HONEYPOT-BASED DATA BREACH AVOIDANCE SYSTEM

Anushka Purwar, Diksha Soni, Gaurangi Rawat, Nisha Yadav
B.Tech
Department of Computer Science and Engineering,
Inderprastha Engineering College, Ghaziabad, 201010, India

Vanshika Gupta
Assistant Professor
Computer Science and Engineering,
Inderprastha Engineering College Ghaziabad, 201010, India

Abstract— **A data breach is an event where information is stolen or attained from a system without the knowledge or authorization of the system's owner. This can be a serious concern for organizations that involve losing sensitive, proprietary, or confidential information such as credit card numbers, customer data, or trade secrets. With the right and smart application of Computer science aptitude, Data breaches cannot only be avoided but also helps understand attackers' moves. One such strategy is Honeypot. This strategy involves maintaining a sacrificial database that's intended to attract cyber attacks. It mimics a target for hackers and uses their intrusion attempts to gain information about cyber criminals and the way they are operating or to distract them from other targets. This system is also powered by detecting change using SHA256 hashing on piece-wise data.**

Keywords— **SHA256 , Honeypot , Intrusion Detection System , Intrusion Prevention System**

I. INTRODUCTION

Honeypots are widely used by cyber security companies with an aim to detect and trap any unsafe attempt of penetrating into the system. There have been a lot of advances in the field of honeypot model as a way of securing servers and other devices. The Modern honeypot network is also used as an Intrusion Detection System (IDS). Government agencies like National ICT Research and training centre also use Honeypots as a security model[1].

Honeypots are viewed as a successful technique to track programmer conduct and uplift the viability of security instruments. Honeypots are specifically designed to not only purposely engage and deceive hackers but also identify malicious activities performed over the Internet and can be counted as an effective method to track hacker behaviour. Honeypots can be defined as systems or assets which are used to not only trap, monitor but to also identify erroneous requests present within a network[2].

A honeypot is nothing but a system which is created to emulate the services that are executed on the server in order to observe the patterns of the attacks[6].

Honeypots aim is to analyze, understand, watch and track attacker's behaviour in order to create systems that are not only secure but can also handle such traffic. It is a closely monitored computing resource that we want to be probed, attacked, or compromised. "More precisely, it is an information system resource whose value lies in unauthorized or illicit use of that resource." [5].

This paper centres around a new investigation of hash work prerequisites for enormous information applications and a related key-based hash work plan procedure that makes the continuous assortment, rundown, examination, and decision-making in light of streaming information. A record-examining strategy is recommended that involves fundamental big data mass processing operations to foster an effective and reliable verification of recoverability calculation.

II. RELATED WORK

With the rapid increase in the number of users, there is a rise in issues related to hardware failure, web hosting, space, and memory allocation of data, which directly or indirectly lead to the loss of data. With the objective of providing services that are reliable, fast, and low in cost, we turn to cloud-computing practices. With tremendous development in this technology, there is an ever-increasing chance of its security being compromised by malicious users. A way to divert malicious traffic away from systems is by using Honeypot. It is a colossal strategy that has shown signs of improvement in the security of systems. Keeping in mind the various legal issues one may face while deploying Honeypot on third-party cloud vendor servers, the concept of Honeypot is implemented in a file-sharing application that is deployed on a cloud server.[2]. "Honeypot is the proactive defense technology, in which resources are placed in a network with the aim to observe and capture new attacks”. A honeypot-based model for intrusion detection systems (IDS) to obtain the best user data about the attacker. Aim to use this trend for early prevention so that preemptive action is taken before any unexpected harm to security system[3].

The honeypot system is relatively easy to maintain and does not face the various threats that more complex security tools do, such as incorrect configuration, system crashes, and failures. A high-interactivity honeypot system borrows the structure of the kernel-based operating system and adopts a modular design to complete the central node part of the highinter activity honeypot system[8].

