in case of losing the smart card. Finally, in [11,13] solutions that eliminate the verification table are suggested, but, various drawbacks such as clock synchronization, difficulties in changing the password, and insider attack vulnerability is still raised.

Many other schemes such as those in may have good usability, they are not graphical-based and need additional support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc. In the early days, the graphical capability of handheld devices was weak; the colour and pixel it could show was limited. Under this limitation, the Draw-a-Secret (DAS) [33] technique was proposed by Jermyn et al. in 1999, where the user is required to re-draw a pre-defined picture on a 2D grid. We directly extract the figure from and show it in Figure 2.1(b). If the drawing touches the same grids in the same sequence, then the user is authenticated. Since then, the graphical capability of handheld devices has steadily and ceaselessly improved with the advances in science and technology.

In 2005, Susan Wiedenbeck et al. [13] introduced a graphical authentication scheme Pass Points [13], and at that time, handheld devices could already show high resolution color pictures. Using the PassPoint scheme, the user has to click on a set of pre-defined pixels on the predestined photo, as shown in Figure 2.1(a), with a correct sequence and within their tolerant squares during the login stage. Moreover, Marcos et al. also extended the DAS based on finger-drawn doodles and pseudo signatures in recent mobile device [34], [35]. This authentication system is based on features which are extracted from the dynamics of the gesture drawing process (e.g., speed or acceleration). These features contain behavioral biometric characteristic. In other words, the attacker would have to imitate not only what the user draws, but also how the user draws it. However, these three authentication schemes are still all vulnerable to shoulder-surfing attacks as they may reveal the graphical passwords directly to some unknown observers in public.

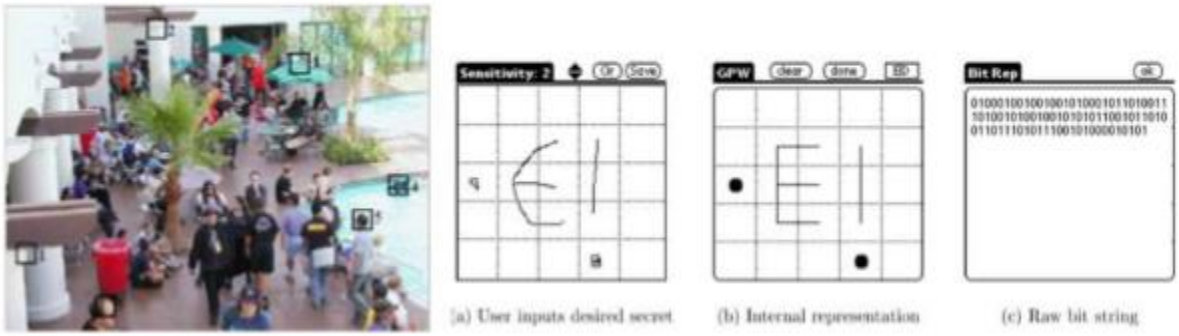


Fig.2.1. Pixel squares selected by users as authentication passwords in PassPoints

In addition to graphical authentication schemes, there was some research on the extension of conventional personal identification number (PIN) entry authentication systems. In 2004, Roth presented an approach for PIN entry against shoulder surfing attacks by increasing the noise to observers. In their approach, the PIN digits are displayed in either black or white randomly in each round. The user must respond to the system by identifying the color for each password digit. After the user has made a series of binary choices (black or white), the system can figure out the PIN number the user intended to enter by intersecting the user's choices. This approach could confuse the observers if they just watch the screen without any help of video capturing devices. However, if observers are able to capture the whole authentication process, the passwords can be cracked easily.

In order to defend the shoulder-surfing attacks with video capturing, FakePointer was introduced in 2008 by T. Takada. It uses Figure 2.2 below to show the usage of Fake Pointer. In addition to the PIN number, the user will get a new "answer indicator" each time for the authentication process at a bank ATM. In other words, the user has two secrets for authentication: a PIN as a fixed secret and an answer indicator as a disposable secret. The answer indicator is a sequence of n shapes if the PIN has n digits. At each login session, the Fake Pointer interface will present the user an image of a numeric keypad with 10 numbers (similar to the numeric keypad for phones), with each key (number) on top of a randomly picked shape. The numeric keys, but not the shapes, can be moved circularly using the left or right arrow keys. During authentication, the user must repeatedly move numeric keys circularly as shown in the leftmost figure in Figure 2, until the first digit of the PIN overlaps the first shape of the answer indicator on the keypad and then confirm a selection by pressing the space key. This operation is repeated until all the PIN digits are entered and confirmed. This approach is quite robust even when the attacker captures the whole

authentication process. However, there is still room to improve the password space. For example, if the device used for authentication is a smartphone, a tablet or a computer rather than a bank ATM, the password space can be enlarged substantially since the PIN could be any combination of alphanumeric characters rather than just numeric digits.

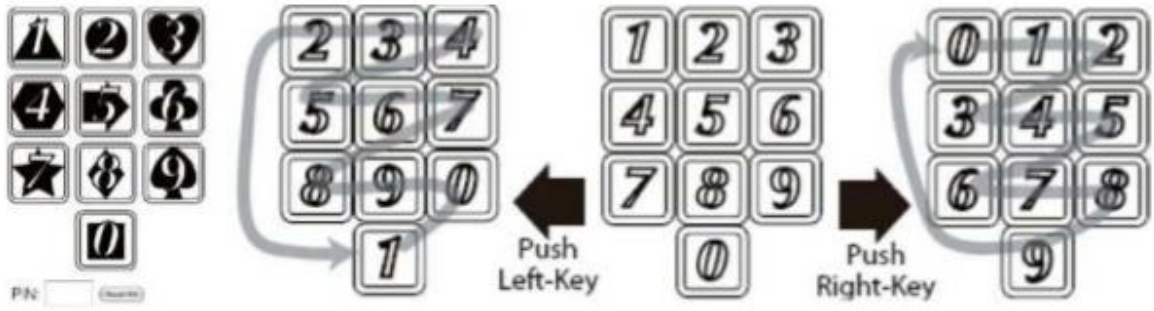


Fig.2.2. Fake Pointer, where a user can move a numeric key layout circularly using right and left arrow keys.

Wiedenback et al. [13] described a graphical password entry scheme in 2006, as shown in Figure (the figure is extracted from. This scheme is resistant to shoulder-surfing attacks using a convex hull method. The user needs to recognize a set of pass-icons on the screen and clicks inside the convex hull formed by all these pass-icons. In order to make the password hard to guess, a large number of other different icons can be inserted into the screen to increase the password space. However, a large number of objects will crowd the display and may make objects indistinguishable. In 2010, David Kim proposed a visual authentication scheme for tabletop interfaces called ”Colour Rings”, as shown in Figure 3(a) where the user is assigned authentication (key) icons, which are collectively assigned one of the four color-rings: red, green, blue, or pink.

In 2010, David Kim et al. [36] proposed a visual authen- tication scheme for tabletop interfaces called “Color Rings”, as shown in Figure 3(a) (the figure is extracted from [36]), where the user is assigned *i* authentication (key) icons, which are collectively assigned one of the four color-rings: red, green, blue, or pink. During login, *i* grids of icons are provided, with 72 icons being displayed per grid. There is only one key icon presented in each grid. The user must drag all four rings (ideally with index finger and thumb from two hands) concurrently and place them in the grid. The distinct key icon should be captured by the correct color ring while the rest of rings just make decoy selections. The user confirms a selection by dropping the rings in position. The rings are large enough to include more than

one icon and can thus obfuscate the direct observer. Unfortunately, these kinds of passwords can be cracked by intersecting the user's selections in each login because the color of the assigned ring is fixed and a ring can include at most seven icons. Thus, the attacker only requires a limited number of trials to guess the user's password.

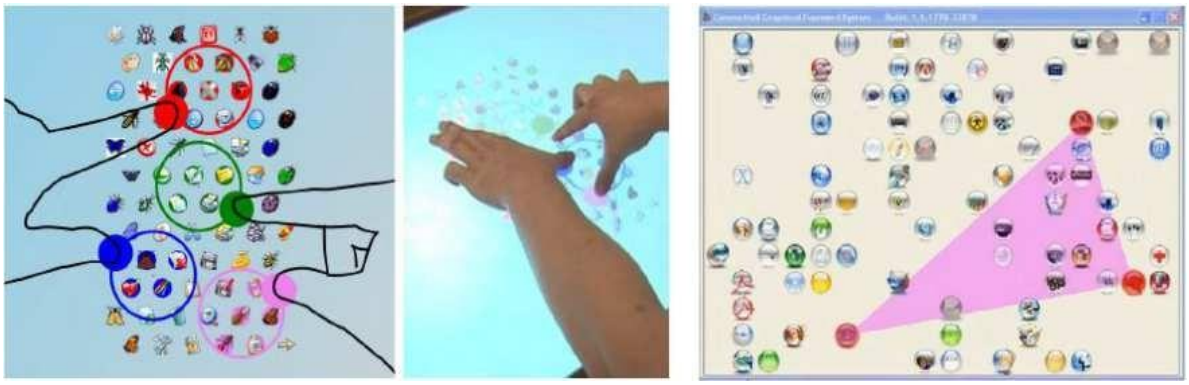


Fig. 2.3. (a) Color Rings method [36]. (b) Convex Hull method [13].

During login, i grids of icons are provided, with 72 icons being displayed per grid. There is only one key icon presented in each grid. The user must drag all four rings (ideally with index finger and thumb from two hands) concurrently and place them in the grid. The distinct key icon should be captured by the correct colour ring while the rest of rings just make decoy selections. The user confirms a selection by dropping the rings in position. The rings are large enough to include more than one icon and can thus obfuscate the direct observer. Unfortunately, these kinds of passwords can be cracked by intersecting the user's selections in each login because the colour of the assigned ring is fixed and a ring can include at most seven icons. Thus, the attacker only requires a limited number of trials to guess the user's password.

Digital watermarking methods for images are usually categorized into two types: invisible and visible. The first type aims to embed copyright information imperceptibly into host media such that in cases of copyright infringements, the hidden information can be retrieved to identify the ownership of the protected host. It is important for the watermarked image to be resistant to common image operations to ensure that the hidden information is still retrievable after such alterations. Methods of the second type, on the other hand, yield visible watermarks which are generally clearly visible after common image operations are applied. In addition, visible watermarks convey ownership information directly on the media and can deter attempts of copyright violations.

Embedding of watermarks, either visible or invisible, degrade the quality of the host media in general. A group of techniques, named reversible watermarking [37]–[47], allow legitimate users to remove the embedded watermark and restore the original content as needed. However, not all reversible watermarking techniques guarantee lossless image recovery, which means that the recovered image is identical to the original, pixel by pixel. Lossless recovery is important in many applications where serious concerns about image quality arise. Some examples include forensics, medical image analysis, historical art imaging, or military applications. Compared with their invisible counterparts, there are relatively few mention so floss less visible watermarking in the literature. Several lossless invisible watermarking techniques have been proposed in the past. The most common approach is to compress a portion of the original host and then embed the compressed data together with the intended payload into the host.

