Secure Banking Application with Image and GPS Location

Prachi B. Gund[1], Manasi M. Khude[2], Shivani P. Nalawade[3], Grunthali V. Tulaskar[4], S.H.Mujawar[5]

***

Introduction and Background of User Based Problem

1. Introduction

Recently there is tremendous growth in usage of Internet, it has become one of the most prominent channels for communication among the mass. Now a day's internet is main source for the communication and security of data over internet can be achieved through authentication, authorization and encryption of data. To be able to achieve successful communication very initial step is registration to the respective website. At the time of registration user's personal as well as financial information is registered and password is one of the essential steps to protect the user's sensitive information. Users are using passwords at many places like Banking, E-Commerce, and Online transaction. During authorization method all details of user like Email-id; bank account information is verified by respective websites. These all user's details are stored in database in conjunction with security. In spite of the fact that passwords are utilized to secure the points of interest of client's to keep away from the authorization but by stealing password by attacker or hacker without the knowledge of genuine user, critical information of user may be used illegally. Mishandling of user's personal and financial data could cause the huge loss of individual. User may be individual or any organization. However the dark side of internet has emerged this includes spam, malware, hacking, phishing, denial of service attacks, click fraud, invasion of privacy, defamation, frauds, violation of digital property rights, etc. The responses to the dark side of the Internet have included technologies, legislation, law enforcement; litigation, public awareness efforts, and etc. Therefore securing user's crucial data is become very important. User selects straightforward password for easy remembrance like name of beloved, birth date, etc. But it leads effortless cracking by attacker by brute force attack .Therefore it is very necessary to select tough password which should not be guessable. There are different policy to select strong password like never share login details ,never use identical password, never write down passwords, never communicates the password via Email, telephone etc. There are different authentication mechanisms like provided to secure online services and to avoid theft of information or misuse of the information.

Proposed system is the system where anyone who is trying to hack the system, whose desktop and laptop take the picture of the person and automatically it send the message to the email of the person whose data he is trying to access. The message will be sent as your account is at risk and this person is trying to access your account.

2. Literature Survey for Problem Identification Specification

2.1 Literature Survey

1. **Honeywords: A New Approach For Enhancing Security.**
   Author:- Manisha Jagannath Bhole Year:- 2015

Users reuse the passwords for login high important account and the reason behind that was it easy to remember also passwords were extremely weak: being too short, containing lowercase letters only, digits only or a combination of the two, or being easily found in dictionaries or lists of names. Typical computer user suffers from password overload. Users still need education and assistance when choosing passwords for important accounts. Algorithm Metropolis-Hastings that can guide users to distribute their passwords more uniformly without having to know a list of common passwords in advance. LinkedIn, Yahoo, and eHarmony these sites have been suffered from several high publicity password leaks. SHA-2 algorithm is cryptographically strong. New mechanism Honeywords to detect an adversary who attempts to login with cracked passwords.

2. **A Survey on Password Stealing Attacks and Its Protecting Mechanism.**
   Author:- Venkadesh .S, K.Palanivel Year:- 2015

People enjoy the convenience of on-line services, however on-line environments might bring several risks. In the on-line communication, the password has a crucial role to secure user personal details. These passwords are taken to be secure and it should be retain in person. The third person might take a password without knowledge of original user and they might do any dishonest activities on the victim's account. The passwords are taken by using anyone of the attack mechanism like Phishing attack, password Stealing Program Attack and etc… The user may use personal details in on-line setting. These personal details should be secured. There are many types of mechanisms available to secure the password and user's information. This paper makes a survey concerning such forms of protection mechanisms and brings awareness to the people.

3. **Honeywords: Making Password-Cracking Detectable.**
   Authors:-Ari Juels, Ronald L. Rivest Year:- 2013

We propose a simple method for improving the security of hashed passwords: the maintenance of additional "honeywords" (false passwords) associated with each user's account. An adversary who steals a file of hashed passwords and inverts the hash function cannot tell if he has found the password or a honeyword. The attempted use of a honeyword for login sets off an alarm. An auxiliary server (the "honeychecker") can distinguish the user password from honeywords for the login routine, and will set off an alarm if a honeyword is submitted.