Honeypots are setup for detection, gathering information and prevention of attacks. They produce early warnings about threats and attacks. The honeypot is a response and detection tool, instead of avoidance. Since honeypots cannot keep a

Specific intrusion or spread virus, it only gathers data and distinguishes the attack pattern[4].

III. PROPOSED METHODOLOGY

In a Cloud environment, when web security is breached or fails, the next big thing that organizations aim at is, securing information stored in the servers and avoiding data breaches. In the proposed system, we aim at deploying a Honeypot server that triggers when intrusion is detected by the system. Once triggered, a smart session analysis is done on the attacker's move, to know even more about the attacker. The proposed solution involves integrating honeypots into an Intrusion Detection System (IDS) to enhance cybersecurity defences. Key components include deploying honeypots strategically, developing a comprehensive IDS architecture (Fig.2), and implementing real-time monitoring for prompt threat detection. Data analysis and correlation, threat intelligence integration, and automated response mechanisms contribute to an adaptive and proactive security posture. Continuous improvement, user training, and regulatory compliance ensure the long-term effectiveness and compliance of the cyber security solution.

A. Advantages of the Proposed System

1. Smart session analysis on Attacker's moves.
2. Main data is not exposed to intruders.
3. Alerts cloud providers about incidents to make the system even more resistant. 4. Backup and recovery

B. Proposed System

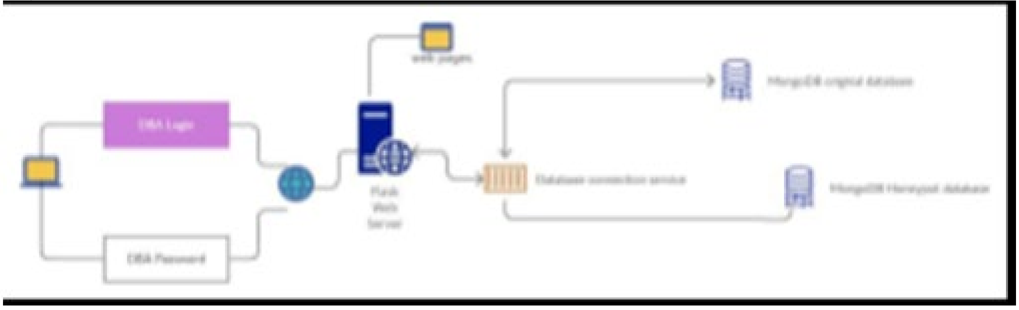

web pages
DBA Login
DBA Password
Flask
Web
Server
MongoDB original database
Database connection service
MongoDB Honeypot database

Fig. 1 System Design

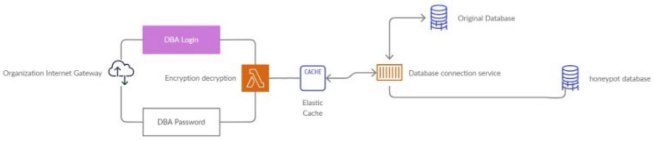


Fig. 2 System Architecture

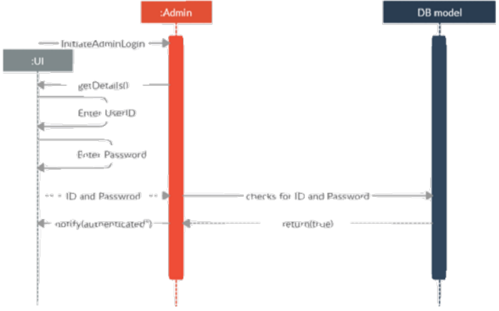


Fig. 3 Sequence Diagram’