Another approach is to superimpose the spread-spectrum signal of the payload on the host so that the signal is detectable and removable. A third approach is to manipulate a group of pixels as a unit to embed a bit of information [44],[45]. Although one may use lossless invisible techniques to embed removable visible watermarks, the low embedding capacities of these techniques hinder the possibility of implanting large-sized visible watermarks into host media. As to lossless visible watermarking, the most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT co-efficients in the watermark region.

Another approach is to rotate consecutive watermark pixels to embed a visible watermark. One advantage of these approaches is that watermarks of arbitrary sizes can be embedded into any host image. However, only binary visible watermarks can be embedded using these approaches, which is too restrictive since most company logos are colorful.

A new method for lossless visible watermarking is proposed by using appropriate compound mappings that allow mapped values to be controllable. The mappings are proved to be reversible for lossless recovery of the original image. The approach is generic, leading to the possibility of embedding different types of visible watermarks into cover images. Two applications of the proposed method are demonstrated, where opaque monochrome watermarks and non-uniformly translucent full-colour ones are respectively embedded into colour images. More specific compound mappings are also created and proved to be able to yield visually more distinctive visible watermarks in the watermarked image. To the best

knowledge of the authors, this is the first method ever proposed for embedding removable translucent full-colour watermarks which provide better advertising effects than traditional monochrome ones.

P. Garbacki in cloud computing system solved the issue of data security by introducing in cloud computing data security: fully homomorphism encryption algorithm, the new type of data security solution to the insecurity of the cloud computing is proposed and the scenarios of this application are hereafter constructed. For the retrieval and processing of the encrypted data effectively, this new security solution is fully equipped leading to the broad applicable prospect storage of the cloud computing and the security of data transmission.

Prakash G L proposed that how to protect the outsourced sensitive data as a service is becomes a major data security challenge in cloud computing. To address these data security challenges, we propose an efficient data encryption to encrypt sensitive data before sending to the cloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key. We analyze the privacy protection of outsourced data using experiment is carried out on the repository of text files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance.

Hanumantha Rao has proposed a business model for cloud computing for data security using data encryption and decryption algorithms. In this method cloud service provider has responsible for data storage and data encryption/decryption tasks, which takes more computational overhead for process of data in cloud server. The main disadvantage of this method is, there is no control of data for data owner i.e, data owner has completely trusted with cloud service provider and he has more computational overhead.

Swati Paliwal proposed an Attribute Based Encryption (ABE) and verifiable data decryption method to provide data security in cloud based system. They have been designed the data decryption algorithm based on the user requested attributes of the out sourced encrypted data. One of the main efficiency drawbacks of this method is, cloud service provider has more computational and storage overhead for verification of user attributes with the outsourced encrypted data. While introducing third party auditor we can reduces the storage, computation, and communication overheads of the cloud server, which improves the efficiency of the cloud data storage.

Shiv Shakti discussed the performance of six different symmetric key RSA data encryption algorithms in cloud computing environment. They have proposed two separate cloud servers; one for data server and other for key cloud server and the data encryption and decryption process at the client side. The main drawback of this method is to maintaining two separate servers for data security in cloud, which creates a more storage and computation overheads.

One of the most popular and elderly remote user authentication schemes was suggested by Lamport [18] in 1981, in which, the server stores the hashed value of a user's password. In Lamport's scheme, password table was used to verify the legitimacy of users, but if this password table is compromised, stolen, or modified by an adversary, then the system could be partially or completely compromised [19],[20]. Some more recent smart card based password authentication schemes have been proposed in [21] – [24], and many of the schemes have been broken as shown by [25] - [29].

Shoup-Rubin [30] proposed extension of Bellare- Rogaway model [31] which is based on three party key distribution protocol and smartcard is used to store the long term secret keys. In their scheme, smartcard is used to prevent the adversaries and it is assumed that smartcard is never compromised. So basically the scheme falls in one factor category as two factor schemes can be broken by compromising both the factors only.

Liao et al. [22] tried to consolidate a number of passwords and smartcard based properties and proposed two factor smartcard and password authentication scheme, which is still vulnerable to many attacks, as demonstrated in [32].

Cloud computing is a variant of client server architecture, where, thousands of clients use the same infrastructure at a large scale. Consequently, it needs stronger authentication than conventional client server inter-networking system.

Lee et al [14] have proposed public key and mobile out of band based authentication for cloud computing. However, the scheme transmits data (e.g. ID, PW, and PKI) in a plaintext form which can be easily intercepted by the adversaries. In addition, their scheme does not care about data confidentiality, data integrity, user privacy and users are not allowed to change their password. As result, their scheme is not fit for real time cloud computing.

In [17], authors study the challenges regarding confidentiality, integrity and availability for cloud computing and mainly concerned about efficient handling of IAM using protocols.

However, prior to identity and access management, access control is more important so that any unauthorised adversary cannot access legal user's data. Furthermore, identity and access control management represents identity assertion relationships to connect services in the cloud. But what do we do to verify end users to establish their identities and raise a question to researchers, how to protect cloud data from illegal users?

Li and Wu [15] proposed a theoretical prototype system, in which cloud computing system is combined with trusted platform support service.

Celesti et al [16] proposed reference architecture to address identity management problem for cloud computing. However, these schemes did not address access control for cloud computing users.

In order to save the fee to hire a professional manager, database as a service [48] (DaaS, for short, which can offer data management service as well as the local database), also known as database outsourcing, has been developed. Database owner delegates his management tasks (e.g. database access, maintenance and management) to a third party, then the user can get the desired data by means of own access privilege. In this new database service mode, there would be some security problems when a database was uploaded to an untrusted database service provider (in which the data could be revealed or tampered maliciously in the cloud).

Traditionally, the data security is mainly protected by using the user authentication [49] and the user privilege management [50] strategies, so as to ensure the integrity, consistency, and the overall quality of data. In some applications, the use of the access control method for data security is often insufficient. Once the access control is cracked, sensitive data will be leaked and used illegally. An effective measure to this issue is to combine both database encryption and database watermarking together. Common comparison operations in database involve indexing technology [51]. Once the index is invalid, the operability of database will be reduced greatly. Therefore, order-preserving encryption (OPE) as a deterministic encryption scheme (whose encryption function preserves numerical ordering of the plaintexts and allows comparison operations on encrypted data without decryption), was firstly proposed in the database community by Agrawal et al. [52]. Here, equality and range queries as well as the MAX, MIN, and COUNT queries can be directly processed

over encrypted data. Nevertheless, Agrawal et al. does not define security nor provide any formal security analysis.

In order to ensure that the adversary cannot get any information about original data from the order even though he or she has got all of the ciphertexts, Boldyreva et al. [53] presented an efficient OPE scheme with provable security definition. Moreover, combining the random order-preserving function (ROPF) and the hypergeometric distribution (HGD), this scheme was suitable for data privacy protection in the cloud and achieved the predictive effect [54, 55].

Furthermore, Boldyreva et al. [56] proposed a modular OPE (MOPE) scheme which improved the security performance of OPE schemes. The resulting scheme was no longer strictly order-preserving, but range query operations can be performed by modular range queries. Later, there were several works on OPES [57–59] by further improving security performance.

There are many issues that Cloud computing undergoes on the integrity and privacy of the user's stored data at cloud. It is important from the user's perspective to develop a secure and efficient method to guarantee the integrity and privacy of data stored in the cloud. Wang et al. [61] has proposed a privacy preserving public auditing protocol. It uses an independent TPA for auditing the data. For this purpose, public key based Homomorphic linear authenticator (HLA) along with random masking techniques is used. But it is susceptible to existential forgeries attacks such as message attack from a malicious cloud server and an outside attacker.

To resolve this issue, Wang et al. [60] proposed a new improved scheme which tends to be more secure than the previous proposed protocol [61]. It is also a public auditing scheme with TPA. It is developed to perform data auditing on behalf of users. It makes use of HLA constructed from Boneh-Lynn-Shacham short signature known as BLS signatures and random masking technique for data hiding. For the purpose of data binding, the new scheme uses computationally intensive pairing operation which makes it inefficient for using. It is practically implemented on Amazon EC2 instance, which provides the fast performance of the design on both the cloud and on the auditor side. But the full-fledged implementation of it on the commercial public cloud is not tested yet. So it is difficult to expect it to work robustly with very large scale of data [62].

Wang et al. [63] proposed another protocol that supports both public auditing and data dynamics by using the BLS based HLA along with Merkle Hash Tree (MHT). It achieves the integrity of data, but fails to provide confidentiality of the data stored on the cloud. Wang et al. [64] has also proposed a design to detect the modified blocks easily using homomorphic token pre-computation and later erasure coded technique is used to acquire the desired blocks from different servers. Solomon et al. [65] proposed a protocol which uses the same security level as Wang et al. [62] but with better efficiency. It generates a signature set which is an ordered collection of signatures on each file block, thus incurring computation and communication overhead.

Meenakshi et al. [66] has proposed a protocol which uses TPA to audit the data of the users using a Merkle Hash Tree algorithm. It supports data dynamics, but fails to provide confidentiality to the data stored in the cloud.

Tejaswini et al. [67] has used Merkle hash tree to achieve data integrity with a TPA. Data confidentiality is maintained with Rivest, Shamir Adleman (RSA) based cryptography algorithm, whereas Jadhav et al. [68] has developed an attacking module that continuously keeps a track on data alteration in the cloud.

Here data confidentiality is maintained by using Advanced Encryption Standard (AES) algorithm for encrypting the data. A method that uses the keyed Hash Message Authentication Code (HMAC) along with homomorphic tokens is developed by Arasu et al. [69]. It tends to enhance the security of TPA. It is a method implemented for checking the integrity of a data transmitted between two parties by agreeing on a shared secret key. HMAC's are key based method that it shared between the two parties. If either party's key is compromised, it is possible for an attacker or unauthorized user to generate fraud messages.

Most authentication protocols [70]–[73], which are designed for single server environment, are not suitable for distributed services environment in which multiple servers offer a plethora of services. Although traditional single sign-on (SSO) schemes such as Passport [74] and Open ID [75] are possible solutions to address this issue, these schemes require the trusted third party to participate in each user authentication session, which could become the bottleneck for traditional SSO systems.

To this end, Tsai and Lo [76] proposed an efficient authentication scheme using identity based cryptosystem [77] for distributed cloud computing services. Their scheme has the following advantages. First, a mobile user can access multiple services from different mobile cloud service providers using only one single private key. Second, no verification table is required to be implemented at service providers or the trusted third party. Third, the trusted third party is not required to be involved in regular user authentication session, thus greatly reducing the total user authentication processing time.

Finally, due to the usage of bilinear pairing in an elliptic curve [78], [79], their scheme incurs less computing resources on both the mobile devices and service providers [80]. It is claimed that the scheme achieves mutual authentication, key exchange, user anonymity, and user untraceability, and withstands all major security threats. However, we observe that their scheme fails to achieve mutual authentication, because it is vulnerable to the service provider impersonation attack. Beside this major defect, it also suffers from some minor design flaws, including misuse of biometrics, wrong password and fingerprint login, and no user revocation facility when the smart card is lost/stolen.