4. **Password Guessing Resistant Protocol**
   Author:- Arya Kumar Year:- 2014

Attacks on passwords are increasing day by day. Brute force attack and dictionary attacks are the well known attacks. Automated Turing Test is effective approach to minimize such attacks and identify malicious logins. But sometimes it may create inconvenience to the authorized user as the user always has to cross or go through the ATTs. So to avoid such inconvenience, a new technique called Password Guessing Resistant Protocol (PGRP) is introduced. It overcomes the drawbacks of existing protocols like Pinkas and Sander. PGRP limit the total number of login attempts from unknown source IP address as low as three attempts and the user can make five failed login from the known and frequently used system. CAPTCHA, used is text based, logical and can also be image based. This could make the password guessing more difficult by the automated programs. Multiple ATTs are used to increase the security.

5. **Password Guessing Resistant Protocol for Securing System from Bots and Illegal Access.**
   Authors:- Arya Kumar, Prof. A.K.Gupta Year:- 2016

Attacks on passwords are increasing day by day. Brute force attack and dictionary attacks are the well-known attacks. Automated Turing Test (ATT) is effective approach to minimize such attacks and identify malicious logins. But sometimes it may create inconvenience to the authorized user as the user always has to cross or go through the ATTs. So to avoid such inconvenience, a new technique called Password Guessing Resistant Protocol (PGRP) is introduced. It overcomes the drawbacks of existing protocols. By using PGRP authorized users, who are logging from the known system doesn't have to undergo ATTs. The users who attempt to login from unknown system will have to pass through ATTs after three failed login attempts. This could make the password guessing more difficult by the automated programs as well as illegal access can be restricted to a great extent. ATTs, security questions and verification codes are used to increase security.

3. Proposed Detail Methodology and Solving the Identified Problem with Action Plan

3.1 Problem Statement

- To tackle the problem of brute force attack other attacks we introduced a system. Password Alert helps protect against phishing attacks.
- If you enter your Google Account password or Google for Work password into anywhere other than Google's sign-in page, you'll receive an alert, so you can quickly change your password if needed.
- Password Alert also checks each page you visit to see if it's impersonating Google's sign-in page, and alerts you if so.
- So if anyone is entering wrong password 3 times his picture will be captured and send to email id which he is cracking. Also a SMS is sent to the user saying please check your email someone is trying to access the account.

Problem Definition

To tackle the problem of phishing attack other attacks we introduced a system. Password Alert helps protect against phishing attacks. If you enter your Google Account password or Google for Work password into anywhere other than Google's sign-in page, you'll receive an alert, so you can quickly change your password if needed. Password Alert also checks each page you visit to see if it's impersonating Google's sign-in page, and alerts you if so. So if anyone is entering wrong password 3 times his picture will be captured and send to email id which he is cracking. . Also a SMS is sent to the user saying please check your email someone is trying to access the account.

Related Work

Passwords are used by user for authentication i.e. it is proof that he is really who he claims to be. Implementation of password but at the same time to save passwords from security threats is big challenge. If password is not fully protected then hacker can easily steal the password and can misuse it. With strong security, password formation is also very important i.e. password must be strong enough that it cannot be targeted by attacker by means of any attack like Brute force attack, Dictionary attack. Password cracking is the process of taking a captured password hash and converting it to its plaintext original. To break security of password, an attacker needs apparatus, for example, extractors for hash guessing, rainbow tables for looking up plaintext passwords, and password sniffers to extract authentication information. There are many techniques used for authorization. Though password is used in many forms like Graphics based password, Biometric based password, Token based password, Alphanumeric password etc. But among all alphanumeric passwords is more popular because of easy to remember and less complex in use. Providing security to text based password became very essential due to simple passwords used by user which are subject to attack.

