International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Providing Security Enhancement for Password : A Quantitative Empirical Analysis

Singampalli Sankeerthi*[1], Mallampati Vasavi Kanyaka Parameswari[2]
*[1]Assistent Professor, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India
[2]PG Students, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

Cloud computing is a simply known as "the cloud," is the delivery of on-demand computing resources. Everything from the user applications to data centers access the data over the Internet on a pay for use basis. In this project we finding the people who are all having multiple accounts in same site or multiple sites, and the user will give same password for all accounts. Whose accounts could have the same password or even stronger passwords. We name this attack as the shadow attack on passwords. In this paper we produce two types of password encryption methods, in this method we encrypt the password and store to the database as the encrypted format at the same time the encrypted password does not work at the login time the user need to decrypt the same password and match with the login password. Here every time user need to enter the password and need to select the password encryption and decryption method.

Keywords: A Quantitative Empirical Analysis, Cloud, Password

I. INTRODUCTION

Cloud computing is a general term for the delivery of hosted services over the internet. Cloud computing enables companies to consume a compute resource, such as a virtual machine (VMs), storage or an application, as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in house. Cloud computing boasts several attractive benefits for businesses and end users.

Three of the main benefits of cloud computing are: Self-service provisioning: End users can spin up compute resources for almost any type of workload on demand. This eliminates the traditional need for IT administrators to provision and manage compute resources. Elasticity: Companies can scale up as computing needs increase and scale down again as demands decrease. This eliminates the need for massive investments in local infrastructure which may or may not remain active. Pay per use: Compute resources are measured at a granular level, allowing users to pay only for the resources and workloads they use. Based on a service that the cloud is offering, we are speaking of either

- ✓ (Infrastructure-as-a-Service)
- ✓ (Platform-as-a-Service)
- ✓ (Software-as-a-Service)

Basically, programs that are needed to run a certain application are now more popularly located on a remote machine, owned by another company. This is done in order not to lose on the quality performance due to processing power of your own computer, to save money on IT support, and yet remain advantageous on the market. These computers that run the applications, store the data, and use a server system, are basically what we call "the cloud".

Cloud computing has become a popular computing infrastructure for many scientific applications. Recently, we have witnessed many workflows from various scientific and data-intensive applications deployed and hosted on the Infrastructure-as-a-Service (IaaS) clouds such as Amazon EC2 and other cloud providers. In those applications, workflows are submitted and executed in the cloud and each workflow is usually associated with a deadline as performance guarantee. This has formed a new software-as-a-service model for hosting workflows in the cloud, and we refer it as Workflowas-a-Service (WaaS). WaaS providers charge users based on the execution of their workflows and QoS requirements. On the other hand, WaaS providers rent cloud resources from IaaS clouds, which induces the monetary cost. Monetary cost is an important optimization factor for WaaS providers, since it directly affects the profit of WaaS providers. In this paper, we investigate whether and how WaaS providers can reduce the monetary cost of hosting WaaS while offering performance guarantees for individual workflows.

II. EXISTING SYSTEM

In existing system the user does not encrypt and decrypt the password while register and login time, it is un-secure method at the same time the unauthorized peoples will misuse the account in the same web site or Different web site.

Architecture

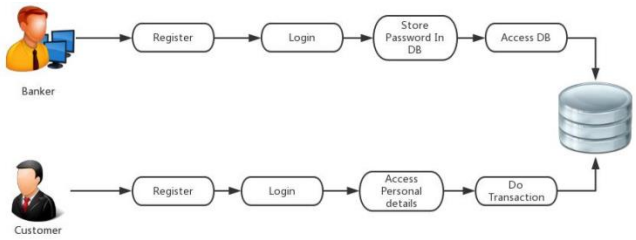

Figure 1

Disadvantages

- Un-secure for user password and information in the data base.
- User providing same password for all there accounts.

Proposed System

In Proposed system the user will encrypt and decrypt the password for there all accounts. In this method we provide encryption and decryption for user passwords. Here every time user needs to enter the password and need to select the password encryption and decryption method.

Advantages

- ✓ Here the user needs to enter plain text password it will encrypt and decrypt the passwords.
- ✓ User transfer the information secure through the login.