3. SYSTEM STUDY AND ANALYSIS

System analysis is the process of gathering and interpreting facts, diagnosing problems and using the information to recommend improvements on the system. It is a problem solving activity that requires intensive communication between system users and developers. System analysis or study is an important phase of any system development process. The system is viewed as a whole, the inputs are identified and the system is subjected to close study to identify the problematic areas. The solutions are given as a proposal. The proposal is reviewed on user request and suitable changes are made. This loop ends as soon as the user is satisfied with the proposal. Here, our software is analysed using the existing system and proposed system in system analysis phase.

3.1 EXISTING SYSTEM

At present, there are numerous methods which provides security for cloud storage services. But none of the methods provide complete solution for user authentication and data security.

The cloud services providers such as Google, Amazon, Microsoft, etc. uses the email id and password as the primary source for logging into the client's data in the cloud. This is not a secure method for accessing the data in cloud because if the hacker acquires the email id and the corresponding password through password guessing or other methods then it might result in data loss in the client's cloud. Another issue is that there is no proper authentication protocol in the cloud to identify the authentic user of the cloud. This is because the password and email id is the only source of authentication to access the cloud and hence can result in accessing of the cloud by an outsider or a hacker or by a friend. Hence, this enable an outsider to download sensitive data from the client's storage in cloud or make the client's cloud open to public.

The following aspects of security must be considered for the different stages of data in the cloud.

- Data lineage
- Data during transmission
- Data at rest

- Data in Process
- Data eminence
- Data in source

Data Lineage

Tracking the data movement in the cloud is referred as data lineage i.e., where it comes in, where it flows to and how it travels through the cloud. This information is important for auditing the cloud. The data lineage solution will record the data sources that are relevant to each stage of the process and then mapping these sources to each other to show how the data flows and how it is transforms. In a public cloud the data lineage problem solving is a challenging task. The data flows non-linear in virtual environment. So it complicates the process of data integrity in the cloud.

Data during Transmission

The data during transmission must be encrypted using the latest encryption technology. The selection of encryption technology must be up to date. The selected technology must provide security against present security threats and by using the protocol the transmission must provide integrity and confidentiality. After encryption the data must be divided into packets and it will be transmitted to the receiver through disjoint paths. It will reduce the chance of capturing all the packets by any threats until the packets are coupled together in a particular format.

Data at Rest

The data managed even the data in rest during its transmission. Managing this kind of data is feasible in IaaS because of the access restriction over data. The major problem with data at rest is loss in control. Recently the encryption techniques are available with storage devices. The lock box approach, homomorphic encryption and public encryption are some of the techniques to manage the data at rest.

Data in Process

Data in a cloud will enter into processing state so that the storage cloud requesting the service for processing data in the cloud. Once the process will activate user data available in

the storage cloud will securely transferred to the processor for processing. During the processing time the cloud must provide security when the data in process.

Data Remanence

Data remanence refers to the data will remain in the cloud in case of data transfer or data removal. The data not only be protected against unauthorized access but also securely deleted at the end of its life cycle. Data remanence is also referred as secure delete, secure purging etc., When documents expire, deleted and if a malicious user gets access to the disk or if disk are say physically stolen the chances of extracting the data block is high. So the storage cloud should provide the end users to delete the data securely. Data remanence may be the secure disclosure of sensitive information in an uncontrolled environment. Different techniques have been developed to answer data remanence.

Data in source

The data must be secure from the source. Data provenance is the security property stating that the source, where a piece of data is generated cannot be spoofed or interferes with. The provenance refers to maintaining data integrity and ensuring that the integrated data are computationally correct.

Classification of Security Issues

The security issues for the cloud storage is classified into two categories

Access Security Issues

Security during communication in the cloud is a potential point at which threats to the service could be exposed. The advent of mobile computing systems a potential threat to security and possibly privacy of users would be a location as this could entail the presence of communication as this to identify the location.

Service Security Issues

Most of the security threats are possible at the point of service provision. This would include device security and storage security. The providers provide the security by using IDS firewall sand malware protection.

Security Issues in Cloud

Security issues in cloud are:

Google Hacking

Google is the best option for searching details regarding anything on the net. By using the Google search engine the attacker try to find sensitive information. That information was used by the attacker for hacking a user's account.

Broken Authentication

The requests submitted by each user are tracked by the session created by the web application. In this attack the attacker hijack the active session by using the session tokens. It is difficult to protect user identity only by protecting authentication credentials, session identifiers in SSL

IP Spoofing

IP spoofing is one of the most common forms of on-line camouflage. In this attack, an attacker gains unauthorized access to a computer or a network newer routers and firewall arrangements can offer protection against IP spoofing

Dictionary attack

In this attack the intruder try to more attempts authentication mechanism by entering each word in a dictionary as a password or try to determine the decryption key of an encrypted message or document.

3.2 PROPOSED SYSTEM

The purpose of the proposed system is to overcome the problems and drawbacks of the existing system regarding the authentication and security of the client's data in the cloud. The proposed system consists of two level visual authentication protocols using QR code: one is used during login phase using virtual keyboard, and the other is a visual -based authentication protocol for file upload and download. For the implementation of this virtual keyboard approach, a colour password authentication scheme is used.

Colour passwords can be used only once and every time a new password is generated. Two techniques are used to generate colour passwords. One of these two use text and the other use colours. PassMatrix protocol is mainly used during uploading or downloading a file and uses a login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder-surfing attacks.

4. DEVELOPING TOOLS

4.1 HARDWARE SPECIFICATION

Processor : Intel Core i3

RAM : 4GB

HDD : 50MB

Cache memory : 512KB

4.2 SOFTWARE SPECIFICATION

OPERATING SYSTEM : WINDOWS OS

FRONT END : Java(For web application)/Android, HTML, CSS

BACK END : MySQL

IDE : Netbeans 8.2, Android Studio

DESIGN TOOLS : Adobe Dreamweaver

WEB BROWSER : Internet Explorer/Google Chrome/Mozilla Firefox

WEBSERVER : Apache(for web applications)

4.2.1 FRONT END

Java

Initially the language was called as “oak” but it was renamed as “java” in 1995.The primary motivation of this language was the need for a platform-independent (i.e. architecture neutral)language that could be used to create software to be embedded in various consumer electronic devices.

Based on the advantages of Java, it gained wide popularity and multiple configurations have been built to suit various types of platforms including Java SE for Macintosh, Windows and UNIX, Java ME for Mobile Applications and Java EE for Enterprise Applications.

Java is a programmer's language

- Java is cohesive and consistent
- Except for those constraint imposed by the Internet environment. Java gives the programmer, full control

Java has had a profound effect on the Internet. This is because; java expands the Universe of objects that can move about freely in Cyberspace. In a network, two categories of objects are transmitted between the server and the personal computer. They are passive information and Dynamic active programs in the areas of security and probability. But Java addresses these concerns and by doing so, has opened the door to an exciting new form of program called the Applet.

Java programming languages has the following advantages for this project.

- Java offers higher cross- functionality and portability as programs written in one platform can run across desktops, mobiles, embedded systems.
- Java is free, simple, object-oriented, distributed, supports multithreading and offers multimedia and network support.
- Java is a mature language, therefore more stable and predictable. The Java Class Library enables cross-platform development.
- Being highly popular at enterprise, embedded and network level, Java has a large active user community and support available.
- Unlike C and C++, Java programs are compiled independent of platform in *bytecode* language which allows the same program to run on any machine that has a JVM installed.
- Java has powerful development tools like Eclipse SDK and NetBeans which have debugging capability and offer integrated development environment.
- Increasing language diversity, evidenced by compatibility of Java with Scala, Groovy, JRuby, and Clojure.
- Relatively seamless forward compatibility from one version to the next

Cascading Style Sheets (CSS)

Cascading Style Sheets (CSS) is a style sheet language used for describing the look and formatting of a document written in a mark-up language. While most often used to

style web pages and interfaces written in html and XHTML, the language can be applied to any kind of xml document, including plain xml, SVG and XUL.

CSS is designed primarily to enable the separation of document content from document presentation, including elements such as the layout, colours, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple pages to share formatting, and reduce complexity and repetition in the structural content (such as by allowing for tables web design).

The CSS provides a lot of advantages for the project development. CSS allows separating content of an html document from the style and layout of that document. It make documents much easier to maintain and give much better control over the layout of the web pages, because content of the entire set of HTML pages can be easily controlled using one or more style sheets. CSS provides easy means to update document formatting and maintain consistency across multiple documents. It is easy for maintenance. Pages load faster as CSS enables multiple pages to share formatting, and reduce complexity and repetition in the structural content .Another advantage is that it saves a lot of time because it enables reuse of the code written once. CSS has much wider presentation capabilities than html hence it is possible to give better look to the html pages. Using CSS the same html document can be presented in different viewing styles for different rendering devices.

CSS can also allow the same mark-up page to be presented in different styles for different rendering methods, such as on-screen, in print, by voice (when read out by a speech-based browser or screen reader) and on brail-based, tactile devices. It can also be used to allow the web page to display differently depending on the screen size or device on which it is being viewed. While the author of a document typically links that document to a CSS file, readers can use a different style sheet, perhaps one on their own computer, to override the one the author has specified. However, if the author or the reader did not link the document to a specific style sheet the default style of the browser will be applied.CSS specifies a priority scheme to determine which style rules apply if more than one rule matches against a particular element in this so-called cascade, priorities or weights are calculated and assigned to rules, so that the results are predictable.

Some of the Advantages of CSS is as follows –

- **Saves time:** With CSS, you only have to specify these details once for any element. It will automatically apply the specified styles whenever that element occurs.
- **Pages load faster:** Less code means faster download times. And faster website loading time.
- **Appearance:** It makes it easy to improve the appearance of a website .By using it you can build well or good looking layouts. It helps to increase user experience.
- **Easy maintenance:** To change the style of an element looks across the whole site, you only have to make an edit in one place and your change will appeared on front-end .
- **Bandwidth savings:** Using CSS instead of tables for layout, a website can reduce its file sizes by up to 45%. This means decreased bandwidth costs. So it helps in load speed also.

4.2.2 BACK END

MySQL

MySQL is the world's second most widely used open-source relational database management system (RDBMS). The SQL phrase stands for Structured Query Language. The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation. MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP (Linux, Apache, MySQL, Perl/PHP/Python) open source web application software stack (and other 'AMP' stacks). Free-software-open source projects that require a full featured database management system often use MySQL. For commercial use, several paid editions are available, and offer additional functionality. Applications which use MySQL databases include: TYPO3, MODx, Joomla, Word Press, phpBB, Drupal and other software. MySQL is also used in many high-profile, large-scale websites, including Wikipedia, Google(though not for searches), Facebook, Twitter, Flickr.

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation. MySQL is a database management system. A database is a structured collection of data. It may be anything from a simple

shopping list to a picture gallery or the vast amounts of information in a corporate network. To add, such as MySQL Server. Since computers are very good at handling large amounts of data, database management system.

MySQL is a free, open-source database management system. A DBMS is a system that manages databases and connects them to software. For example, a MySQL database can be used to run a website, to run the database of an ERP or any other software. MySQL is a powerful, free open-source database management system that has been around for years. It is very stable and has a big community that helps maintain, debug and upgrade it. MySQL might not be as popular for larger systems that will mostly run on Microsoft SQL Server or Oracle. These proprietary DBMS are more scalable, have more resources available on the market and have more advanced features that MySQL.