3.2 Requirement Specifications

Software Requirements: -

1. Java
2. Android software
3. Php
4. Xampp server
5. My SQL
6. Cryptography

Hardware Requirements:-

1. Laptop

3.3 Proposed System

- **We are proposing a system that will provide a 2 layer security for our application:-**

Two-factor authentication (2FA) is a second layer of security to protect an account or system. 2FA increases the safety of online accounts by requiring two types of information from the user, such as a password or PIN, an email account, an ATM card or fingerprint, before the user can log in.

- **When someone tries to crack password of our application, maximum 3 failed attempts are allowed:-**

Brute force attacks involves repeated login attempts using every possible letter, number, and character combination to guess a password. An attacker using brute force is typically trying to guess one of three things: A user or an administrator password, a password hash key, or an encryption key.

- **After 3 attempts, the application will get blocked for 15 mins and the 2nd layer will be executed:-**

By default, the application allows users to enter passwords as many times as they want. To prevent this, you can limit the number of failed login attempts per user. For example, you can say after 3 failed attempts, lock the user out temporarily. If someone has 3 failed attempts, then the application block their IP for a temporary period of time based on your settings. You can make it 15 minutes, 24 hours, and even longer. We here had set it for 15 minutes.

- **The webcam will capture the image of the person trying to crack the account:-**

After the 3 unsuccessful attempts, the application will be blocked and the intruders image will be captured. And with the captured image even the location, date and time will also be stored into the database.

- **A SMS will be sent to the user:-**

Also a SMS will be sent to the user saying that please check your email someone is trying to hack your account.

- **All the details from the database will be sent to the email of the user:-**

Along with the details of the intruder stored in the database an email will be send to the owner. So that even if the intruder tries to erase the details it will be kept safe in the Gmail account of the owner. And the even the owner can report the incident to the nearby police station.

3.4 METHODOLOGY(Project Plan)

1. **Project estimate**

For a successful project we first need to estimate the various resources that are required to complete the project. Effective software project estimation is an important activity in any software development project. One of the main reasons software programs fail is our inability to accurately estimate software size. Because we almost always estimate size too low, we do not adequately fund or allow enough time for development. Poor size estimates are usually at the heart of cost and schedule overruns.

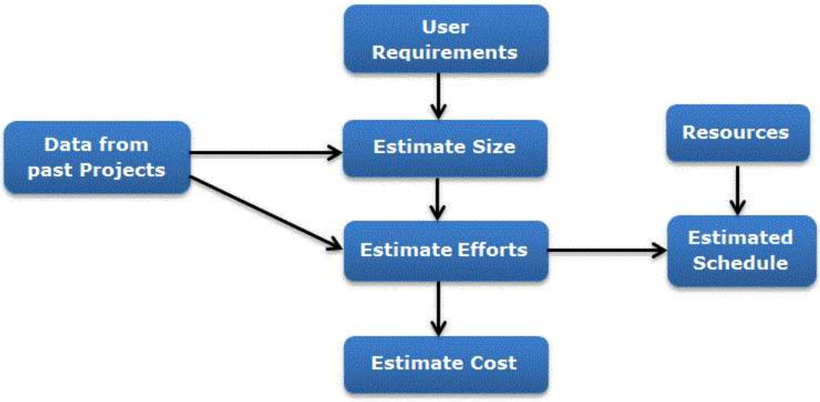

Fig.1:- Project Estimation

Step 1: Gather and Analyze Software Functional & Programmatic Requirements

In this step we Analyze and refine software requirements, software architecture, and programmatic constraints.

Responsible persons: *Software manager, system engineers, and cognizant engineers.*

Step 2: Define the Work Elements and Procurements

The purpose of this step is to define the work elements and procurements for the software project that will be included in the software estimate.