Proposed Architecture

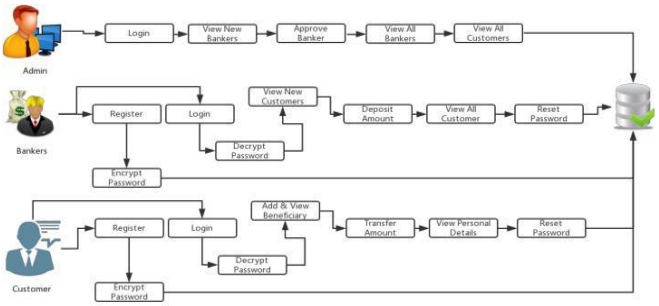

Figure 2

Algorithm

```
def iterative_bsearch(a, value)
  low, hi = get_limits(a)
  while low < hi
    mid = (low + hi) / 2
    if a[mid] == value
      return mid
    elsif a[mid] < value
      low = mid + 1
    else
      hi = mid
    end
  end
  false
end
```

Figure 3

Overall Dataflow Diagram

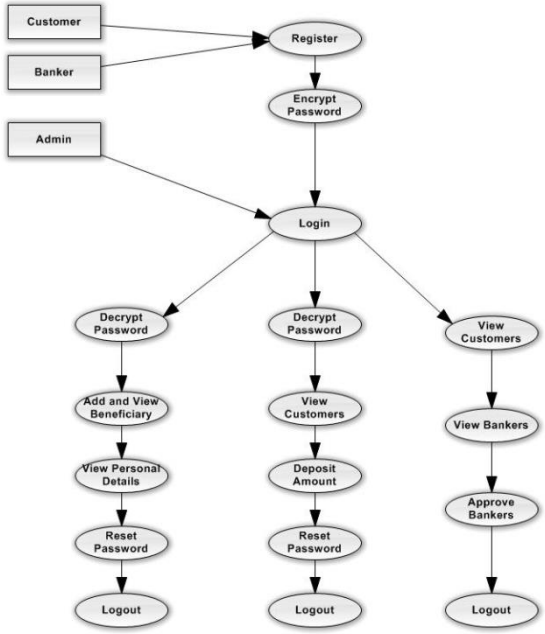

Figure 4

Authentication Module:

In this application they are only two users, One the main site owner Admin and another one is a normal users. For Admin there is registration process because he is the site owner. But, for users there is a registration process, from this they will get a user id and password to get into this application. And Admin also have his particular user id and password to enter this application.

Password Encryption and Decryption:

In this module the user and Banker will encrypt the password with they own way the encrypted password only store in the database, on the retrieve time the encrypted password only decrypted and compare with the original password.

User Management:

In this module the banker and the admin will manage the user details and the user details always monitor and the same time the baker deposit the money to the customers and records always stored in the database.

Add new Bankers and Approve:

In this module the baker will register on the website and get the approve from the admin, after the admin approve the banker details will show to the user, after the user view the banker details the user register or open the account on the bank.

Add Beneficiary:

In this module the banker and the admin will manage the user details and the user details always monitor and the same time the baker deposit the money to the customers and records always stored in the database. In this module the baker will register on the website and get the approve from the admin, after the admin approve the banker details will show to the user, after the user view the banker details the user register or open the account on the bank.

Inter site password:

The security strength of the reused passwords in terms of how easily they can be guessed correctly by an adversary with dictionaries. With the same metrics. We find that the reused passwords across sites are stronger (i.e., harder to guess) against online password guessing attacks than all passwords, while intra-site reused passwords perform similarly to all passwords against online password guessing attacks. When we conducted offline password guessing attacks, all reused passwords perform weaker than all passwords.

Cross site password:

In this module Even though some users use different passwords for their accounts across different websites, their passwords are sometimes created using the same building blocks. For example, among the users who use different passwords on the four websites add prefix to create passwords add suffix. The definitions of prefix and suffix patterns are described.

III. CONCLUSION

This is the Project empirical study on web password reuses by analyzing a large number of sample data.

Although the web password reuses are known to researchers and Internet users, it is yet to perform a large-scale empirical study. We obtained distinct users each of whom has at least two accounts from the same site distinct users each of whom had at least two accounts from different websites.

IV. REFERENCES

[1]. JoseLuisGarcia-Dorado "Cost-aware Multi Data-Center Bulk Transfers in the Cloud From a Customer-Side Perspective".

[2]. ShankaranarayananPN, AshiwanSivakumar, Sanjay Rao, MohitTawarmalani "Performance sensitive replication in geo-distributed cloud datastores".

[3]. XingliangYuan,HuayiDuan , and Cong Wang "Bringing Execution Assurances of Pattern Matching in Outsourced Middleboxes"

[4]. Karthik.S,Muruganandam .A "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System"

[5]. Jun Du, Chunxiao Jiang, ,YiQian,,ZhuHanandYongRen "Resource Allocation with Video Traffic Prediction in Cloud-based Space Systems".

[6]. M. Hovestadt, O. Kao, A. Kliem, and D. Warneke, "Evaluating adaptive compression to mitigate the effects of shared I/O in clouds".