Features of MySQL

The following list shows the most important properties of MySQL.

- **Relational Database**

  Like most all other database systems on the market, MySQL is a relational database system.

- **Client/Server Architecture**

  MySQL is a client/server system. There is a database server and arbitrarily many clients, who communicate with the server; that is, they query data, save changes etc. The clients can run on the same computer as the server or on another computer. Almost all of the familiar large database systems such as Oracle, Microsoft SQL Server etc are client/server systems.

- **SQL Compatibility**

  MySQL supports as its database language as its name suggests- SQL (Structured Query Language). SQL is a standardized language for querying and updating data and for the administration of the database. There are several SQL dialects. MySQL adheres to the current SQL standard although with significant restrictions and large number of extensions.

- **Scalability and Limits**

  Support for large databases. We use MySQL server with databases that contain 50 million records. Support for up to 64 indexes per table. Each index may consist of 1 to 16 columns or parts of columns. The maximum index width is 767 bytes for InnoDB tables, or 1000 for MyISAM. An index may use a prefix of a column for CHAR, VARCHAR, BLOB or TEXT column types.

- **Clients and Tools**

  The MySQL server has built-in support for SQL statements to check, optimize and repair tables. These statements are available from the command line through the mysqlcheck client. MySQL also includes myisamchk, a very fast command-line utility for performing these operations on MyISAM tables. All MySQL programs can be invoked with the –help or -? options to obtain online assistance.

- **Security**

  A privilege and password system that is very flexible and secure and that allows host based verification. Passwords are secure because all password traffic is encrypted when you connect to a server.

- **Web and Data Warehouse Strengths**

  MySQL is the de-facto standards for high traffic websites because of its high performance query engine, tremendously fast data inserting capability and strong support for specialized web functions like fast full text searches.

The importance of MySQL database management system for this project are as follows –

- MySQL is used to handle the data entered in the database in each phase of the software program. It is mainly used for maintaining the data entered in the database.
- It helps in connecting the database with the application. Since SQL is a standardised language, it is used for querying and updating the changes in the database and also enables easy communication with the server.
- MySQL is considered to be the fastest database program.

- It has a user friendly user interface which helps in creating better and efficient database system for the project with ease.

4.3 IDE

NetBeans IDE

In computer programming, NetBeans is a multi-language software development environment NetBeans is an open-source integrated development environment (IDE) for developing with Java, PHP, C++, and other programming languages. NetBeans is alsoreferred to as a platform of modular components used for developing Java desktopapplications. NetBeans is coded in Java and runs on most operating systems with a JavaVirtual Machine (JVM), including Solaris, Mac OS, and Linux.

NetBeans manages the following platform features and components:

- User settings
- Windows (placement, appearance, etc.)
- NetBeans Visual Library
- Storage
- Integrated development tools
- Framework wizard

NetBeans uses components, also known as modules, to enable software development. NetBeans dynamically installs modules and allows users to download updated features and digitally authenticated upgrades. NetBeans IDE modules include NetBeans Profiler, a Graphical User Interface (GUI) design tool, and NetBeans JavaScript Editor. NetBeans framework reusability simplifies Java Swing desktop application development as well as Java web application development, which provides platform extension capabilities to third-party developers.

The NetBeans is considered to be the best choice among other IDEs for the project for many reasons. It is used for easy and efficient coding since it can indent lines, match words and brackets, and highlights source code syntactically and semantically. It allows easy refactor code, with a range of handy and powerful tools. It also provides code templates, coding tips, and code generators. Moreover, NetBeans supports many languages from Java, HTML,

JavaScript, JSP, etc. which are considered to be the core programming languages used in the project. When new developer joins the project, they can understand the structure of the application since it is well organized.

Other advantages include writing bug free codes.in addition Netbeans Debugger lets you place breakpoints in your source code, run into methods, etc. The NetBeans profiler provides expert assistance for optimizing the application's speed and memory usage. It also includes visual debugger for Java SE applications, which enables debugging the user interface without looking into the source code.

4.4 WEBSERVER

Apache Tomcat

Apache Tomcat is a web server that is an open source software implementation of the Java Servlet and Java Server Pages technologies. The Java Servlet and Java Server Pages specifications are developed under the Java Community Process. Apache Tomcat is developed in an open and participatory environment. Apache Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. Apache Tomcat powers numerous large-scale, mission-critical web applications across a diverse range of industries and organizations

Apache Tomcat is an open source software implementation of the Java Servlet and Java Server Pages technologies. The Java Servlet and Java Server Pages specifications are developed under the Java Community process. Apache Tomcat, Tomcat, Apache, the Apache feather, and the Apache Tomcat project logo are trademarks of the Apache Software Foundation.

5. SYSTEM DESIGN

5.1 MODULES

The CloudSec system consists of two modules:

- User module
- Admin module

5.1.1 USER MODULE

User module consists of a user interface page. They can enter the site directly. The user has to follow the steps as shown below:

- Registration Module
- QR Code Generator Module
- Login Module
- File upload
- File download
- Water Marking Module

5.1.1.1 Registration Module

- User has to register into the system using providing a username, IMEI number and other personal information.
- User is provided with a QR code that is generated when the IMEI number is provided.
- User also has to select the image and a grid from the selected as the password for uploading or downloading a file.

5.1.1.3 QR Code Generator Module

- After the username and IMEI Number is provided, QR code is generated in the computer.
- User has to scan the QR code using mobile phone during logging into the storage and also during the uploading and downloading of the file.

5.1.1.2 Login Module

- User has to login into the system by providing the username and password.
- User is subjected to scan the QR code using a smart phone for IMEI verification for accessing the data.
- User also has to choose the grid that was chosen during the registration phase which serves as a password for uploading and downloading a file.

5.1.1.4 Watermarking Module

- The image that is chosen by the user as the password is watermarked with a cover image using generic visible watermark embedding algorithm.

5.2.1 ADMIN MODULE

The cloud service providers are the admin of this system. The main tasks of the admin are as follows:

- Provides security on user data in the cloud.
- Provides timely update and maintenance on the cloud storage.
- Provides on-time cloud services to user.
- Provides 24/7 customer services and IT help desk.

5.2. DATA FLOW DIAGRAM

A data flow diagram is a graphical tool used to describe and analyze movement of data through a system. These are the central tool and the basis from which the other components are developed. The transformation of data from input to output, through processed, may be described logically and independently of physical components associated with the system. These are known as the logical data flow diagrams. The physical data flow diagrams show the actual implements and movement of data between people, departments and workstations. A full description of the system actually consists of a set of data flow diagrams. Using two familiar notations Yourdon, Game and Samson notations develop the data flow diagrams. Each component in a DFD is labelled with a descriptive name. Process is further identified with a number that will be used for identification purpose. The development of DFD'S is done in several levels. Each process in lower level diagrams can be broken down in to a more detailed DFD in the next level. THE top-level diagrams is

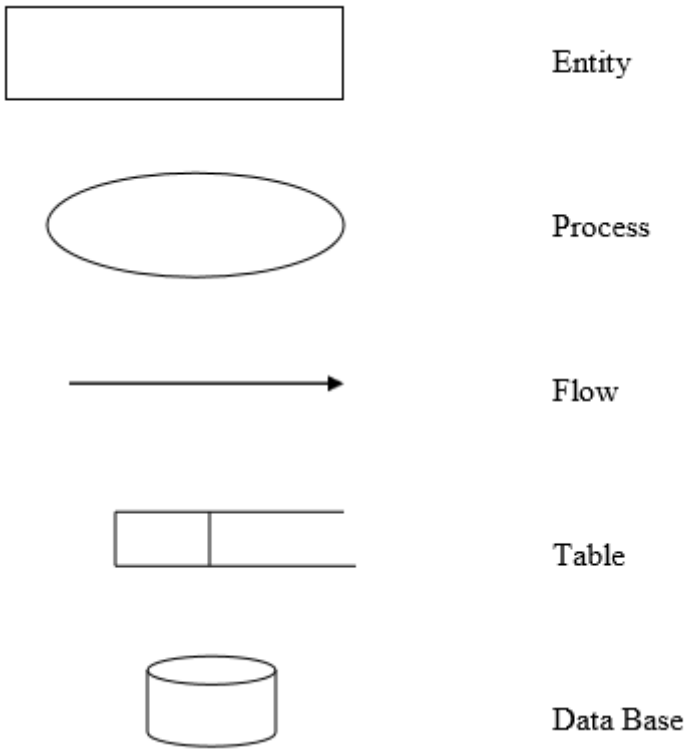
often called context diagram. It consists of a single process bit, which plays vital role in studying the current system. The process in the context level diagram is exploded into other process at the first level DFD.

A DFD is also known as a “bubble Chart” has the purpose of clarifying system requirements and identifying major transformations that will become programs in system design. So it is the starting point of the design to the lowest level of details. A DFD consist of a series of bubbles joined by a data flows in the system.

DFD symbols:

In DFD there are 4 symbols

1. A square defines an entity
2. An arrow identifies data flow. It is the pipeline through which the information flows
3. An ellipse which represents a process that transforms incoming data flow into outgoing data flows
4. An open rectangle is a table
5. A magnetic disk represents data base

