International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Honey Cloud: A Honeypot Network Approach for Enhanced Security to the Cloud

A.VISHNU PRIYA [1],I.Y BHARATH[2], P.SAI KIRAN[3],V.NARESH KUMAR, G. SWARANALATHA

UG Student, UG Student, UG Student, Associate Professor, Assistant professor

Department of CSE
CMR Technical Campus Hyderabad, Telangana, India
vishnupriya28a@gmail.com, iybharath339@gmail.com, saikiranpuppala774@gmail.com, nareshkumar99890@gmail.com, gswarnalatha.cse@cmrtc.ac.in

How to Cite this Article:

PRIYA, A., BHARATH, I., KIRAN, P. & SWARANALATHA, G. (2026). Honey Cloud: A Honeypot Network Approach for Enhanced Security to the Cloud. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.336

https://doi.org/ 10.55041/ijcope.v2i4.336

Abstract—

Cloud computing systems have become very popular because they make it easy for users to store and access data from anywhere. At the same time, these systems face several security challenges. Attacks such as credential stuffing, password guessing, and brute-force attempts are common, where an attacker keeps trying different combinations of usernames and passwords to gain access.

To counteract these threats, one common method is to restrict the number of login attempts. When a user enters incorrect credentials multiple times, the account may be temporarily locked. While this approach can reduce unauthorized access, it does not help in understanding how the attacker is attempting to break into the system. As a result, administrators get very little information about attack patterns.

Firewalls are also used to filter and block suspicious requests. However, they mainly focus on prevention and do not provide detailed insights into attacker behavior. To address this issue, a honeypot system can be used. A honeypot is a dummy system designed to look like a real one and is placed between users and the actual backend server.

In this approach, normal users continue to access the system as usual, but any suspicious activity is redirected to the honeypot. Since attackers believe they are interacting with a genuine system, they continue their actions without realizing they are being observed. This helps in protecting the real system from damage.

The honeypot also allows administrators to safely study attacker behavior. As a future step, logging and monitoring features should be developed and integrated to record login attempts and to examine how attackers interact with the system. These improvements will help collect data on attack techniques and provide concrete information for enhancing overall security measures.

Keywords—Brute force attacks, Honeypot Environment, Cloud Security, Credential Stuffing, Attack Monitoring and Logging

I. INTRODUCTION

Cloud computing has significantly reshaped the way organizations handle data and applications. It enables businesses to store, process, and access information from anywhere while benefiting from scalability, flexibility, and reduced operational costs. As a result, its adoption has grown rapidly across various sectors. However, this widespread usage also introduces serious security challenges. The distributed and dynamic nature of cloud environments makes them vulnerable to a wide range of cyber threats, including data breaches, Distributed Denial of Service (DDoS) attacks, malware intrusions, and advanced persistent threats (APTs).

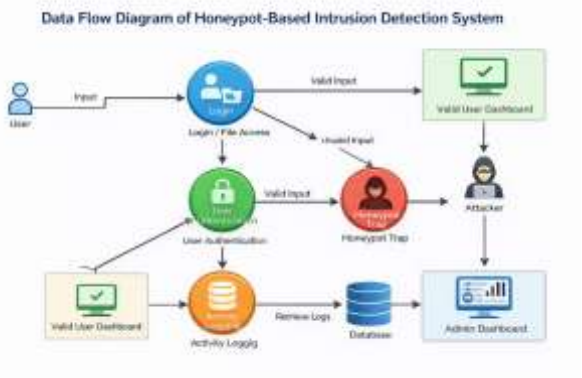
Conventional security techniques such as firewalls and signature-based intrusion detection systems continue to play an important role in protecting systems. However, these methods are often limited when it comes to detecting sophisticated or unknown attacks, especially zero-day vulnerabilities that do not match existing attack patterns. This limitation highlights the need for more intelligent and proactive security mechanisms.

One effective strategy to enhance cloud security is the use of honeypots. A honeypot acts as a decoy system designed to mimic real services or resources, intentionally attracting potential attackers. Rather than directly preventing attacks, it allows security analysts to monitor malicious activities in a controlled environment. This helps in understanding attacker behavior, identifying new attack patterns, and improving overall defense mechanisms without risking actual systems.

