Cipphering Transactions Using Cryptocurrency

C. Balamurugan¹, S. Manoharan², K. Manoj Kumar³, Mansoor Habib⁴
¹Associate Professor, Dept. of Computer Science & Engineering, Adhiyamaan College of Engg., Hosur, India
²,³,⁴Student, Dept. of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India

Abstract: In today’s world, banking plays an indispensable role among all people. If the banking is user friendly, then it would benefit all users. So this situation has forced us to move towards mobile banking system. Emerging technologies have supported people with mobile devices and data connections. Mobile banking applications provide an easy door-step solution for customers. In the current trend of digital and cashless economy, mobile based app solutions are comprehensible and omnipresent, expediting a wide range of banking financial services and non-financial services. UPI is one of the mobile based applications which facilitate online transaction. It is simple and reliable application. Besides positives, there are also some hidden security issues to be resolved. UPI uses PIN to complete the transaction. The PIN entry can be noticed by nearby adversaries. Hence, a direct observation attack based on shoulder surfing becomes a great concern. To cope up with this issue, we come up with the solution of providing high level security after acknowledging that there was a pitfall with the assumption of the previous methods. In our proposed method, we strongly focus on security by proposing a novel approach called Covert Attentional Shoulder Surfing(CASS). In our proposal, we also implement the RNN Classifiers to analyze the behaviour characteristics of the user to detect or to resist access by unauthorized people. Our solution or model is also supported by all platforms. It is designed to be used in all platforms (platform Independent) like Android, iOS and other mobile platforms.

Keywords: Cipphering, Cryptocurrency.

1. Introduction

The system suggests that a method i.e. two cryptosystem methodology data security protection mechanism with factor revocability for server storage system.

System allows a sender to send an encrypted message to a receiver through a data storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the cipher text. The first thing is secret key stored in the computer. The cloud server which will immediately execute some algorithms to change the existing cipher text to be undercryptable by this device. This process is completely transparent to the sender. The security and efficiency analysis show that our system is not only secure but also practical. The technologies and methodologies used in the system are discussed below:

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

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

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

Cloud computing has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability.

Digital Signature: For every transaction, the account number, the account number of the person we are sending to and the amount of cryptocurrency exchanged is announced. But, this information about the account numbers will not be disclosed because of cryptographic keys. The private key is used to digitally sign the data and using the public key which is available to all in the network can verify the signature but cannot decrypt the data content hence making it secretive.

SHA1: It is a cryptographic hash function which takes input and produces a 160-bit hash value called message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long.

Example:
Input: hello world
Output: 2aae6c35e94cfb415d6be95f408b9ce91ee846ed

A. Blowfish algorithm

In BLOWFISH, the plain text which comes as input is 64 bits. The plaintext is divided into two halves L and R which enters a loop which is repeated 16 times. L is XORed with
current value of P-box say Pi(16-bits). We then take R which is XORed with function of L (here, F).

Function: L1, L2, L3 are S Box entries and can have 256 entries of 32-bit. Lastly we swap L & R and we repeat the loop all over again for 16 times. After completion of all the loops we swap L&R once more. P box has 18 entries so the two entries which are left are XORed with L&R individually which is combined to get Cipher Text

2. Literature review

Rajani Sharma and Rajender Kumar Trivedi. Literature review: Cloud computing–security issues, solution and technologies.

Cloud computing has grabbed the spotlight in the year 2013 at a conference in San Francisco, with vendors providing plenty of products and services that equip IT with controls to bring order to cloud chaos. Cloud computing trend is increasing rapidly so to make cloud computing more popular the very first step for the organization is to identify exact area where the cloud related threats lie. At an unusual pace, cloud computing has transformed business and government. And this created new security challenges. The development of the cloud service model provide business – supporting technology in a more efficient way than ever before. The shift from server to service based technology brought a drastic change in computing technology. However, these developments have created new security vulnerabilities, including security issues whose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and security solutions.

Techniques used:

A Markov chain is "a stochastic model describing a sequence of possible events in which the probability of each event depends only on the state attained in the previous event."

In probability theory and related fields, a Markov process, named after the Russian mathematician Andrey Markov, is a stochastic process that satisfies the Markov property (sometimes characterized as "memorylessness"). Roughly speaking, a process satisfies the Markov property if one can make predictions for the future of the process based solely on its present state just as well as one could knowing the process's full history, hence independently from such history; i.e., conditional on the present state of the system, its future and past states are independent.

A Markov chain is a type of Markov process that has either discrete state space or discrete index set (often representing time), but the precise definition of a Markov chain varies. For example, it is common to define a Markov chain as a Markov process in either discrete or continuous time with a countable state space (thus regardless of the nature of time) but it is also common to define a Markov chain as having discrete time in either countable or continuous state space (thus regardless of the state space).

Random walks on integers and the gambler's ruin problem are examples of Markov processes. Some variations of these processes were studied hundreds of years earlier in the context of independent variables. Two important examples of Markov processes are the Wiener process, also known as the Brownian motion process, and the Poisson process, which are considered the most important and central stochastic processes in the theory of stochastic processes and were discovered repeatedly and independently, both before and after 1906, in various settings. These two processes are Markov processes in continuous time, while random walks on the integers and the gambler's ruin problem are examples of Markov processes in discrete time Markov chains have many applications as statistical models of real-world processes, such as studying cruise control systems in motor vehicles, queues or lines of customers arriving at an airport, exchange rates of currencies, storage systems such as dams, and population growths of certain animal species. The algorithm known as Page Rank, which was originally proposed for the internet search engine Google, is based on a Markov process. Furthermore, Markov processes are the basis for general stochastic simulation methods known as Gibbs sampling and Markov Chain Monte Carlo, are used for simulating random objects with specific probability distributions, and have found extensive application in Bayesian statistics.