Responsible Persons: *Software manager, system engineers, and cognizant engineers.*

Step 3: Estimating the size of the project

Estimating the size of the software to be developed is the very first step to make an effective estimation of the project. A customer's requirements and system specification forms a baseline for estimating the size of a software. At a later stage of the project, a system design document can provide additional details for estimating the overall size of software.

- The ways to estimate project size can be through past data from an earlier developed system. This is called estimation by analogy.

- The other way of estimation is through product feature/functionality. The system is divided into several subsystems depending on functionality, and the size of each subsystem is calculated.

Responsible Persons: *Software manager, cognizant engineers.*

Step 4: Estimating the Effort

When we are finished with the size estimation process, the next step is to estimate the effort based on the size. The estimation of effort can be made from the organizational specifics of the software development life cycle. The development of any application software system is more than just coding of the system. Depending on deliverable requirements, the estimation of effort for project will vary. Efforts are estimated in the number of man-months:

- The best way to estimate effort is based on the organization's own historical data of development process. Organizations follow similar development life cycle for developing various applications.

- If the project is of a different nature which requires the organization to adopt a different strategy for development, then different models based on algorithmic approach can be devised to estimate effort.

Responsible persons: *Software manager, cognizant engineers, and software estimators.*

Step 5: Estimating Schedule

After estimating the efforts, estimating the project schedule from the effort estimated is the next step in the estimation process. The schedule for a project will generally depend on human resources involved in a process. Efforts in man-months are translated to calendar months.
Schedule in calendar months = 3.0 * (man-months) 1/3
The parameter 3.0 is variable, used depending on the situation which works best for the organization.

Responsible Persons: *Software manager, cognizant engineers, and software estimators.*

3.5 DFD Diagram

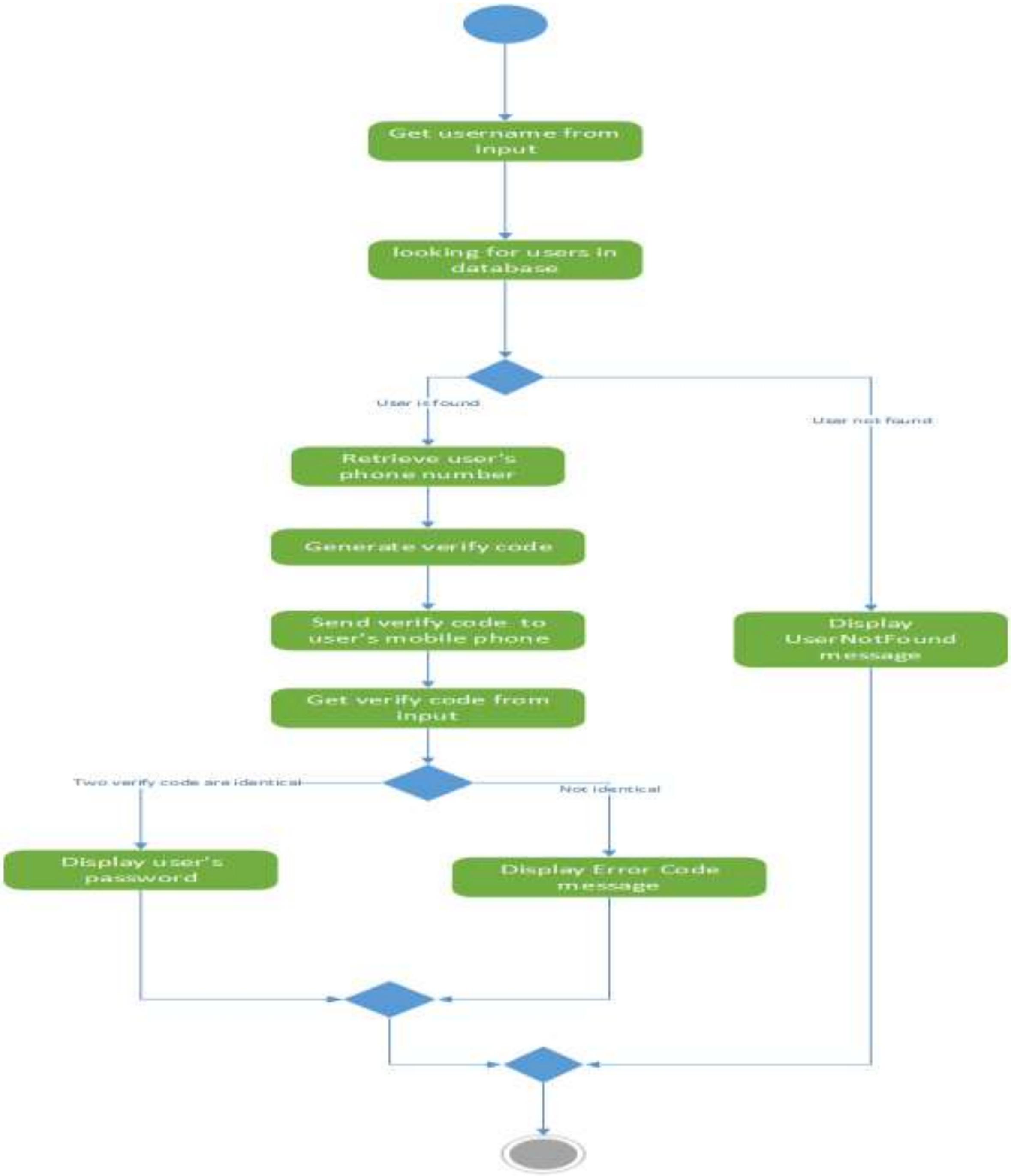
Get username from input
looking for users in database
User is found
User not found
Retrieve user's phone number
Generate verify code
Send verify code to user's mobile phone
Get verify code from input
Display UserNotFound message
Two verify code are identical
Not identical
Display user's password
Display Error Code message

