International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 4, May-June 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Detection of Attacker using Honeywords

**Senthilnayaki B[1], Mahalakshmi G[1], Dharanyadevi P[2], Narashiman D[1]**

[1]Department of Information Science and Technology, CEG, Anna University, Chennai, Tamil Nadu, India
[2]Department of CSE, Puducherry Technological University, Pillaichavadi, Puducherry, India

## ABSTRACT

With the growth of the Internet, there has been a tremendous increase in the number of attacks, and therefore intrusion detection systems (IDS's) have become a mainstay of information security. The purpose of IDS is to help the computer systems deal with attacks. This anomaly detection system creates a database of normal behaviour and deviations from normal behaviour to trigger events during the occurrence of intrusions. Based on the source of data, IDS are classified into host-based IDS and network-based IDS. The proposed work is to validate the correct user or attacker. The system is identified as an abnormal user. An alert will be sent to the authorised user. The proposed system is to supply the fake information to the attacker by using the honeywords technique. A new system is proposed to secure content from various unauthorised users.

***KEYWORDS:*** *Honeywords, Security, Password, Hash Function, Authentication, Attacker*

***How to cite this paper:*** Senthilnayaki B | Mahalakshmi G | Dharanyadevi P | Narashiman D "Detection of Attacker using Honeywords" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-4, June 2022, pp.827-831, URL: www.ijtsrd.com/papers/ijtsrd50074.pdf

IJTSRD50074



## INTRODUCTION

Network security provides the policies and techniques used to prevent and monitor illegal access, abuse, modification, or denial of a computer network. The network administrator controls network security, which entails the permission of access to data on the network. Users select or are granted an ID, password, or other type of authentication that gives them access to information and applications under their control. Network security refers to a wide range of public and private computer networks that are utilised in everyday tasks such as completing transactions and communications between organizations, government agencies, and individuals. Hence, it concerns security for accessing the data from organizations, corporations, and other sorts of institutions. It secures the network while also safeguarding and managing activities. Assigning a unique name and password to a network resource is the most popular and straightforward method of safeguarding it.

### Honeyword

Honeywords are phoney passwords that are kept together with actual passwords and are linked to each user's account. When an attacker obtains the password list, he or she retrieves a large number of password candidates for each account, and the intruder has no way of knowing which one is correct. As a result, if an intruder attempts to log in using a honeyword, the cracked password files can be discovered by the system administrator. Exposure of passwords is a serious security issue that has prompted a huge number of users and organizations, including Yahoo, Rock You, LinkedIn, eHarmony, and Adobe, to take action. One way of detecting the existence of a password database breach is to use a honeypot.

The administrator establishes fake user accounts on purpose to catch intruders and detects a password leak if any of the honeypot credentials are utilized. Making password hashing more complicated and time-consuming is another way to improve the problem. For each account, the Honeyword technique involves having many possible passwords, only one of which is correct. The false page is used to give the hacker the impression of accessing the original data. This decoy page is a fake page that the hacker accesses as if it were the real thing. Also, when the

hacker accesses the fake website, the legitimate user will quickly notice through warnings that an unauthorised user is attempting to access the page. Using the honeywords technique, a novel system is constructed in this paper. The system's basic concept may be utilised as a platform in institutes, businesses, and anywhere else where credential data is protected by a password. It also aids in the monitoring of administrative procedures and the evaluation of performance in order to make improvements. This system takes advantage of services like notification, which increases the system's overall efficiency and customer happiness.

## LITERATURE SURVEY

Imran (2016) provided a new honeyword generating method, which produces better results in terms of flatness. When honeywords are appropriately chosen, a cyber-attacker who bargains a file of hashed passwords has no way of knowing whether the password is the real one or a honeyword for any account. Senthilnayaki et al. (2015) studied several forms of network system attacks and classified them using multiple classifications.

Rivest (2013) developed a way of making hashed passwords more secure. Honeywords must be generated for each user account to increase security. When an attacker acquires a file of hashed passwords and inverts the hash function, the author has no way of knowing whether they have discovered the password or a honeyword. With developments in graphics processing unit (GPU) technology, Kardas et al. (2013) suggested a way to crack a password hash significantly simpler. No server can detect any unauthorised user authentication once the password has been obtained.