Li and J. Du. Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing.

In cloud computing, trust management is more important than ever before in the use of information and communication technologies. Owing to the dynamic nature of the cloud, continuous monitoring on trust attributes is necessary to enforce service-level agreements. This study presents Cloud-Trust, an adaptive trust management model for efficiently evaluating the competence of a cloud service based on its multiple trust attributes. In Cloud-Trust, two kinds of adaptive modelling tools (rough set and induced ordered weighted averaging (IOWA) operator) are organically integrated and successfully applied to trust data mining and knowledge discovery. Using rough set to discover knowledge from trust attributes makes the model surpass the limitations of traditional models, in which weights are assigned subjectively. Moreover, Cloud-Trust uses the IOWA operator to aggregate the global trust degree based on time series, thereby enabling better real-time performance. Experimental results show that Cloud-Trust converges more rapidly and accurately than do existing approaches, thereby verifying that it can effectively take on trust measurement tasks in cloud computing.

Techniques:

PSO: Particle Swarm Optimization

Particle swarm optimization (PSO) is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. It solves a problem by having a population of candidate solutions, here dubbed particles, and moving these particles around in the search-space according to simple mathematical
formulæ over the particle’s position and velocity. Each particle's movement is influenced by its local best known position, but is also guided toward the best known positions in the search-space, which are updated as better positions are found by other particles. This is expected to move the swarm toward the best solutions. PSO is a metaheuristic as it makes few or no assumptions about the problem being optimized and can search very large spaces of candidate solutions. However, metaheuristics such as PSO do not guarantee an optimal solution is ever found. Also, PSO does not use the gradient of the problem being optimized, which means PSO does not require that the optimization problem be differentiable as is required by classic optimization methods such as gradient descent and quasi-newton methods.

3. Existing system

Nowadays, security password is the most well-known way to verify a customer to sign in to Computer Systems. However, we all know that conventional text-based security password techniques are susceptible to the shoulder-surfing strike. Through this document we use the phrase “shoulder-surfing” in the following sense: A shoulder-surfing strike includes a customer being shot during his/her sign in.

4. Proposed system

This product can be used by all the users who are provided with the bank account. In this solution, we have provided various features for the UPI users so as to benefit them with the seamless transaction. So to, in the proposed system, the product can be used in commercial transaction such as an interaction between two or more parties in which goods, services or something of value is exchanged for some type of remuneration and personal transactions (Person-to-person payments (P2P) is an online technology that allows customers to transfer funds from their bank account or credit card to another individual’s account via the Internet or a mobile phone). Since our solution supports platform independency, it would really benefit a large number of users and we provide with the following features,

Behaviour Analyses using RNN classifiers:

The gesture data capturing information reflects the way users interact with their mobile devices. This data is stored and analyzed and if any mismatch is found with the behavioral characteristics, fraudulency is detected and alert message is automatically sent.

Covert Attentional Shoulder Surfing (CASS):

When a user enters a PIN, there is a chance of direct observation attack by the intruder. So this becomes a great concern and CASS plays a vital role in preventing the shoulder surfing attack.

Platform Independent:

When a product is supported by all the mobile platforms, then it would facilitate most of the users to easily connect with the mobile transaction applications from any platform.

5. Modules description

- Registration Phase
- Login
- PIN Entry
- View Account Summary
- View Transaction Details

A. Registration phase

The users can register into the system through this phase.

B. Login

After registering the users sign in to the system

C. PIN Entry

The improved method runs as follows: The system displays a set of ten digits, $A = \{0, \cdots , 9\}$, on the regular numeric keypad with two split colors, chosen from $P$, in each numeric key; and the four colour keys below.

A colour is chosen at random from $P$ and fills five random splits of distinct keys; each split could be either upper or lower one.

The remaining colours fill five splits, respectively, in the same way. The user attends to the PIN digit and enters either of its colour through the colourkey. The user and the system repeat this procedure for 2 rounds that the PIN digit is identified by intersection, and until all the PIN digits are identified.

The required number of rounds is obviously $2 \times 4$. If the selected colour is corrected with the first digit number in second round, then enter into the next round. Else it moves to login page. Those above rounds are repeated until enter all the pin digit. After that Pin digit is correct then enter into the banking main page.

D. View Account Summary

In this phase user can view the current account details.
E. View Transaction Details

In this phase user can view the all money transaction details. And also the user can view the particular date or month report.

F. Unusual payment

When there is a large amount to be transacted, it is important to ensure the authorization. So, to confirm whether this huge transaction is performed by an authorized user, RNN classifiers has been implemented. This analyses the previous transaction history of the user and calculates the mean and mode and finally it sets the range of the amount to be transacted. If the amount to be transacted exceeds the range, then to verify the exact authorization, an OTP is sent to the user’s mobile number. Entering a wrong OTP will identify unusual transaction and the process will be terminated. Hence through this Unusual Transactions can be prevented.

![Flow Diagram](image)

**Fig. 2. Flow Diagram, platform independent**

6. Conclusion

The security password techniques are susceptible to neck browsing; many neck browsing proof color palette authentication password techniques have been suggested. However, as most users are more familiar with textual security passwords than pure visual security passwords, text-based visual security password techniques have been suggested. Unfortunately, none of existing text-based neck browsing proof visual security password techniques is both secure and efficient enough. In this paper, we propose an improved text-based neck browsing proof visual security password plan by using colors. In the suggested plan, the user can easily and efficiently sign in to neck browsing and random sign in.

References