isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 2 ,Apr,2023 ,ISSN_NO: 2321-3337

Analysis Of User Behaviour Tracking, Detection and Elimination Of Thief

Auvula Mohan[1] , C. Lokasai Reddy[2] , Ravella Narasimha Rao[3], Cirivella Siva Sai[4] , Aarthi.V[5]

UG Scholar[1 2 3 4]-Department of CSE, GRT Institute of Engineering and Technology, Tiruttani.

Aarthi.V[5.] Asst. Professor -Department of CSE, GRT Institute of Engineering and Technology, Tiruttani.

mohanyadav30175@gmail.com, lokasair@gmail.com, narasimhachowdary122@gmail.com, cirivellasivasai@gmail.com, Aarthi.v@grt.edu.in.

ABSTRACT— *Social networks Accounts are tracked & detected. If hacker attacks the Genuine user then our allows the attacker to proceed further until our system captures all the important information about the attacker. We generate Honeywords based on the user info provided and the original password is converted into another format and stored along with the Honeywords. We deploy Intermediate server, Shopping server for purchase and Cloud server for maintaining user account details. Attacker who knows the E mail account of original user can easily reset the password of the cloud server. Attacker is invited to do attack in this Project, so as to find him out very easily. Now attacker logins into the purchase portal, where he is been tracked unknowingly & he is allowed to do purchase. Server identifies the attacker and sends the info to the Original owner and also it blocks the attacker even doing transaction from his original account.*

Keywords – Honeywords, Cloud Server

1. INTRODUCTION

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed, including. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. Password Segmentation Algorithm can be used to segment password and user attributes, and later the correlation between a segmented password and user attributes is achieved [1]. Cloud Data can be split into multiple blocks. TPA will verify the data integrity and on the overlay Block chain technology which is used for secured data storage in the cloud server [2]. Various different algorithms can be used to identify the load for every Virtual Machine like Bayesian Stackelberg game and Risk assessment framework is used to identify the Attacks [3]. We need to deploy multi user data access with highly secured multi encryption and decryption Policies for secured data access [10]. We use label and pseudorandom function to encrypt message, which significantly reduce the computations on the servers and enable us to use homomorphic MACs technology to realize verifiable computations naturally [11]. We need to focus on a mobile cloud scenario where data is stored within a geographically-limited area A by a community of mobile devices, For ease of illustration, we consider a single file. A user within A can download F from the mobile devices via direct communication links without accessing the network infrastructure [12]. The concept which is proposed to deal with secured data storing and sharing in multiple cloud providers. Big data based geo dispersed data storage services. Secured data storing using encryption Techniques [13]. To ensure the integrity of the data stored in the cloud, many data integrity auditing schemes can be used. Biometric data can be used (e.g. iris scan, fingerprint) as the user’s fuzzy private key to avoid using the hardware token. Meanwhile, the scheme can still effectively complete the data integrity auditing [14]. Encrypted keyword using block chain can be integrated for the Data security in this Project [15].

1. BACKGROUND

1.1 ARCHITECTURE DIAGRAM

The overall architecture represents the working procedure of the entire system. User will register their details on the portal with two email ids like primary and secondary account. while user login with correct user id password they can purchase the product with normal portal or else if any one try to login user id with fake password by trying more than three system will automatically divert them into fake portal and fetch the fake user's delivery address and IP of the system.

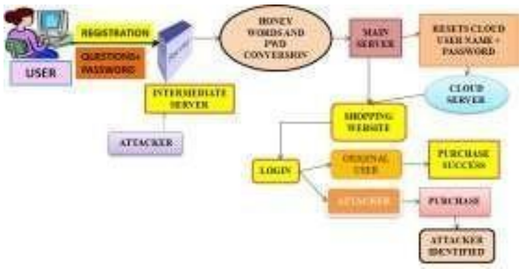


Fig 2.1 Architecture Diagram

1.2 Modules

A modular design reduces complexity, facilities change (a critical aspect of software maintainability), and results in easier implementation by encouraging parallel development of different part of system. Software with effective modularity is easier to develop because function may be compartmentalized and interfaces are simplified. Software architecture embodies modularity that is software is divided into separately named and addressable components called modules that are integrated to satisfy problem requirements.Modularity is the single attribute of software that allows a program to be intellectually manageable. The five important criteria that enable us to evaluate a design method with respect to its ability to define an effective modular design are: Modular decomposability, Modular Comps ability, Modular Understandability, Modular continuity, Modular Protection.