In this research, we propose Honey Cloud, a cloud-focused security framework based on honeypot technology. The system deploys multiple virtual honeypots across different layers of the cloud infrastructure, creating a distributed monitoring environment. This approach enables continuous observation of suspicious activities and supports real-time threat detection. By leveraging these insights, the system aims to strengthen cloud security and provide a more adaptive defense against evolving cyber threats.

II. LITERATURE REVIEW

The rapid growth of cloud computing has led to increased attention on security mechanisms, particularly in the areas of intrusion detection and attack prevention. As cloud platforms continue to



evolve, traditional security solutions such as firewalls and signature-based intrusion detection systems (IDS) have shown limitations in detecting sophisticated and unknown attacks. These systems primarily depend on predefined rules and known attack patterns, making them less effective in identifying zero-day threats and adaptive attack strategies.

To address these limitations, researchers have explored advanced and proactive security techniques. One of the most promising approaches is the use of honeypot systems. A honeypot is a deliberately designed decoy environment that imitates real systems or services to attract attackers. Instead of directly preventing attacks, honeypots focus on monitoring and analyzing malicious activities. This approach allows security administrators to gain deeper insights into attacker behavior, techniques, and strategies without exposing critical resources.

Several studies highlight the effectiveness of honeypots in detecting unauthorized access attempts such as brute-force attacks, credential stuffing, and unauthorized scanning activities. By capturing real-time interaction data, honeypots provide valuable information that can be used to strengthen existing security mechanisms. Unlike traditional IDS, which may generate false positives, honeypots generally interact only with malicious users, making the collected data more relevant and accurate.

With advancements in cloud technology, modern honeypots have been adapted to support distributed and scalable environments. Researchers have proposed cloud-based honeypot frameworks that can be dynamically deployed across virtual machines and network layers. These systems are capable of simulating realistic services, thereby increasing the chances of deceiving attackers. Integration of logging and monitoring tools has further enhanced the ability to track attacker actions, including login attempts, navigation patterns, and exploitation methods.

Despite these advantages, existing research also identifies several challenges associated with honeypot systems. Scalability remains a major issue when deploying honeypots in large-scale cloud infrastructures. Additionally, real-time detection and response capabilities are often limited due to the high volume of generated data. Managing and analyzing this data efficiently requires advanced processing techniques and resources. There are also concerns related to legal and ethical considerations, particularly when dealing with attacker data collection and system interaction.

Another important challenge is the integration of honeypot systems with existing cloud security frameworks. Many traditional systems are not designed to work seamlessly with deception-based techniques, which can lead to compatibility issues. Furthermore, if not properly configured, honeypots themselves may become targets for misuse or may fail to convincingly simulate real systems.

In conclusion, the literature indicates that honeypots play a significant role in enhancing cloud security by providing a proactive approach to threat detection and analysis. While they offer valuable insights into attacker behavior and improve overall system defense, further research is required to address challenges related to scalability, data management, real-time response, and system integration. Continuous advancements in these areas will help in developing more effective and reliable honeypot-based security solutions for modern cloud environments.

III. METHODOLOGY

Step	Module	Description
1	User Interaction	Users access the system through login, registration, upload, and download
2	Fake Login (Honeypot)	Fake login page captures attacker credentials and behavior
3	Request Processing	Django backend processes user requests using views and URL routing
4	Activity Logging	Stores attacker details like username, password, and actions performed
5	File Handling	Allows file upload and download to simulate a real system
6	Database Storage	Stores user data, login attempts, and activity logs in database
7	Admin Monitoring	Admin dashboard is used to view and analyze suspicious activities
8	Result Analysis	Helps in detecting threats

The proposed Honey Cloud framework is designed as a distributed security system that uses honeypot technology to improve protection in cloud environments. The main idea is to combine deception with continuous monitoring so that suspicious activities can be detected and studied as they occur. The system is divided across different layers of the cloud, such as the application, network, and data layers, where decoy environments are placed carefully.