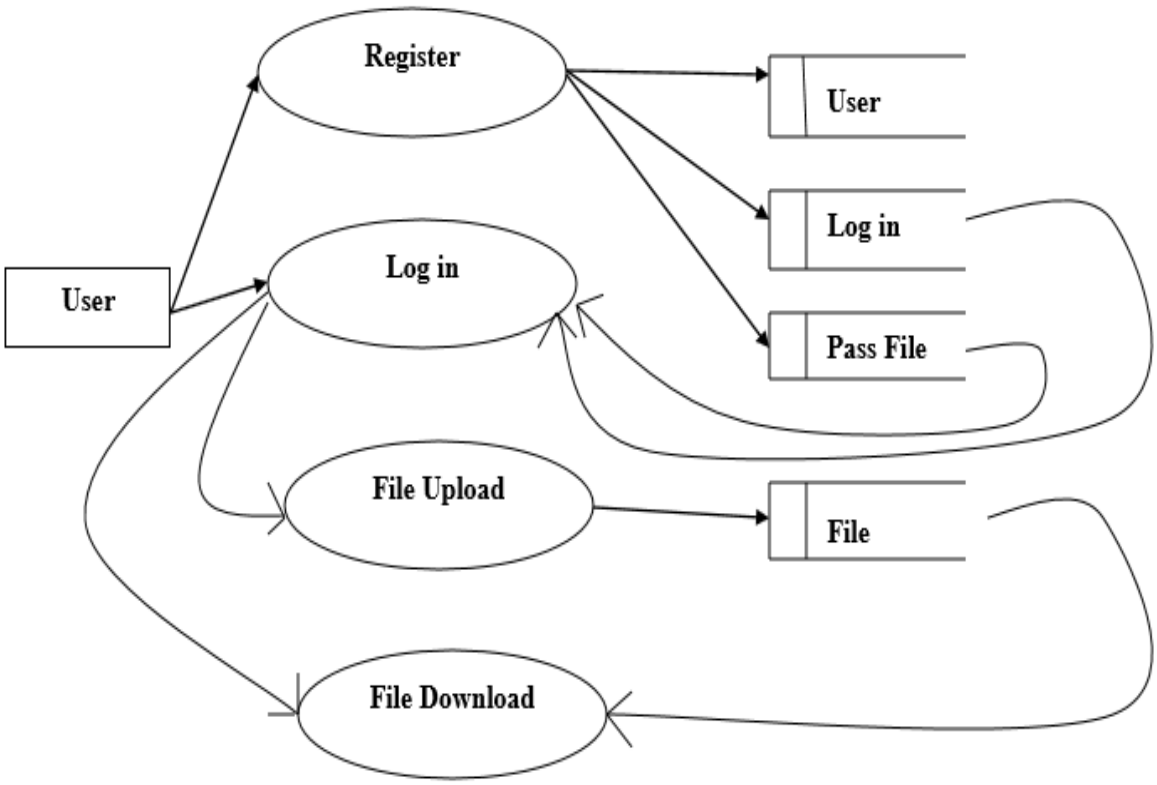


LEVEL 0

Fig 5.2.1 Level 0 DFD

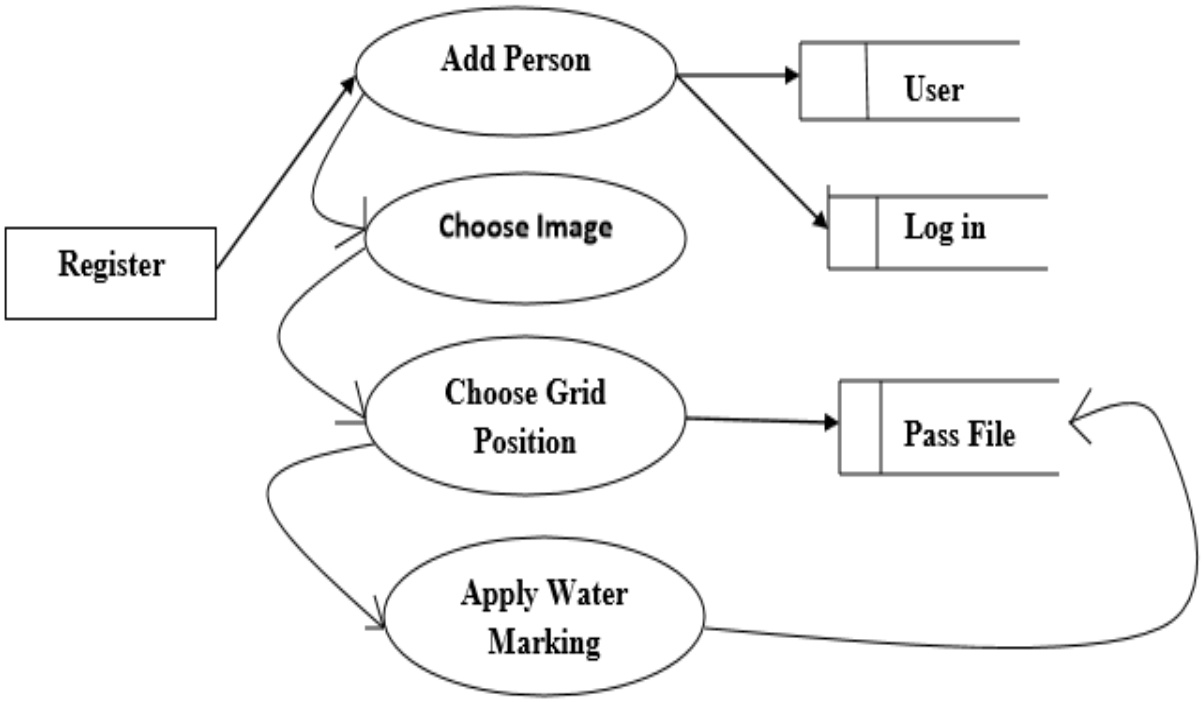
LEVEL 1

FIG 5.2.2 Level 1 DFD



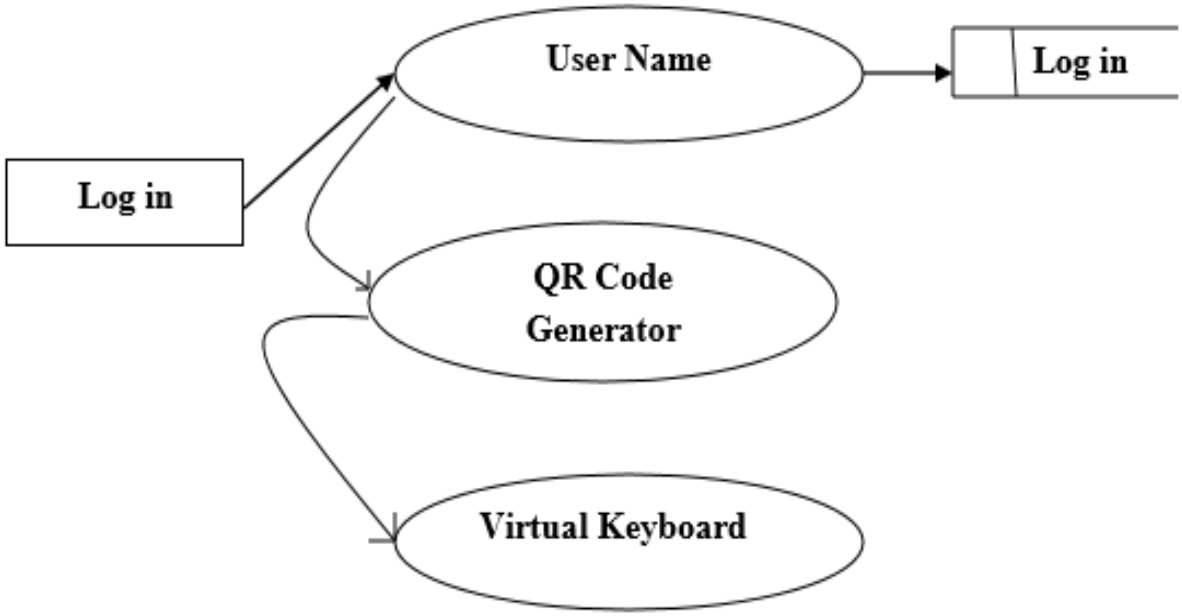
LEVEL 1.1

Fig 5.2.2.1 Level 1.1 DFD



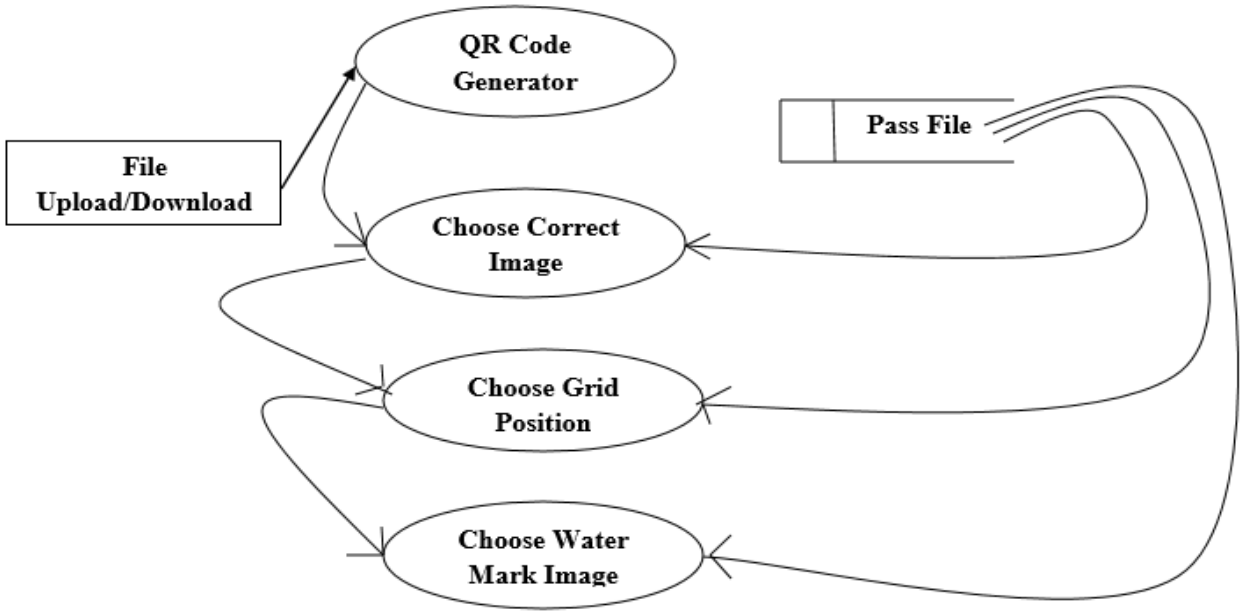
LEVEL 1.2

Fig 5.2.2.2 Level 1.2 DFD



LEVEL 1.3

Fig 5.2.2.3 Level 1.3 DFD



6. DATABASE DESIGN

Database design is required to manage the large bodies of information. The management of data involves both the definition of structure of information and provisions of mechanism for the manipulation of information. In addition the database system must provide for the safety of information handled, despite the system crashes due to attempts of unauthorized access. For developing an efficient database, we will have to fulfill certain condition such as:

- Control redundancy.
- Ease of use.
- Data independence.
- Accuracy and integrity.
- Avoiding inordinate delays.
- Recovery from failure.
- Privacy and security.
- Performance.

There are 6 major steps in design process. The first 5 steps are usually done on paper and finally the design is implemented.

- Identify the tables and relationships.
- Identify the data that is needed for each table and relationship.
- Resolve the relationship.
- Verify the relationship.
- Implement the design.

Normalization

Normalization is the process of analyzing the given relation schemas based on their functional dependencies and primary keys to achieve the desirable properties of

- Minimizing Redundancy
- Minimizing the insertion, deletion and updating anomalies.

Normalization is carried out for the following reasons:

- To structure the data so that perfect relationship between entries can be represented.
- To permit simple retrieval of data in response query and report requests.
- To reduce the need to restructure or reorganize data when new application requirement arises.

Normalization consists of various levels:

1. First Normal Form (1NF)

A table is in 1NF if there are no duplicate rows in the table. Each cell is single valued. Entries in a column are of the same kind.

2. Second Normal Form (2NF)

Second Normal Form is based on the concept of full functional dependency. A table (relation) is in 2NF if

It is in First normal Form and if all non-key attributes are dependent on the key.

Dependent on only a part of the (composite) key, the definition of 2NF is sometimes phrased as "A table is in 2NF if it is in 1NF and if it has no partial dependencies.

3. Third Normal Form (3NF)

Third Normal Form is based on the concept of transitive dependency. A table (relation) is in 3NF if it is in Second Normal Form and if it has no transitive dependencies.

