IDENTIFICATION OF HACKER BY TRAPPING MECHANISM IN SOCIAL MEDIA AND SHOPPING PORTALS

[1]C Ramprasath, [2] C Raghavendra, [3] J Varun, [4] M Vishal Vishnu/ [5] S Sri Heera
[1]UG Student, [2] UG Student, [3] UG Student, UG Student, Assistant Professor
[1]Computer Science and Engineering,
[1]Easwari Engineering College, Chennai, India

Abstract: To steal information rather than to cause vulnerability to the network or organization, hackers use Advanced persistence threat (APT) attack. Here, user's behavior is analyzed based on preceding behavior such as posted data, content type, time, IP address and location of the electronic device. Basically, it includes two processes. [1] The Social network accounts are analyzed, stored in the database. If the hacker attacks the social website account, he/she is tracked and then detected. [2] Meanwhile if the hacker attacks the original user's shopping portal account, then the system allows the attacker to proceed further until the system captures all the important information about the attacker by directing the hacker to the fake website. The system generates Honeywords based on the user information provided and the original password is converted into a different format using Name generation algorithm and stored along with the honeywords in the cloud. An attacker who knows the E-mail account of the original user can easily reset the password of the cloud server. When the attacker tries to log in to the purchase portal, he/she is tracked and allowed to do purchase. The server identifies the attacker and sends an alert message to the owner and blocks the attacker from doing the transaction from his original account.

Index Terms **- Cloud security; Hacker; Honeywords; Sentimental Analysis**

I. INTRODUCTION

The sentimental analysis is the process mainly used to predict the emotions based on the content of the text, which may be positive, negative or neutral**. It is also known as data mining, deriving the view or attitude of a speaker. The sentimental analysis is mainly based on machine learning where the system classifies the emotions and opinions of the humans based on the content, which may be a text or voice**. The sentimental analysis predicts the emotions based on the understanding of the opinions and content of the social data given by the user. The sentimental analysis is immensely used because it gives an abstracted view of the public opinions about certain topics or emotions. Social media monitoring tools make that process faster and easier than ever before. Today's algorithm-based sentiment analysis tools can handle huge volumes of customer feedback consistently and accurately. Paired with text analytics, sentiment analysis reveals the customer's opinion about topics ranging from your products and services to your location, your advertisements, or even your competitors.

HONEYWORD

Honeywords are a sequence of characters that are generated by humans that look like a password. Honeywords are proposed as part of a honeypot, so that any intruder attempting to log in with the password may be assumed to be an attacker. Some hackers perform a weighted random walk against a PCFG grammar that was trained on real human generated passwords. In this approach, first, a

probabilistic context-free grammar, (PCFG), is trained on a set of passwords that you want the honeywords to resemble. The (P) in PCFG stands for "probability". This means for each transform in the PCFG a random number is generated, and a transform is chosen based on that random number and the weighted probability of a transform. For example, if the grammar contains the transform S-> 'word' + '132' and that transform has a probability of 90%, then on average around 90% of the generated honeywords will end with '132'.

CLOUD SECURITY

Cloud computing security is a service that includes protecting critical information from theft, data leakage, and deletion. One of the benefits of cloud services is that it can be operated at scale and remain secure. It proposes how to manage security and different ways of delivering security solutions that address new areas of concern. Client requests from the service provider server occurrence and enters most settings and choose the operating system. Then clients determine the size and other settings needed that allows them accessing the cloud and using the applications they requested. Cloud storage services such as Dropbox, Google Drive, and SugarSync are convenient, efficient and notoriously insecure. The data is not encrypted, and transfer of data is not secure so private data of the organizations are highly enlightened to vulnerabilities.

LITERATURE SURVEY

[1] The paper proposes a mechanism called Advanced Persistent threats[APT] along with Socialbots. The main objective is to gain knowledge about the deployment process, creation, and management of the social honeypots, as well as their efficiency and security enhancements.

[2] It uses OpenStack in Cloud handling. OpenStack consists of a set of open-source projects which provide a variety of services for an IaaS model. Its five main projects deliver basic functionalities that are required for a cloud infrastructure and mainly produce secured enhancements in cloud

[3] The paper applies COMPA to two datasets from popular social networks, Facebook and Twitter, and show that the system would have been able to detect compromised accounts. It also shows that COMPA would have been able to detect four high profile negotiations that affected popular Twitter accounts.