Malone and Maher (2012) investigate how passwords are chosen and shared. In lists of chosen terms, Zipf's Law is commonly found. The authors analyse if Zipf's law is a viable contender for characterising the frequency with which passwords are chosen using password lists from four different online sources. Komal et al. (2016) employed the honeywords approach to protect against assaults by unauthorized insiders, preventing them from discerning between genuine sensitive customer data and useless data.

Senthilnayaki and colleagues (2021), In this article, authors simulated Ad Hoc On-Demand Distance Vector networks and examined the impact of different assaults on the network, including wormhole, black hole, and flooding attacks. Researchers are employed WEKA as data mining tools for analysis, which let us retrieve transmitted, received, and discarded packet information in the networks under assault.

Manisha (2015) suggested the Chaffing-With-Tweaking method. The user password is used to seed the generating algorithm, which then changes chosen character locations of the genuine password to generate honeywords. When irregular information access is identified, Dipali and Shyam (2014) provided a method for assessing whether data access is permitted or not. Providing false information to the attacker. This guards against the abuse of the users' personal information. Senthilnayaki et al (2015) reviewed different types of attacks affected in network system and provides various classification to classifies. Sethilnayaki et al (2021) provides the anomaly detection system creates a database of usual behavior and deviations from it, which it utilizes to trigger intrusion detection when it happens. Based on the data source, the IDS model is separated into two types: hostbased IDS and network-based IDS. Honeywords are generated using a variety of current honeyword creation techniques. As a result, every attempted login puts the attacker at danger of being identified. The attacker will also be noticed if they use a brute force approach.

## PROPOSED SYSTEM ARCHITECTURE

The system architecture of the proposed work is shown in Figure 1. It consists of various modules, namely user registration module, honey words generation module, cloud storage, authentication checking, and alert generation.

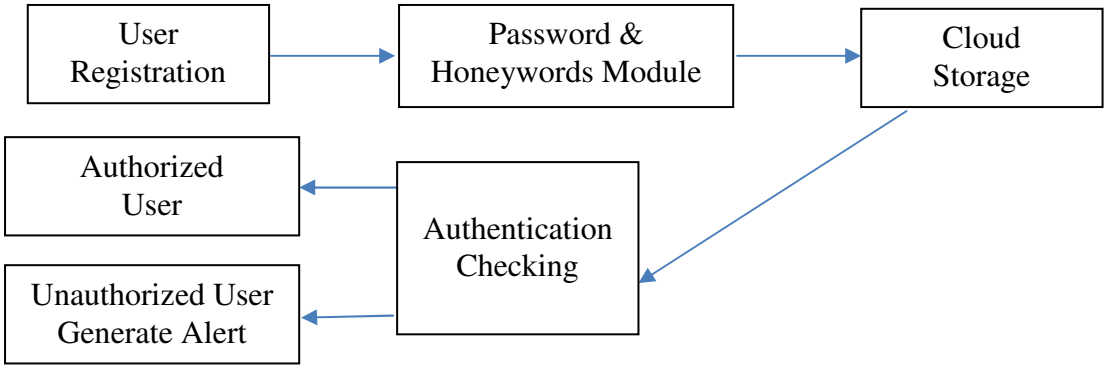


**Figure 1 Unauthorized User System Architecture**

In this proposed work, first create a user profile using the registration module and then generate the user account. Using this information, the registered users can access the data from the database server. Using an existing user account, the system is allowed to access organisational network data. Hence, they are allowed to access their application using the correct login account message. However, the server responds to the end user query based on the authorised users' request. The database server contains username, password, questions and answers with personal information. The authentication checking module is used to check for a legitimate user or a decoy user. The system is detected by an authorised user, then they are allowed to access the organisational database. Else, the user is allowed to access fake pages and this information is sent to the admin.

**Honeyword Checker**

The proposed is to create the module called "authentication checking" here to check and allow correct information on user pages with the help of honeywords. Using honeychecker is to collect hardened systems where the information is stored in secret. The detection of anomalies in the system should have lots of experimentation done by using honeychecker. Once the checker detects the anomaly, it generates an alert message and sends it to an administrator or other authorised person. After sending the silent alert to the correct user, the checker continues the system work. Later, the checker acts as a login monitoring system and tracks the processed operation.