In this framework, the honeypots are built to look like real services, including web applications and databases. This makes attackers believe they are interacting with an actual system, which increases the chances of capturing their actions. Both low-interaction and high-interaction honeypots are used. Low-interaction honeypots are mainly useful for identifying simple or automated attacks, while high-interaction honeypots provide a more realistic setup that helps in observing detailed attacker behaviour.

To make the system flexible and easy to expand, virtualization and container technologies are used. These technologies allow multiple honeypots to be deployed and managed efficiently based on the system's needs. Each honeypot works independently, but all of them contribute to the overall security setup.

All activities inside the honeypots are monitored continuously. Details such as IP addresses, login attempts, request patterns, and attack data are recorded and stored in a central logging system. This information is later analyzed to understand how attacks are carried out and to identify possible weaknesses in the system.

In summary, this approach helps in detecting threats while keeping the real cloud system safe. By using deception along with monitoring and scalable deployment, the framework provides a practical way to study attacks and improve security over time.

IV. RESULTS AND DISCUSSION

The Honey Cloud framework was tested in a controlled cloud-based environment to examine how effectively it can detect and handle security threats. During the testing phase, the system was able to attract and record different types of malicious activities, such as repeated login attempts, unauthorized access, and injection-based attacks. The placement of honeypots at different layers of the cloud helped in observing attacker behavior from multiple points within the system.

The observations show that the proposed system improves threat detection when compared to traditional intrusion detection approaches. Since the honeypots directly interact with suspicious users, the chances of identifying real attacks are higher. The use of both low-interaction and high-interaction honeypots played an important role in this process. Low-interaction honeypots were effective in quickly identifying basic and automated attacks, while high-interaction honeypots allowed a more detailed study of attacker actions and methods.

Another important outcome is the improved visibility of attack patterns. The data collected from different honeypots provided useful information about how attackers attempt to access the system and what techniques they use. This makes it easier to analyze threats and take preventive measures in the future.

Overall, the results show that the Honey Cloud framework not only helps in detecting attacks but also provides better understanding of attacker behavior. This combination of detection and analysis makes the system more effective in strengthening cloud security.

V. CONCLUSION

This work presented the Honey Cloud framework, a security approach based on honeypot technology for enhancing protection in cloud environments. With the increasing use of cloud services, security threats have become more frequent and complex, making traditional defense methods less effective against modern attack techniques.

The proposed system addresses this challenge by deploying distributed honeypots across different layers of the cloud. These decoy systems are designed to engage attackers and capture their activities without exposing the actual infrastructure to risk. By combining low-interaction and high-interaction honeypots, the framework is capable of detecting both simple automated attacks and more advanced intrusion attempts.

The study shows that this approach not only improves threat detection but also helps in understanding attacker behavior. Such insights are useful for strengthening existing security measures and preparing better defense strategies. Overall, the Honey Cloud framework provides a practical and effective solution for improving cloud security in a controlled and scalable manner.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their institution for providing the necessary resources and support to carry out this work. Special thanks are extended to the project guide for their valuable guidance, suggestions, and continuous encouragement throughout the development of this project.

The authors also appreciate the support and cooperation of friends and peers who contributed indirectly to the successful completion of this work.

REFERENCES

Lance Spitzner, Honeypots: Tracking Hackers, Addison-Wesley, 2003.

Jyatiti Mokube and Michele Adams,
Honeypots: Concepts, Approaches, and Challenges, Proceedings of the 45th Annual Southeast Regional Conference, 2007.

Karthik Sadasivam, Banuprasad Samudrala, and T. Andrew Yang,
Design of Network Security Projects Using Honeypots, Journal of Computing Sciences in Colleges.

Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,
Ensuring Data Storage Security in Cloud Computing, IEEE International Workshop on Quality of Service, 2009.

Balachandra Reddy Kandukuri, Ramya Paturi, and Atanu Rakshit,
Cloud Security Issues, IEEE International Conference on Services Computing, 2009.

Abdul Elminaam, Mohamed Kader, and Mohamed Hadhoud,
Performance Evaluation of Symmetric Encryption Algorithms, International Journal of Network Security.