1.2.1 USER REGISTRATION

In this module we are going to create a User application by which the User is allowed to access the data from the Server. Here first the User wants to create an account and then only they are allowed to access the Network. Once the User creates an account, they are allowed to login into their account to access the application. Based on the User's request, the Server will respond to the User. All the User details will be stored in the Database of the Server. In this module bank user details are registered with the fields like username, password, and personal details with some set of questions and answers. These details are saved into the server. After proper registration only the user cal allowed to login into the server.

2.2.2 SERVER

In this Server module server will deployed to access the database and web based application. Server will verify the users and generates honey word for save the users password. In case illegal actions happened means server will generates alert and intimate it to user. The Server will monitor the entire User's information in their database and verify them if required. Also the Server will store the entire User's information in their database. Also the Server has to establish the connection to communicate with the Users. The Server will update the each User's activities in its database. The Server will authenticate each user before they access the Application. So that the Server will prevent the Unauthorized User from accessing the Application.

2.2.3 HONEY WORDS GENERATION

Password files have got a lot of security problem that has affected millions of users as well as many companies. Password file is generally stored in encrypted format, if a password file is stolen or theft by using the password cracking techniques and decryption technique it is easy to capture most of the plaintext and encrypt passwords. So In this module we deployed honey word creations. That is the user's password and registered questions are combined and then it will generate a key as unknown Name.

2.2.4 INTERMEDIATE SERVER & SHOPPING SERVER DEPLOYMENT

An intermediate server is a program that handles communications requests to a resource manager program on behalf of a user program. The user program can be referred to as a client of the intermediate server.Here we will generate the Intermediate server to make communication between user and Server. All requests comes from the users are first sent to the intermediate server to verifies the password and user details. Shopping server is to collect the details from customer and sent to the details to the intermediate server for verification.

2.2.5 PASSWORD HACKING PROCESS

Hacking is the process of recovering pass words from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. Another common approach is to say that you have "forgotten" the password and then change it. Password Hacking is blocked in this Module. Because we modifies the users original passwords into unknown Name and saved into server.

2.2.6 IDENTIFICATION OF ATTACKERS & REMOVE DDOS ATTACKS

A distributed denial of service (DDos) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites and present a major challenge to making sure people can publish and access important information. If there is anybody trying with wrong password or any illegal action means server will block that action and intimate to the Specified Users. If the same request comes from same user or from different user's means server will blocks that actions also. This is done in DDOS attack.

2. PROPOSED SYSTEM

We include two processes. As per the Paper Compromised Social networks Accounts are tracked & detected.If hacker attacks the Genuine user then our allows the attacker to proceed further until our system captures all the important information about the attacker. We generate Honeywords based on the user info provided and the original password is converted into another format and stored along with the Honeywords. We deploy Intermediate server, Shopping server for purchase and Cloud server for maintaining user account details. Attacker who knows the

E mail account of original user can easily reset the password of the cloud server. Attacker is invited to do attack in this Project, so as to find him out very easily. Now attacker logins into the purchase portal, where he is been tracked unknowingly & he is allowed to do purchase. Server identifies the attacker and sends the info to the Original owner and also it blocks the attacker even doing transaction from his original account.

4. EXISTING SYSTEM

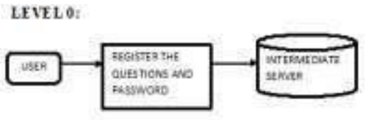
Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes has not much of security to store the data safely.

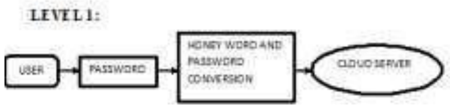
4.1 Disadvantages of Existing System

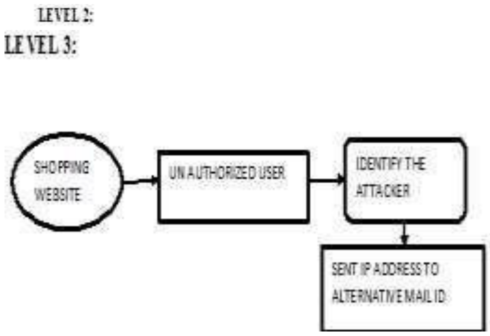
Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes has not much of security to store the data safely.

5. DATA FLOW DIAGRAM

DFD graphically representing the functions, or processes, which capture, manipulate, store, and distribute data between a system and its environment and between components of a system. The visual representation makes it a good communication tool between User and System designer. A process receives input data and produces output with a different content or form. Processes can be as simple as collecting input data and saving in the database. A data store or data repository is used in a data-flow diagram to represent a situation when the system must retain data because one or more processes need to use the stored data in a later time.