**Honeyword Generation Algorithm**

Password files contain a number of security issues that have impacted millions of individuals and businesses. If a password file is stolen or stolen, it is straightforward to capture most of the plaintext and encrypt passwords using password cracking tools and decryption procedures. So we used honey word creations in this proposed module. That is, the user's password and registered questions are merged, and a key with the name "unknown" is generated.

**Honey Word Generator:**

Step1: Get the position po of the input and password pa.

Step2: reverse the order of the password.

Step3: From 1 to 20, repeat the following steps.

Step4: If each position po corresponds to the checking value,
With pa, assign a real password.
Create a new hash password.

Step5: Otherwise, use the real password as the replacement password.

Step6: Create a new hash password

Step7: The password is a hashmap

Step8: Retrieve the password result

The general flow of the algorithm is

1. Receive string input of password
2. Determine the string's category or categories.
3. Choose the number of buckets
4. Fill bucket with chaff after placing password in it.
5. Fill the remaining buckets with chaff from the respective strategy.
6. Shuffle the set of honeywords and locate the password.
7. return the honeyword set and the sugarword index

**EXPERIMENTATION RESULTS**

This section explains the implementation details of the proposed work. The experimental has been done in Java using NetBeans. First, the hacker detection proposed system is a registration page. On the registration page, you must enter your name, user name, email address, password, confirm password, contact number, and address. The user must register if they are not already a registered user. Figure 2 shows the registration page for the user.

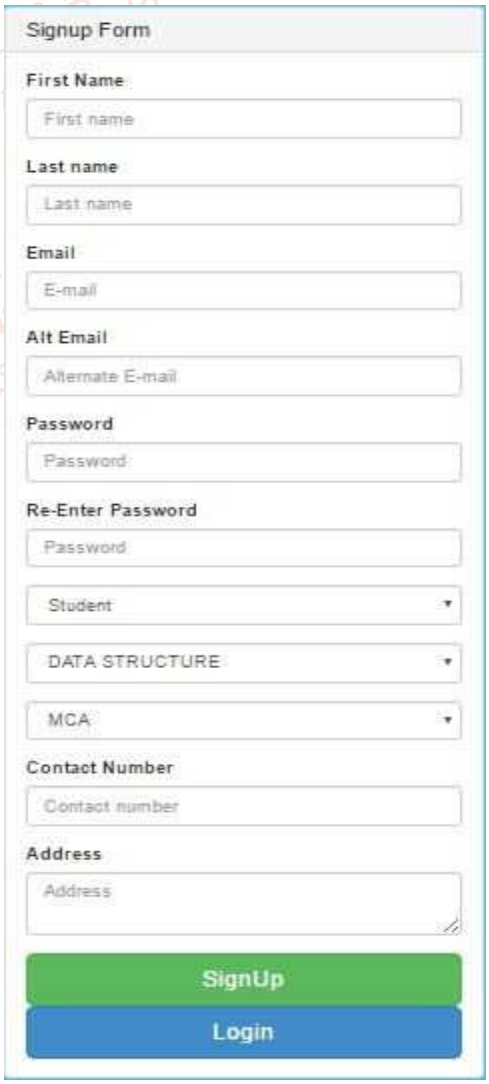


**Figure 2 User Registration Form**

The system collects the page for the planned honeyword generation procedure. All of them include inquiries, such as phone model, mother's name, and school name. People have a pet name, a favorite colour, favorite food, favorite drink, a nickname, a favorite season, and a favorite place. The replies to these questions form the basis of the honeyword production process. After that, go to the legal page by logging in with the right username and password. If a phoney user tries to view the page, the task is delegated to a fake page. Finally, the authorized user receives the alert message. This shows how the system handles notifications. An alarm will ring if the honeywords are typed incorrectly more than three times, informing the original user of the password breach. It will take them to a fake website that looks just like the real one. That page will keep track of them and provide the original user with the updated information. Figure 3 gives the email message to the authorized person.