Fig.2:- DFD Diagram

It is also called a Context Diagram. It's a basic overview of the whole system or process being analyzed or modeled. It's designed to be an at-a-glance view, showing the system as a single high-level process, with its relationship to external entities.

Sometimes, it is called as a Context Diagram.

- It visualizes the glance as if you are looking into a system through a helicopter.
- It's a basic overview of the whole system.

- It shows the system as a single high-level process, along with its relationship to the external entities.

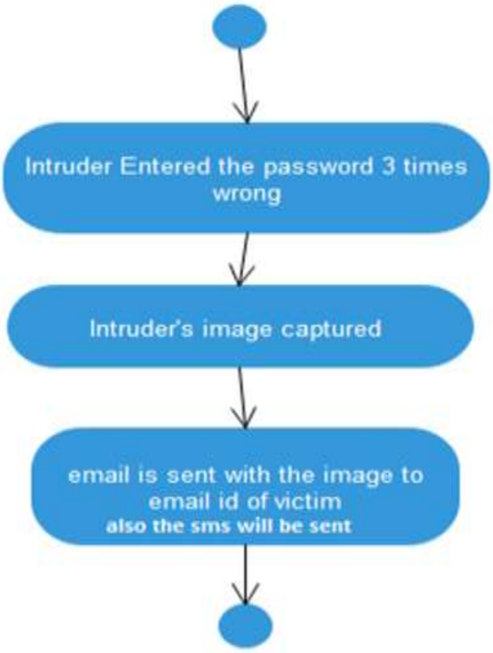
Intruder Entered the password 3 times wrong
Intruder's image captured
email is sent with the image to email id of victim
also the sms will be sent