6. RESULT ANALYSIS

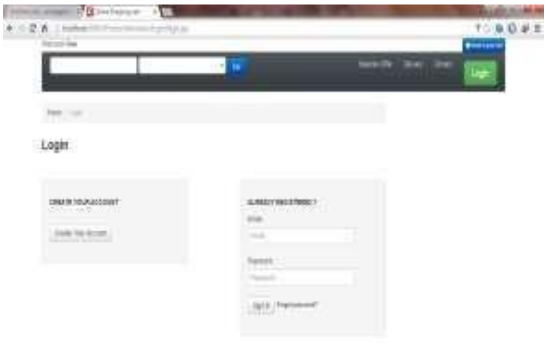


Fig 6.1 Login Page

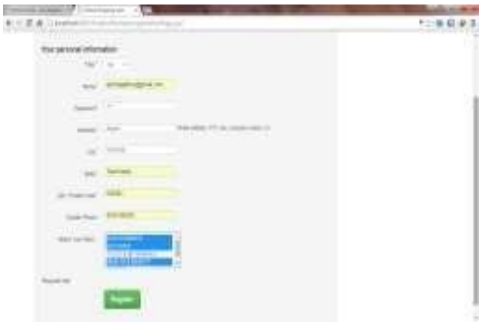


Fig 6.2 Register Page

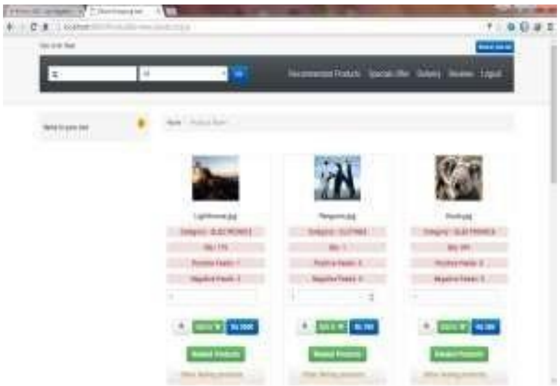
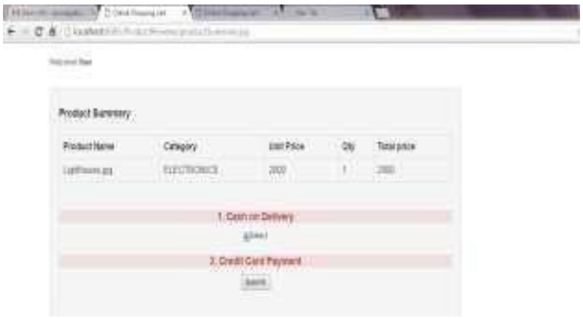


Fig 6.3 User Dashboard



Product Summary

Product Name	Category	Unit Price	Qty	Total price
LightHouse.jpg	ELECTRONICS	2000	1	2000

1. Cash on Delivery

2. Credit Card Payment

Submit

Fig 6.4 Payment Gateway

7. CONCULSION

In this project, we have to implement secured purchasing system in online. Honey words are generated based on the user info provided and the original password is converted into another format and stored along with the Honey words. If identify the hacker means ,Hacker's IP Address, E mail ID, Phone number and postal Address are tracked and stored. Finally these details are sent to original user alternative mail id.

REFERENCES

[1] D. Mirante and C. Justin, "Understanding password database compromises,"Dept. of Comput. Sci. Eng. Polytechnic Inst. of NYU, NewYork, NY, USA: Tech. Rep. TR-CSE-2013-02, 2013.

[2] A. Vance, "If your password is 123456, just make it hackme," NewYork Times, Jan. 2010.

[3] K. Brown, "The dangers of weak hashes," SANS InstituteInfoSec Reading Room, Maryland US, pp. 1–22, Nov. 2013,[Online].Available: http://www.sans.org/reading-room/whitepapers/authentication/dangers-weak-hashes-34412.

[4] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Passwordcracking using probabilistic context-free grammars," in

Proc. 30thIEEE Symp. Security Privacy, 2009, pp. 391–405.

[5] F. Cohen, “The use of deception techniques: Honeypots anddecoys,” Handbook Inform. Security, vol. 3, pp. 646–655, 2006.

[6] M. H. Almeshekah, E. H. Spafford, and M. J. Atallah, “Improvingsecurity using deception,” Center for Education and ResearchInformation Assurance and Security, Purdue Univ., WestLafayette, IN, USA: Tech. Rep. CERIAS Tech. Rep. 2013-13, 2013.

[7] C. Herley and D. Florencio, “Protecting financial institutions frombrute-force attacks,” in Proc. 23rd Int. Inform. Security Conf., 2008,pp. 681–685.

[8] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, “Kamouflage:Loss-resistant password management,” in Proc. 15th Eur. Conf.Res. Comput. Security, 2010, pp. 286–302