User Interface Design

User Interface Design is the design of computer, appliances, machines, mobile communication devices, software applications, and websites with the focus on user's experience and interaction. The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals-what is often called user-centered design. Good user interface design facilities finishing the task at hand without drawing unnecessary attention to itself. Graphic design may be utilized to apply a theme or style to the interface without compromising its usability. The design process of an interface must balance the meaning of its visual elements that confirm the

mental model of operation, and the functionality from a technical engineering perspective, in order to create a system that is both usable and easy to adapt to the changing user needs.

User Interface Design is involved in a wide range of projects from computer systems, to cars, to commercial planes; all of these projects involve much of the same basic human yet also require some unique skills and knowledge. As a result, user interface designers tend to specialize in certain types of projects and have skills centred around their expertise, whether that be software design, user research, web design, or industrial design.

Process Design

"Process Design" (in contrast to "design process") refers to the planning of routine steps of a process aside from the expected result. Processes (in general) are treated as a product of design, not the method of design. The term originated with the industrial designing of chemical processes. With the increasing complexities of the information age, consultants and executives have fund the term useful to describe the design of business processes as well as manufacturing processes.

System Objective

- Proposed system can easily overcome the drawbacks in the existing system.
- The time consumption will be less and performance of the proposed system is high.
- The system can be designed in such a way that it is interactive and user friendly. Easy data input storing that makes the system easy.
- The probability of occurrence of error is negligible.

  The proposed system ensures:

  - Synchronization of files across different systems.
  - Easy view and restore.
  - Remote access to files from anywhere.

user_id	name	DOB	email_id
1	jinsha	23/9/1996	jinshaktly@gmail.com
2	ansha	12/5/1998	anshapavithran@gmail.com
3	aaradhya	27/3/2008	aaradhyadhanesh@gmail.com
4	devangena	27/3/2008	devangenadhanesh@gmail.com
5	shaarav	13/9/2012	shaaravmanoj@gmail.com

Fig. 6.1 User Table

user_id	username	password	IMEI	IMEI_backup	no_of_imag
1	jini	jini	a23456789012345	123456789012345	2
2	anu	anu	94958	94105	3
3	aaradhya	aaradhya	80861	78520	2
4	deva	deva	545434543454345	565634543454345	2
5	shaarav	shaarav	12345	54321	2

Fig. 6.2 Log in Table

user_id	image	image_feature	watermarking_image	file_id	file_index
1	file_949525_1.jpg	12	(NULL)	1	1
1	file_949525_2.jpg	0	water_949525_2.jpg	2	2
2	file_94958_1.jpg	2	(NULL)	3	1
2	file_94958_2.jpg	2	(NULL)	4	2
2	file_94958_3.jpg	7	water_94958_3.jpg	5	3
3	file_80861_1.jpg	22	(NULL)	6	1
3	file_80861_2.jpg	15	water_80861_2.jpg	7	2
4	file_049023_1.jpg	6	(NULL)	8	1
4	file_049023_2.jpg	17	water_049023_2.jpg	9	2
5	file_12345_1.jpg	17	(NULL)	10	1
5	file_12345_2.jpg	29	water_12345_2.jpg	11	2

Fig. 6.3 Pass_file Table

7. COST ESTIMATION

COCOMO(Constructive Cost estimation Model)was proposed by Boehm, ,1981.Boehm provides different sets of expressions to predict the effort (in units of person months) and development time from the size estimation given in KLOC(kilo lines of source code).The expression for basic COCOMO model is given by

Effort= a1* (KLOC)^{a2} PM

Tdev = b1 * (Effort)^{b2} Months

KLOC is the estimated size of the software product expressed in kilo lines of source code.

a1,a2,b1,b2 are constants

Tdev is the estimated time to develop the software expressed in months .Effort is the total effort required to develop the software product expressed in person months.

There are many classes of software product, we consider the semidetached product , so

Effort = 3.0 (KLOC)$^{1.12}$ PM

Tdev = 2.5 (Effort)$^{0.35}$ Months

Assume that size of our semidetached software product has been estimated to be 600 lines of source code .Assume that the average spending is Rs.1500 per month

From the basic COCOMO estimation formula for semidetached software:

Effort = 3.0 * (7.3)$^{1.12}$ = 27.8 PM

Tdev = 2.5 * (27.8)$^{0.35}$ = 8 Months

Cost = 8 * 1500 = 12000

8. SCREENSHOTS

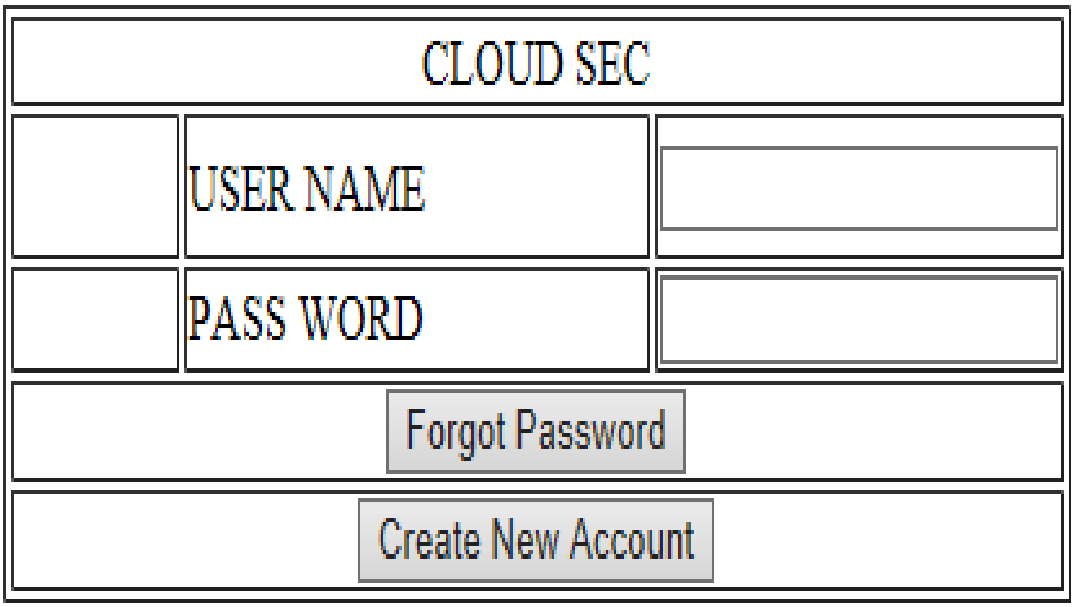


Fig 8.1 Home Page

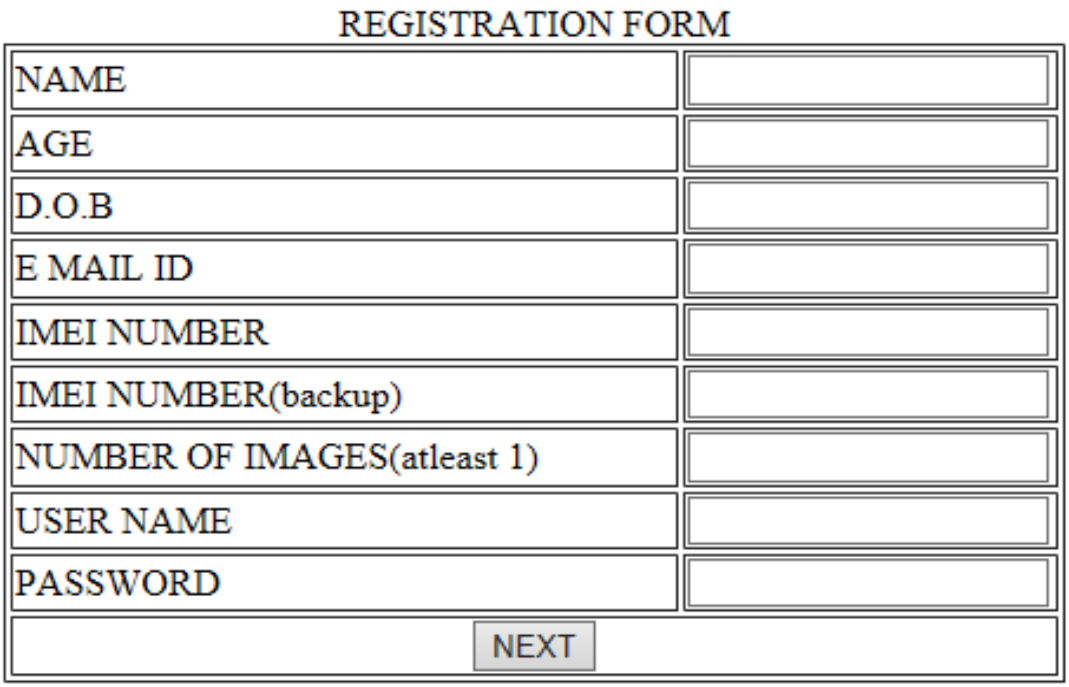


Fig 8.2 Registration Form

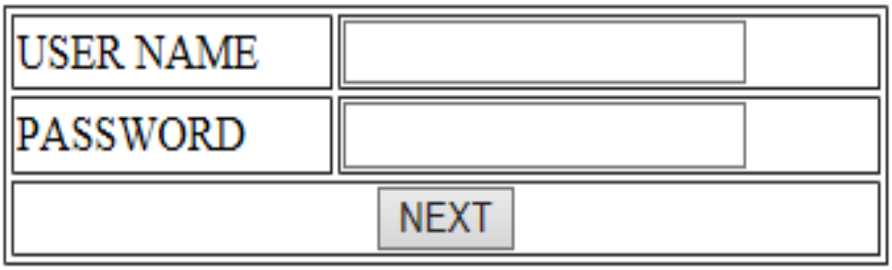


Fig 8.3 Log in Page

9. SYSTEM TESTING

Testing is vital to the success of the system. Testing makes a logical assumption that all the parts of the system are correct; the goal will be successfully achieved. The user tests the developed system and changes according to the need. Inadequate testing leads to errors that may not appear until months later.

This helps in the prevention of errors in a system and builds confidence that the system will work without error after testing. It is the process of executing a program with the intent of finding an error. Testing adds value to the product by conforming to the user requirements. Testing involves a series of operation of a system or application under controlled conditions and subsequently evaluating the results. The controlled condition should include both normal and abnormal conditions. The philosophy behind testing was to find errors. A set of sample data is processed in this system as a normal input. However data created the express internet of determining whether the system will process correctly. The software was tested for 2 strategies, code testing and specification testing.

Code testing strategy examined the logic of the program. Executing every path through the program is tested. Running each program separately did specification testing and verifies how it performed under various conditions. They were developed for each condition or combination of condition seemed satisfactory.

Testing objectives

The objectives of testing are:

1. Testing is the process of finding error in existing program.

2. A good test can is the one that has high probability of finding as yet undiscovered error.

3. A successful set of error is one that uncovers an as yet undiscovered error.

System testing is the implementation, which ensures that the system works accurately and efficiently before live operations commence. During the development of a software project, errors of various types can occur at any stage. System testing makes logical assumption that the system is correct and that the goals are successfully achieved.

The first major hurdle in the process of implementation is the period of testing the system. The debugging part is the most unpredictable part of the testing procedure. To make the system reliable and accepted, various testing methods were used, the most basic of them being the three mentioned below:

a) Running the program to identify any error(whether syntactic or semantic)that might have occurred while feeding the programs into the system.

b) Applying the screen formats to regulate users to gauge the extent to which the screen was comprehensible to the user.

c) Presenting the format to the administrator for the purpose of obtaining approval and checking if any modifications have to be done or whether the proposed serves their purpose.