C. Activity Diagram

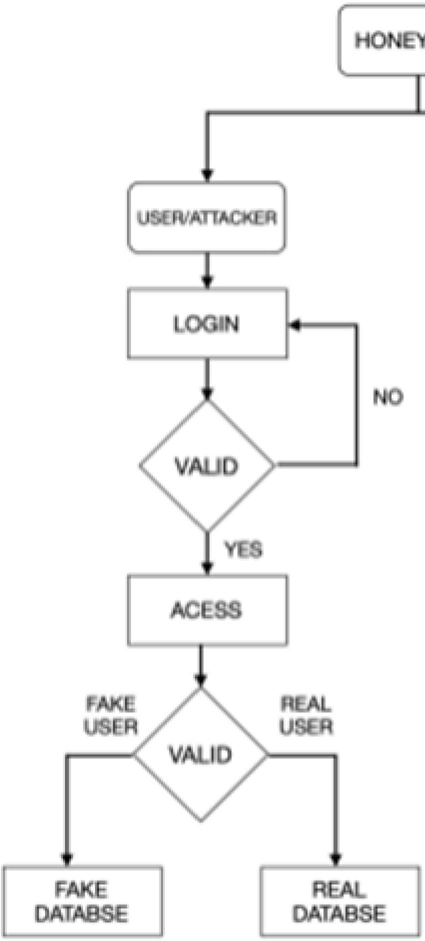


Fig. 4 Activity Diagram

IV. IMPLEMENTATION

A. Modules in Proposed System

1. MongoDB Application with MongoDB Server running at the desired Port.
2. Python Driver Code
3. Web pages along with Script Sheets (.js) and Style Sheets (.css).
4. Database (JSON Data of Users)

B. Implementation of Modules

The first Module, MongoDB Software, will be downloaded from the official MongoDB site and installed at the desired location. Next, a Mongo DB server will be running in the background at port number 27017. This server will be receiving the Queries from Module 2, which is Python driver Code. Once the query is received, the server will execute it and sends the result back to that driver code.

In Second Module, The Python program will be using two essential libraries, Flask and Mongo. Python program will use Flask for all web application creation and maintenance tasks.

The Third Module consists of all the desired web pages along with Style Sheets i.e., CSS files, and Script Sheets i.e., JavaScript Files needed for the application.

The Fourth module is the database collection of User data, and Also Honeypot Data. These files are encrypted and securely stored.

C. Implementing Flask Server

Without a web server, In a traditional static web application, we write the “on click” function for the button in the web page to redirect any other desired web page (rendering a web page without doing any computation).

But with a web server and an API like python flask, we want a specific python function to be executed whenever we click on an action-listener button. So in the “on click” field of any button, we now mention the function to be executed instead of mentioning the name of the web page to be rendered.

Now In the python function, we do perform some computations like taking input from text fields, analyzing

some logic/flags, and then, with some intelligence, we render an appropriate web page.
The Flask server will be running at the desired port number (7000 in our application).

V. RESULTS

Data sets are small as Honeypots collect the data about any malicious activity which includes attack or any kind of unauthorised act. Honeypots collect the data which can be easily managed and analyzed [7]. False Alarms about a attack are reduced when they capture unauthorized activity. Honeypots usually tend to make use of least possible number of resources.[9]. Even encrypted attacks can be captured by Honeypots. Some versions of Honeypot are easily deployed and hence can be easily maintained.
"Fig. 5" shows the initial login page of the app, where the user /DBA can log into their account using their DBA code and password.