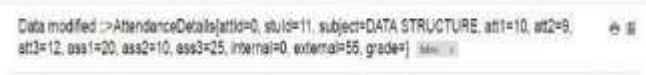


**Figure 3 Email Notification Message**

The comparison clarifies the distinctions between the present and existing systems. It describes the aspects of the proposed system as well as its performance characteristics. Table 1 compares the features of the existing and proposed systems.

**Table 1 Comparison of Existing and Proposed Systems**

| PARAMET ER | EXISTING SYSTEM | PROPOSED SYSTEM |
|---|---|---|
| Notification | Absent | Using email |
| ip detection | Absent | Present |
| Record Activities | Absent | Present |
| Speed of performance evolution | slow | Fast |

The present system lacks feature such as notification, IP detection, and activity recording, but the proposed system does. It sends out alert notifications through email. Performance is evolving at a faster rate than the current system. As a consequence, the suggested system outperforms the current system significantly.

## CONCLUSION

The honeywords technique is used to create a new system in this proposed work. The system's basic concept may be utilised as a platform in institutes, businesses, and anywhere else where credential data is protected by a password. It also aids in the monitoring of administrative procedures and the evaluation of performance in order to make decisions for improvement. This system takes advantage of services like notification, which increases the system's overall efficiency and customer happiness. In the future, this work will be extended to include better notification techniques.

## References

[1] Imran Erguler, (2016). 'Achieving Flatness: Selecting the Honeywords from Existing User Passwords', IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 284-295.

[2] Senthilnayaki B, G. Mahalakshmi, Duraimurugan, Anbarasi N and Prasath Kumar, "Intrusion Detection Using Information Gain Feature Selection and Classification", International Research Journal of Humanities and Interdisciplinary Studies, vol 2. no 11, pp 155-166, 2021.

[3] R. L. Rivest and Juels, (2013). 'Honeywords: Making password cracking detectable', in ACM SIGSAC conference on Computer & communications security, pp. 145-159.

[4] GenKardas, S and Kiraz, M. S. (2013). 'Examination of a New Defense Mechanism: Honeywords'. IACR Cryptology ePrint Archive, pp. 690-696.

[5] D. Malone and K. Maher. (2012). 'Investigating the Distribution of Password Choices', in ACM 21st International Conference on World Wide Web, pp. 301-310.

[6] Ms.Komal Naik, Varsha Bhosale and Vinayak D.Shinde. (2016). 'Generating Honeywords from Real Passwords with Decoy Mechanism'. International Journal for Research in Engineering Application & Management. Vol. 2, no.4, pp. 1-7.

[7] Senthilnayaki, B., Chandralekha, M and Venkatalakshmi, K, "Survey of data mining technique used for intrusion detection", International Journal of Technology and Engineering System, vol.7, no 2, pp.166-171, 2015.

[8] Senthilnayaki, B, Anbarasi, N., Mahalakshmi, G and Duraimurugan, J, (2021). IoT: Analysis of Various Attacks Using AODV Protocol. International Journal of Progressive Research in Science and Engineering, 2(11), 29-32, 2021.

[9] Manisha Jagannath Bhole. (2015). 'Honeywords: A New Approach For Enhancing Security'. International Research Journal of Engineering and Technology (IRJET). Vol.2, no. 8, pp. 1563-1566.

[10] Dipali Dhumal, Shyam Gupta. (2015). 'Effective Approach to Detection of Password File Using Honeywords'. International Journal of Science and Research (IJSR). vol. 4, no. 12, pp. 930-932.

[11] Balakrishnan, S., Venkatalakshmi, K., & Kannan, A. (2014). Intrusion detection system using feature selection and classification technique. International journal of computer science and application, 3(4), 145-151.

[12] F. Cohen. (2006). 'The use of deception techniques: Honeypots and decoys'. Handbook on Information Security, vol. 3, pp. 646–655.

[13] Senthilnayaki, B., Venkatalakshmi, K., & Kannan, A. (2019). Intrusion detection system using fuzzy rough set feature selection and modified KNN classifier. Int. Arab J. Inf. Technol., 16(4), 746-753.