Testing is carried out in order to ensure that the system does not fail, that it meets the specification and it satisfies the user. The system testing was carried out in a systematic manner with the test data containing all the possible combinations of data to check the feature of the system. A test data was prepared for each module, which took care of all possible branches and sub procedures in the programs. During the first round of testing each module is tested individually because the fixing and rectification of the errors in this state would be easier.

Any software can be tested in any of the following two ways.

- White Box Testing
- Black Box Testing

WHITE BOX TESTING

White box testing of software is predicted on a close examination of procedural detail. The status of program may be tested to various points to determine whether the expected or asserted status. Using the following test can be derived.

- All independent paths within the module have been exercised at least once.
- All logical decisions are exercised for their true and false values.
- All loops are tested at their boundaries.
- All the internal data structures are exercised in their validity.

This software has much validation and testing to be done. There are many forms which takes only certain values, database checking etc. has to be done here.

The system checking for forms were done by providing different values, such as the registration form has password and confirm password fields are same. And query details field checks the user email id should contain the dot and at the rate of symbol.

BLACK BOX TESTING

Black box testing focuses on the functional requirements of the software. It is complementary approach i.e. likely to uncover a different class of error than white box method.

Black box testing attempts to find the errors in the following categories:

- Incorrect or missing function.
- Interface errors.
- Error in data structure or database.
- Performance errors.
- Initialization errors.
- Termination errors.

A black box testing examines some aspects of a system with little regard for the internal logical structure of the software.

Black box testing is complementary to the white box testing. This testing is done after the completion of the software the system is first run completely. During this time we try to find any errors are there in the forms error, loading error, interface errors etc are there or not. In our system there was loading problem which was later successfully rectified.

9.1 TESTING STRATEGIES

A strategy for software testing integrates software test case design methods into a well-planned series of steps that result in the successful completion construction of software. A software testing strategy provides a road map for the software developer, the quality assurance organization, and the customer.

A software product goes through 3 levels of testing:

- Unit Testing
- Integration Testing
- System Testing
- Output Testing
- User Acceptance Testing

9.1.1 UNIT TESTING

Unit testing verification efforts on the smallest unit of software design, the module. This is also known as "Module Testing". The modules are tested separately. This testing is carried out during programming stage itself. Unit testing exercises specific paths in a modules control structure to ensure complete coverage and maximum error detection. Unit testing is the testing of different units or modules of the system in isolation. Unit testing is undertaken when a module has been coded and successfully reviewed. In order to test a single module we need a complete environment to provide all that is necessary for execution of the module. That is besides the module under test will need the following in order to be able to test the modules.

- The procedures belonging to other modules that the module under test calls.
- Non local data structures that the module accesses.
- A procedure to call the functions of the module under test with appropriate parameters.

The front end design consists of various forms they were tested for data acceptance. Similarly the back-end that is the database was also tested for the successful acceptance and retrieval of data.

9.1.2 INTEGRATION TESTING

The primary objective of the integration testing is to test the module interfaces in order to ensure that there are no errors in the parameter passing, when one module invokes another module. During integration testing, different modules of the system are integrated in a planned manner using an integration planning. The integration plan specifies the steps and the order in which modules are combined to realize the full system. After each integration

step, the partially integrated system is tested. Correction is difficult because the isolation of causes is complicated by the vastness of the program.

Using integration test plan prepared in the design phase of the system development as a guide, integration test is carried out and all the errors found in the system are corrected for next testing steps.

9.1.3 SYSTEM TESTING

System test are designed to validate a fully developed system to assure that it meets its requirements. In this testing system is tested by team within the organization, group of friendly customers, then customer itself.

9.1.4 OUTPUT TESTING

After performing the validation testing the next step is output testing of the proposed system, since no system could be useful if it does not produce the required output in the specified format. The outputs generated or displayed by the system under consideration are tested by asking users about the format required by them. Hence the output format is considered in two ways. One is on screen and another is printed format.

9.1.5 ACCEPTANCE TESTING

User acceptance of a system is a key factor to the success of a system. The system under consideration was tested for user acceptance by constantly keeping in the prospective system user at the time of developing and making changes whenever required. This is done with regard to the following points:

- Input screen design
- Output screen design
- Event-driven system

9.2 MAINTAINANCE

Software maintenance is a set of software engineering activities that occur after software has been delivered for the customer and put into operation. The success of the software and the project relies on the maintenance procedure adopted. As with the venture of human, not a single one is perfect. The further modifications are left to the followers. It is because of the

opinion or vision of a thing differs from individual to individual. Development is a single activity. Maintenance is a continuous activity. Maintenance involves activities like inspections, corrections and enhancements. Once the system is delivered and deployed, it enters the maintenance phase. The system need to be maintained not because of some of its components wear out and need to be replaced, but they are discovered. This includes activities related to debugging the software after it goes live, changes required to address evolving software and enhancement to meet changing customer requirements. So maintenance phase involves:

- Understanding the effects of the change
- Testing the new parts
- Retesting the old parts that were not changed
- Making changes to both the code and the documents

These changes have to be signed by the user before the change can be carried out. Since requirement change request involves cost, user will be cautious while requesting the software changes. The software will require continuous support. The system maintenance means the maintenance activities after and during the system development processes. This include activities related to debugging the software after it goes live, changes required to meet changes in user requirement.

Maintenance phase identifies if there are any changes required in the current system. If the changes are identified, then an analysis is made to identify if the changes are really required. Cost benefit analysis is a way to find out if the change is really essential. The maintenance is performed at regular intervals to keep the project safe and reliable. Maintenance covers a wide range of activities including correcting codes, design errors, updating documentation and test data and updating user support. The software will change or modify with user requirements in future.

10. CONCLUSION

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder-surfing attacks. Even a complicated password can be cracked easily through shoulder-surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones.

To overcome this problem, we proposed a shoulder-surfing resistant and key-logger authentication system based on graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder-surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. Furthermore, we implemented a PassMatrix prototype on Android and carried out user experiments to evaluate the memorability and usability.

We also use a colour password authentication scheme. Colour password can be used only once and every time a new password is generated.

11. FUTURE ENCHANCEMENTS

The future scope of CloudSec website is made in such a way that the users find it easy to use the website than the present schemes. In the future scope, we intend to upgrade the virtual keyboard with iris scanning and the visual authentication protocol with the fingerprint scanning protocols. This is possible since all the smartphones available consists of iris scanner and fingerprint scanner. These implementations further enhance cloud security in our website.

The future enhancements can be used only in high-end devices. This is because of the reason that high- end devices consists of both built-in fingerprint and iris scanning equipments. The fingerprint scanning and iris scanning protocols helps the user to use their cloud storage seamlessly and allows them to access their data without consuming more time. Hence the future scope enhances the present scheme by changing the complex protocols with easy ones.

-

12. REFERENCES

[1] M. Ahmadi, M. Chizari, M. Eslami, M. J. Golkar and M. Vali, "Access control and user authentication concerns in cloud computing environments," 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), Kuala Lumpur, 2015.

[2] F. Sabahi, "Cloud computing security threats and responses," 2011 IEEE 3rd International Conference on Communication Software and Networks, Xi'an, 2011, pp. 245-249.

[3] J. L. Tsai and N. W. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," in IEEE Systems Journal, vol. 9, no. 3, pp. 805-815, Sept. 2015.

[4] A. J. Choudhury, P. Kumar, M. Sain, H. Lim and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," 2011 IEEE Asia-Pacific Services Computing Conference, Jeju Island, 2011, pp. 110-115.

[5] L. Jiang, X. Li, L. L. Cheng and D. Guo, "Identity authentication scheme of cloud storage for user anonymity via USB token," 2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID), Shanghai, 2013, pp. 1-6.

[6] Hong, Sunghyuck. "Two-channel user authentication by using USB on Cloud", Journal of Computer Virology and Hacking Techniques, 2015. [7] H.Y.Chien, J.K. Jan, Y.M. Tseng, “An efficient and practical solution to remote authentication: Smart card”, Computers & Security 2002.

[7] Hwang, M.S. "A simple remote user authentication scheme", Mathematical and Computer Modelling, 200207.

[8] Abdellaoui, Abderrahim, Younes, Idrissi,Khamlichi, and HabibaChaoui. "A Novel Strong Password Generator for Improving Cloud Authentication", Procedia Computer Science, 2016

[9] Li, Chun-Ta. "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card", IET Information Security, 2013.

[10] Ronggong Song, "Advanced smart card based password authentication protocols", Computer Standards & Interfaces, vol.32(5-6), pp.321-325, 2010.

[11] SunghoKim ,EunjunYo, KeeyonugYoo, " A security enhanced remote user authentication scheme using smart cards", International Journal of Innovative Computing Information and Control 2012.

[12] Yung Cheng Chan , Chun I Fan, Zhi Kai Zhang, " Robust remote authentication scheme with smart cards", Computers &SecurityVolume 24, Issue 8, November 2005.

[13] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 102–127, 2005.

[14] S. Lee, I. Ong, H.T. Lim, H.J. Lee, "Two factor authentication for cloud computing", International Journal of KIMICS, vol 8, Pp. 427-432

[15] Z. Shen, L. Li, F. Yan, X. Wu, "Cloud Computing System Based on Trusted Computing Platform", Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on , vol 1, Pp 942-945.

[16] A. Celesti, F. Tusa, M. Villari, A Puliafito, "Security and Cloud Computing: InterCloud Identity Management Infrastructure", 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 , Pp 263-265.

[17] S. A. Almulla, C. Y. Yeun," Cloud Computing security Management", IInd International Conf. engg systems management and its applications(ICESMA),2010.

[18] L. Lamport, "Password authentication with insecure communication," Comm. ACM 24(11), Nov 1981, 770–771.

[19] M.S.Hwang, and L.H. Li, "A New Remote User Authentication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics 46 (1) (2000) 28-30.

[20] M.K. Khan, "Cryptanalysis and Security Enhancement of Two Password Authentication Schemes with Smart Cards", Multi topic Conference, 2007. INMIC 2007. IEEE International.

[21] H.Y. Chien, J.K. Jan, Y.M. Tseng, "An efficient and practical solution to remote authentication: Smart card," Comput. Secur. 21 (4) (2002) 372–375.

[22] I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, "A password authentication scheme over insecure networks," J. Comput. System Sci. 72 (4) (2006) 727–740.

[23] E.J. Yoon, E.K. Ryu, K.Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," IEEE Trans. Consum. Electron. 50 (2) (May 2004) 568–570.

[24] E.J. Yoon, K.Y. Yoo, "New authentication scheme based on a one-way hash function and Diffie–Hellman key exchange," 4th International Conference of

Cryptology and Network Security, CANS 2005, LNCS vol. 3810, Springer-Verlag, 2005, pp. 147–160.

[25] M.-S. Hwang, "Cryptanalysis of remote login authentication scheme," Comput. Commun. 22 (8) (1999). Pp. 742–744.