[4] It focuses on four factors related to user authentication: authentication by something the user knows (e.g., password), authentication by something user has (e.g., physical token), authentication by something the user is (e.g., biometric authentication) and authentication by someone user knows.

[5] This system speaks about the security intensity of the user passwords. It uses techniques like Chaffing-by-tweaking, Chaffing with “toughnuts”, Chaffing-with-a-password-model for the analysis of the obtained passwords. Also, the security mechanisms like Denial of service attack, brute force attack.

ISSUES IN THE EXISTING SYSTEM

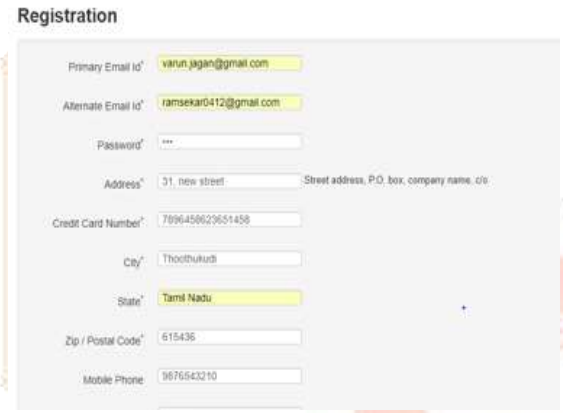
When it comes to identification of hacker, the current system blocks the attacker at the gateway of the module rather permitting. It creates complications in recognizing the attacker evidence like IP address, location and time of access. To sort out these issues, the current system is proposed where the hacker can enter the fake website and perform their actions.

PROPOSED SYSTEM

In the social networking sites, sentimental analysis of the user is performed and the details like username and passwords are stored in the database. Later if the attacker tries to post anonymous content in the user's account, the hacker is tracked, and the IP address, time and location are identified. In shopping portals, the honeywords are generated based on the security questions and stored in the cloud. The hacker can enter the password three times. Post three tries, it redirects to a fake website and the fake transaction is made. During the transaction, the delivery address of the hacker is emailed with a notification message to the original user. Four modules namely Profile manager, Authenticity check, Trap the hacker and Behavior analysis are used.

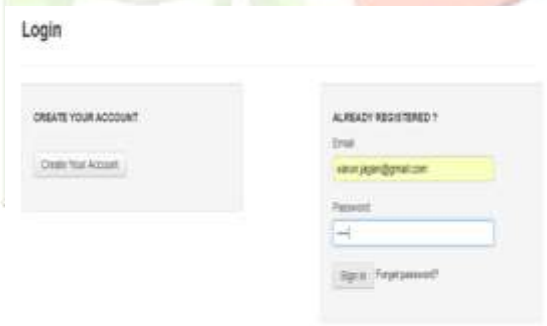
PROFILE MANAGER

In the profile manager, the user can create a new account by giving the required information to the system. Followed by that, comes a unique email and password. The user uses these credentials to login to the shopping portal. Through the add item page, the products are uploaded for shopping in the portal.



AUTHENTICITY CHECK

The second module authenticity check, the user is directed to the appropriate page based on the contents provided by them. If the entered details are true, it directs to the original website. If the entered credentials are found to be inappropriate(honeywords) it is directed to the fake website.