Fig.3:-State chart Diagram

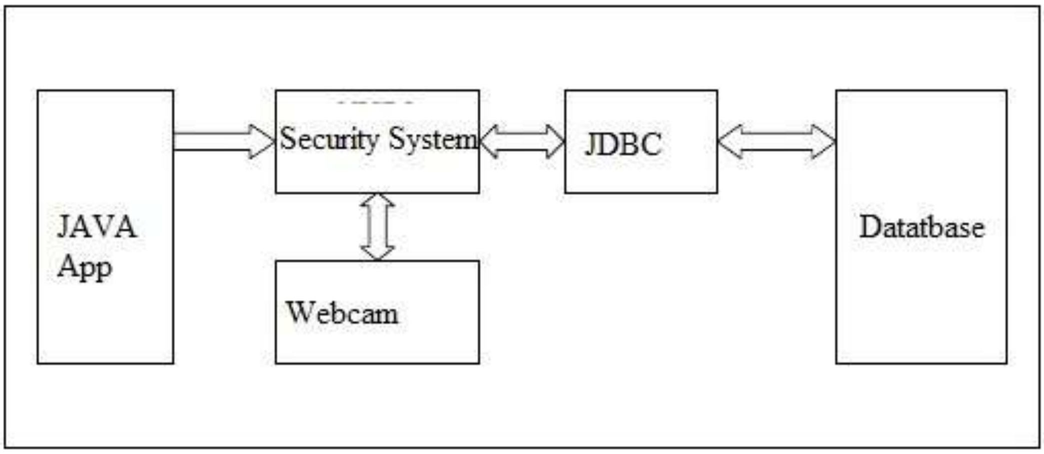

Fig.4:-Functional Block Diagram

3.6 Attacks

This section reviews more carefully various attacks possible against the methods proposed here.

General password guessing

Legacy-UI methods don't affect how users choose passwords, so they have no beneficial effect against adversaries who try common passwords in an online guessing attack. We do favor methods such as those proposed by Schechter et al. requiring users to choose uncommon passwords. Modified-UI methods like take-a-tail also affect the choice of password—

appending a three-digit random tail to a user chosen password effectively reduces the probability of the password by a factor of 1000.

Targeted password guessing

Personal information about a user could help an adversary distinguish the user's password from her honeywords. It is often feasible to deanonymize users, that is, ascertain their real-world identities, based on their social network graphs or just their usernames . Given a user's identity, there are then many ways to find demographic or biographical data about her online—by exploiting information published on social networks, for example. Knowing a user's basic demographic information, specifically his/her gender, age, or nationality, is known to enable slightly more effective cracking of the user's hashed password.

Attacking the HoneyChecker

The adversary may decide to attack the honeychecker or its communications with the computer system. The updates ("Set" commands) sent to the honeychecker need to be authenticated, so that the honeychecker doesn't incorrectly update its database. The requests ("Check" commands) sent to the honeychecker also need to be authenticated, so that the adversary cannot query the honeychecker so as to cause an alarm to be raised. The replies from the honeychecker should be authenticated, so that the computer system doesn't improperly allow the adversary to login.

Likelihood Attack

If the adversary has stolen F and wishes to maximize his chance of picking pi from Wi, he can proceed with a "likelihood attack" as follows. We assume here that we are dealing with an approach based on generating honeywords using a probabilistic model. Let G(x) denote the probability that the honeyword generator generates the honeyword x. Similarly, let U(x) denote the probability that the user picks x to be her password. (This may not be mathematically well-defined; it can be interpreted as a Bayesian prior for the adversary on such probabilities, and may or may not be user-specific).

Denial-of-service

We briefly discuss denial-of-service (DoS) attacks—a potential problem for methods such as chaffing-by-tweaking that generate honeywords by predictably modifying user supplied passwords. (In contrast, chaffing-with-a-password model as well as the hybrid scheme of Section 5.5 offer strong DoS resistance.) The concern is that an adversary who has not compromised the password file F, but who nonetheless knows a user's password—e.g., a malicious user or an adversary mounting phishing attacks—can feasibly submit one of the user's honeywords. For example, with chaffing-by-tweaking-digits, with $t = 2$, such an adversary can guess a valid honeyword with probability $(k - 1)/99$. A false appearance of theft of the password file F results. An overly sensitive system can turn such honeyword hits into a DoS vulnerability. One (drastic) example is a policy that forces a global password reset in response to a single honeyword hit.