[26] M.-S. Hwang, C.-C. Lee, Y.-L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," Internat. J. Inform. 12 (2) (2001).pp. 297–302.

[27] M. Scott, "Cryptanalysis of an id-based password authentication scheme using smart cards and fingerprints," SIGOPS Oper. Syst. Rev. 38 (2) (2004). Pp. 73–75.

[28] B. Wang, J.H. Li, Z.P. Tong, "Cryptanalysis of an enhanced timestamp-based password authentication scheme," Comput. Secur. 22 (7) (2003). pp. 643–645.

[29] E.J. Yoon, K.Y. Yoo, "New authentication scheme based on a one-way hash function and Diffie–Hellman key exchange," 4th International Conference of Cryptology and Network Security, CANS 2005, LNCS, vol. 3810, Springer-Verlag, 2005, pp. 147–160.

[30] V. Shoup, A. Rubin, "Session key distribution using smartcards", in: Proc. EUROCRYPT 96, in: LNCS., vol 1070, Springer-Verlag, 1996, pp 321-333

[31] M. Bellare, P. Rogaway, Provably secure session key distribution —The third party case, in: Proc. 27th ACM Symp. on Theory of Computing, ACM, Las Vegas, 1995, pp 57-66.

[32] G.Yang, D. S. Wong, H. Wang, X. Deng, "Two-factor mutual authentication based on smart cards and passwords", Journal of Computer and System Sciences, vol 74, 2008, Pp. 1160-1172.

[33] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proceedings of the 8th conference on USENIX Security Symposium-Volume 8*. USENIX Association, 1999, pp. 1–1.

[34] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical password- based user authentication with free-form doodles," *IEEE Transactions on Human-Machine Systems*, vol. PP, no. 99, pp. 1–8, 2015.

[35] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method re-silient against shoulder surfing," in *Proceedings of the 11th ACM conference on Computer and communications security*, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 236–245.

[36] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nichol- son, and P. Olivier, "Multi-touch authentication on tabletops," in *Proceedings of the 28th international conference on Human factors in computing systems*. ACM, 2010, pp. 1093–1102.

[37] Y. J. Cheng and W. H. Tsai, "A new method for copyright and integrity protection for bitmap images by removable visible watermarks and irremovable invisible watermarks," presented at the Int. Computer Symp.—Workshop on Cryptology and Information Security, Hualien, Taiwan, R.O.C., Dec. 2002.

[38] P.M.Huangand W.H.Tsai, "Copyright protection and authentication of gray scale images by removable visible watermarking and invisible signal embedding techniques: A new approach," presented at the Conf. Computer Vision, Graphics and Image Processing, Kinmen, Taiwan, R.O.C., Aug. 2003.

[39] Y. Hu, S. Kwong, and J. Huang, "An algorithm for removable visible watermarking," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 1, pp. 129–133, Jan. 2006.

[40] Y. Hu and B. Jeon, "Reversible visible watermarking and lossless recovery of original images," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 11, pp. 1423–1429, Nov. 2006.

[41] B.Macq ,"Lossless multi resolution transform for image authenticating watermarking," presented at the European Signal Processing Conf., Tampere, Finland, Sep. 2000. [13] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—New paradigmindigitalwatermarking,"J.Appl.SignalProcess.,vol.2002, no. 2, pp. 185–196, Feb. 2002.

[42] M. Awrangjeb and M. S. Kankanhalli, "Lossless watermarking considering the human visual system," presented at the Int. Workshop on Digital Watermarking, Seoul, Korea, Oct. 2003.

[43] M.Awrangjeb and M.S.Kankanhalli, "Reversible watermarking using a perceptual model,"J.Electron.Imag.,vol.14,no.013014,Mar.2005.

[44] C. de Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media assetmanagement,"IEEETrans.Multimedia,vol.5,no.1,pp.97–105, Mar. 2003.

[45] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[46] H. M. Tsai and L. W. Chang, "A high secure reversible visible watermarking scheme," in Proc. IEEE Int. Conf. Multimedia and Expo, Beijing, China, Jul. 2007, pp. 2106–2109.

[47] S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, "Lossless visible watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2006, pp. 853–856.

[48] Weis, J., Alves-Foss, J.: 'Securing database as a service: issues and compromises', IEEE Security Privacy, 2011, 9, (6), pp. 49–55. doi: 10.1109/ MSP.2011.127.

[49] Mario, G.: 'New challenges in teaching database security'. Proc. 3rd Annual Conf. Information Security Curriculum Development, Kennesaw, GA, USA, September 2006, pp. 64–67.

[50] Murray, M.C.: 'Database security: what students need to know', J. Inf. Technol. Educ., 2010, 9, pp. 61–77

[51] Prabavathy, B., Devi, M.S., Babu, C.: 'Multi-index technique for metadata management in private cloud storage'. Proc. 2013 Int. Conf. Recent Trends in Information Technology (ICRTIT), July 2013, pp. 84–89.

[52] Agrawal, A., Kiernan, J., Srikant, R., et al.: 'Order preserving encryption for numeric data'. Proc. 2004 ACM SIGMOD Int. Conf. Management of Data, Paris, France, June 2004, pp. 563–574.

[53] Boldyreva, A., Chenette, N., Lee, Y., et al.: 'Order-preserving symmetric encryption'. Proc. 28th Annual Int. Conf. Advances in Cryptology, Cologen, Germany, April 2009, pp. 224–241.

[54] Wang, C., Cao, N., Li, J., et al.: 'Secure ranked keyword search over encrypted cloud data', IEEE Int. Conf. Distributed Computing Systems, 2010, pp. 253–262.

[55] Tang, Q.: 'Privacy preserving mapping schemes supporting comparison'. Proc. 2010 ACM Workshop on Cloud Computing Security, New York, USA, October 2010, pp. 53–58.

[56] Boldyreva, A., Chenette, N., ONeill, A.: 'Order-preserving encryption revisited: improved security analysis and alternative solutions'. Proc. 31st Annual Int. Conf. Advances in Cryptology, Santa Barbara, USA, August 2011, pp. 578–595.

[57] Wang, C., Cao, N., Ren, K., et al.: 'Enabling secure and efficient ranked keyword search over outsourced cloud data', IEEE Trans. Parallel Distrib. Syst., 2012, 23, (8), pp. 1467–1479. doi: 10.1109/TPDS.2011.282

[58] Li, K., Zhang, W.M., Yang, C., et al.: 'Security analysis on one-to-many order preserving encryption-based cloud data search', IEEE Trans. Inf. Forensics Sec., 2015, 10, (9), pp. 1918–1926.doi: 10.1109/TIFS.2015.2435697

[59] Popa, R.A., Li, F.H., Zeldovich, N.: 'An ideal-security protocol for order preserving encoding'. Proc. 2013 IEEE Symp. Security and Privacy, Berkeley, USA, May 2013, pp. 463–477.

[60] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," http://eprint.iacr.org/2009/579.pdf.

[61] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy preserving and public auditing service for data storage in cloud computing," INFOCOM, 2010 Proceedings IEEE, pp. 1–9, 2010.

[62] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, Feb. 2013.

[63] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public Auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.

[64] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, Apr. 2012.

[65] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage," Computers & Electrical Engineering, vol. 40, no. 5, pp. 1703–1713, Jul. 2014.

[66] M. IK and S. George, "Cloud server storage security using TPA," International Journal of Advanced Research in Computer Science & Technology (IJARCST), 2014. [10] V. Tejaswini, K. Sunitha, and S. K. Prashanth, "Privacy preserving and public auditing service for data storage in cloud computing," Paripex - Indian Journal Of Research, vol. 2, no. 2, pp. 131–133, Jan. 2012.

[67] S. Jadhav and B. R. Nandwalkar, "Privacy preserving and batch auditing in secure cloud storage using AES," Proceedings of 13th IRF International Conference, 2014.

[68] A. S Ezhil, B. Gowari, and S. Ananthi, "Privacy-preserving public auditing in cloud using HMAC algorithm, "International Journal of Recent Technology and Engineering (IJRTE) ISSN, vol. 2277, 2013.

[69] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-based authentication for cloud computing,” in Proc. Cloud Comput., 2009, pp. 157–166.

[70] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, “A privacy preserving three-factorauthenticationprotocolfore-healthclouds,”J.Supercomput., 2016. DOI: 10.1007/s11227-015-1610-x.

[71] D.He,S.Zeadally, N.Kumar, and J.-H.Lee, “Anonymous authentication for wireless body area networks with provable security,” IEEE Syst. J., 2016. DOI: 10.1109/JSYST.2016.2544805.

[72] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Netw. Appl., vol. 8, no. 6, pp. 1070–1081, 2015

[73] J. L. Tsai and N. W. Lo, “A privacy-aware authentication scheme for distributed mobile cloud computing services,” IEEE Syst. J., vol. 9, no. 3, pp. 805–815, Sep. 2015.

[74] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. Adv. Cryptol., 2001, vol. 2139, pp. 213–229.

[75] K. Lauter, “The advantages of elliptic curve cryptography for wireless security,” IEEE Wireless Commun., vol. 11, no. 1, pp. 62–67, Feb. 2004.

[76] D. He, S. Zeadally, and L. Wu. “Certificateless public auditing scheme for cloud-assisted wireless body area networks,” IEEE Syst. J., 2015, DOI: 10.1109/JSYST.2015.2428620.

[77] C. Paar and J. Pelzl, Understanding Cryptography: A textbook for students and practitioners. Heidelberg: Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2009.

[78] S Dhanaya. Privacy preserving third partyauditing in cloud. Dissertation report, 2015.

[79] Mohan Atreya, Stephen Paine, Benjamin Hammond, Stephen Wu, and Paul Starrett. Digitalsignatures. Osborne/McGraw-Hill, 2002.

[80] S. More and S. Chaudhari, "Third party public auditing scheme for cloud storage," Procedia Computer Science, vol. 79, pp. 69–76, 2016. F. Hao.“ON ROBUST KEY AGREEMENT BASED ON PUBLIC KEY AUTHENTICATION” Proceedings of the 14th International Conference on Financial Cryptography and Data Security, Tenerife, Spain, LNCS 6052, pp. 383-390, Jan 2010.

[81] Arjun Kumar, Byung Gook Lee,Hoonjae Lee,Anu. ”SECURE STORAGE AND ACCESS OF DATA IN CLOUD COMPUTING ” IEEE 2012 P.336339.

[82] S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing” In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[83] Ankit Kumar Singh, Saroj Kumar and Abhishek Rai “Secure Cloud Architecture Based on YAK and ECC” International Journal of Computer Applications, ISBN 0975 – 8887 Volume 90, Number 19 (March 2014), pp. 29–33, © International Journal For Computer Application, http://www.ijca.org.

[84] Victor Rigworo Kebande, Kenneth Otula Sigar, George Yogo Odongo, “Meta-Modeling Cloud Computing Architecture in Distance Learning”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2013 ISSN (Print): 1694-0814, ISSN (Online): 1694-0784 www.IJCSI.org

[85] Pankaj Arora* Rubal Chaudhry Wadhawan Er. Satinder Pal Ahuja, “Cloud Computing Security Issues in Infrastructure as a Service”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.