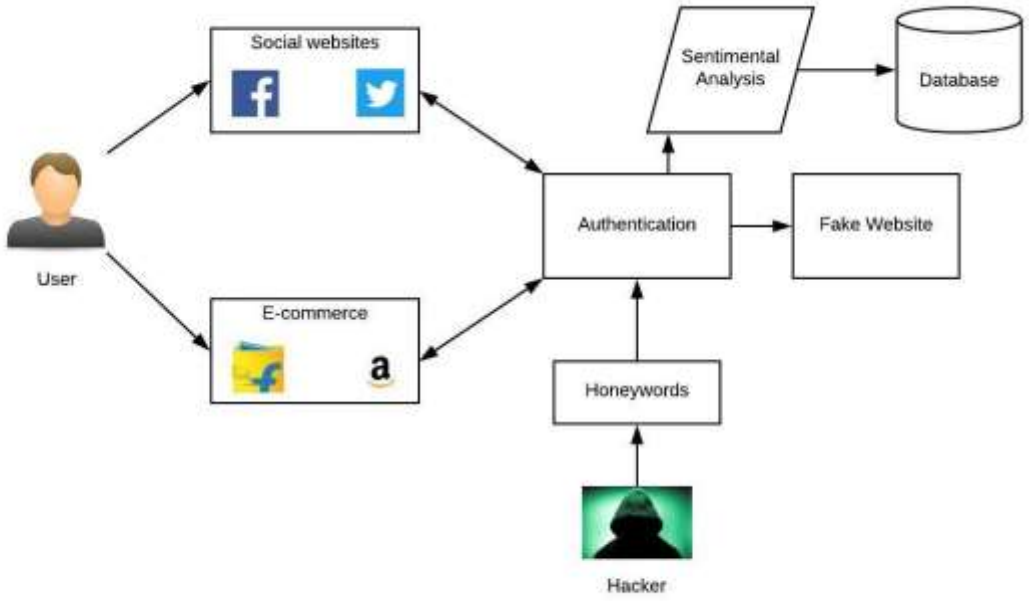
TRAP THE HACKER

In the third module called as Trap the Hacker, the details of the hacker are sent to the owner with a notification saying that the account was hacked. Before this, the system confirms the honesty of the user to narrow down to a decision to decide him/her as an owner.

BEHAVIOUR ANALYSIS

In this module, an analysis report is made based on the content posted and the regular accessing time of the user. This analysis report is used to deny the attacker who tries to post any unrelated content anonymously in the user's account.

SYSTEM ARCHITECTURE



CONCLUSION AND FUTURE ENHANCEMENTS

Though 100% data security is difficult to achieve, there are ways to save data and this system mainly conceptualizes the field of security. It restricts the eccentricity of the data loss and mainly plays a vital role in securing online fraud. In the field of online social media, when it comes to hacking data, the sentimental analysis identifies the behavior of the user. Thereby doing so the users are safeguarded from the hackers. So, in future, this system can be used in securing data which are succumbed to high eccentricity. Hence the redundancy in the system is increased.

REFERENCES

1.Abigail Paradise, Asaf Shabtai, AviadElyashar, Christoph Peylo, Mehran Roshandel, Rami Puzis and Yuval Elovici, "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks", IEEE Transactions on Computational Social Systems (2017)

2. Aryan Taheri Monfared and Martin GiljeJaatun, "Handling Compromised Components in an IaaS Cloud installation", Journal of Cloud Computing (2016 Springer)

3.Christopher Kruegel, Gianluca Stringhini, Giovanni Vigna and Manuel Egele, "Towards Detecting Compromised Accounts on Social Networks", IEEE Transactions on Dependable and Secure Computing (2017)

4.Francesca Casamassima and Marco Cremonini, "Controllability of social networks and the strategic use of random information", Computational Social Networks (2017 Springer)

5. Guoyong Zhao and Zhiyu Zhou, "Design and Implementation of the Online Shopping System", Springer-Verlag Berlin Heidelberg (2012)
6. Haining Wang, Sushil Jajodia, Xin Ruan and Zhenyu Wu, "Profiling Online Social Behaviors for Compromised Account Detection", IEEE Transactions on Information Forensics and Security (2016)
7. Imran Erguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords", IEEE Transactions on Dependable and Secure Computing (2017)
8.Niharika Garg, Sandeep Kumar Singh and Simran Bajaj, "A Novel User-based Spam Review Detection", Information Technology and Quantitative Management (2017 ITQM)
9. Nilesh Chakraborty and Samrat Mondal, "Towards Improving Storage Cost and Security Features of Honeyword Based Approaches",6thInternational Conference on Advances in Computing & Communications, (2016 ICACC)
10. Nour EI-Mawass and Saad Alaboodi, "Data Quality Challenges in Social Spam Research", (2017)
11. C. Ramprasath, J. Varun and S. Sri Heera "Survey on Identification of Hacker by Trapping Mechanism", International Journal of Trend in Scientific Research and Development (March 2018).