Multiple systems

As users commonly employ the same password across different systems, an adversary might seek an advantage in password guessing by attacking two distinct systems, system A and system B—or multiple systems, for that matter. We consider two such forms of attack, an "intersection" attack and a "sweet word-submission" attack. Intersection attack. If a user has the same password but distinct sets of honeywords on systems A and B, then an adversary that compromises the two password files learns the user's password from their intersection. (Of course, without honeywords, an attacker learns the password by compromising either system.) We would aim instead that an intersection attack against systems using honeywords offer an adversary no advantage in identifying the password on either system.

3.7 Risk Management

Risk management is the process of identifying, assessing and controlling threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters. The ISO recommended the following target areas, or principles, should be part of the overall risk management process:

- The process should create value for the organization.
- It should be an integral part of the overall organizational process.
- It should factor into the company's overall decision-making process.

- It must explicitly address any uncertainty.
- It should be systematic and structured.
- It should be based on the best available information.
- It should be tailored to the project.
- It must take into account human factors, including potential errors.
- It should be transparent and all-inclusive.
- It should be adaptable to change.
- It should be continuously monitored and improved upon.

Risk Management Strategies and Process:

All risk management plans follow the same steps that combine to make up the overall risk management process:

Risk identification

The company identifies and defines potential risks that may negatively influence a specific company process or project.

Risk analysis

Once specific types of risk are identified, the company then determines the odds of it occurring, as well as its consequences. The goal of the analysis is to further understand each specific instance of risk, and how it could influence the company's projects and objectives.

3.8 Future Scope & Conclusion

Future Scope

- As the use of Internet is raising day by day the cyber-crime is also increasing simultaneously.
- This software will help us to secure our personal and important data from spams.

Conclusion

- Online password guessing attacks are common against web applications.
- The brute force and dictionary attacks are commonly observed attacks in web applications.
- In these kinds of attack, attackers run automated password guessing programs.
- For web login servers an attacker generally does not have an offline attack on a particular account.
- For all the attach of password this system is effective and it will also know that who is trying to crack the system and access the accounts.

4. References

4.1 References

1) ManishaJagannathBhole, “Honeywords: A New Approach For Enhancing Security,” International Research Journal of Engineering and Technology (IRJET) , Volume: 02 Issue: 08 | Nov-2015.
2) Venkadesh .S, K.Palanivel, “A Survey on Password Stealing Attacks and Its Protecting Mechanism”, International Journal of Engineering Trends and Technology (IJETT) – Volume 19 Number 4 ,Jan 2015.
3) Ari Juels,Ronald L. Rivest “Honeywords:Making Password-Cracking Detectable”; International Conference on Science and Technology 2015, RMUTT, ACM SIGSAC Conf. Comput.Commun. Security, 2013.

4) Arya Kumar et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 2(Version 1), February 2014, pp.656-660
5) Arya Kumar, Prof. A.K.Gupta, "Password Guessing Resistant Protocol for Securing System from Bots and Illegal Access", January 2016 | IJIRT | Volume 2 Issue 8 | ISSN: 2349-6002
6) Ari Juels, Thomas Ristenpart, "Honey Encryption :Security Beyond Brute Force Bound", January 29, 2014,Version 1.1
7) Juels, A.; Ristenpart, T., "Honey Encryption: Encryption beyond the Brute-Force Barrier," Security Privacy, IEEE , vol.12, no.4, pp.59,62, July-Aug.2014
8) PrashantDhas, Ismail Mohammed " Efficient Approach for High Level Security Using Honeywords," IJARCSSE ,Volume 5, Issue 11, 2015
9) NirvanTyagi,Jessica Wang ,Kevin Wen ,Daniel Zuo "Honey Encryption Applications," 6.857 Computer &Network Security, Massachusetts Institute of Technology, Spring 2015.
10) A. Vance, "If Your Password is 123456, Just Make It Hackme," The New York Times,vol. 20, 2010.