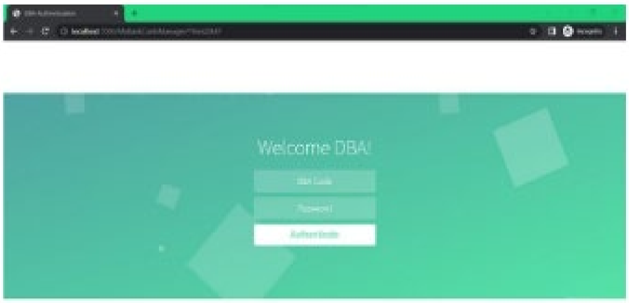
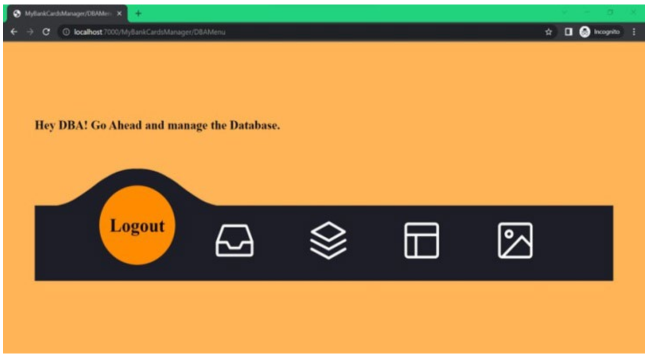


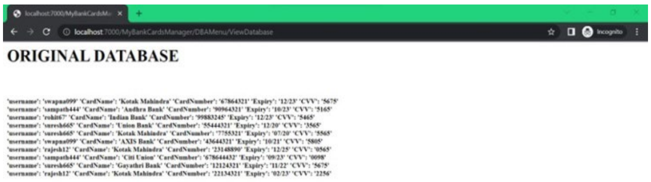
Fig. 5 Login Page

If DBA authentication is successful then DBA will land on main page and can view original database as shown in "Fig. 6" and "Fig 7" respectively.



Hey DBA! Go Ahead and manage the Database.

Fig. 6 Main Page

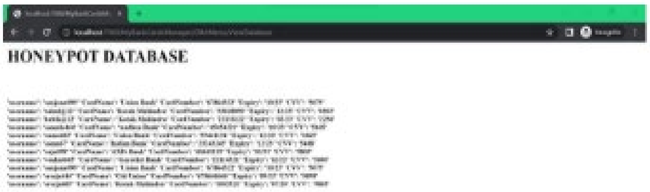


localhost:7000/MyBankCardsManager/DBAMenu/ViewDatabase

ORIGINAL DATABASE

```
'username': 'swapna099' 'CardName': 'Kotak Mahindra' 'CardNumber': '67864321' 'Expiry': '12/23' 'CVV': '5675'
'username': 'sampath444' 'CardName': 'Andhra Bank' 'CardNumber': '90964321' 'Expiry': '10/23' 'CVV': '5165'
'username': 'rohit67' 'CardName': 'Indian Bank' 'CardNumber': '99883245' 'Expiry': '12/23' 'CVV': '5465'
'username': 'suresh665' 'CardName': 'Union Bank' 'CardNumber': '55444321' 'Expiry': '12/20' 'CVV': '3565'
'username': 'suresh665' 'CardName': 'Kotak Mahindra' 'CardNumber': '7755321' 'Expiry': '07/20' 'CVV': '5565'
'username': 'swapna099' 'CardName': 'AXIS Bank' 'CardNumber': '43644321' 'Expiry': '10/21' 'CVV': '5805'
'username': 'rajesh12' 'CardName': 'Kotak Mahindra' 'CardNumber': '23148890' 'Expiry': '12/25' 'CVV': '0565'
'username': 'sampath444' 'CardName': 'Citi Union' 'CardNumber': '678644432' 'Expiry': '09/23' 'CVV': '0098'
'username': 'suresh665' 'CardName': 'Gayathri Bank' 'CardNumber': '12124321' 'Expiry': '11/22' 'CVV': '5675'
'username': 'rajesh12' 'CardName': 'Kotak Mahindra' 'CardNumber': '22134321' 'Expiry': '02/23' 'CVV': '2256'
```

Fig. 7 Original Database



HONEYPOT DATABASE

[illegible]

Fig. 8 SacriFcial Database

If Login fails 3 times then attacker will be diverted to a sacrificial database as shown in "Fig. 8"

VI. CONCLUSION

In conclusion, the implementation of a cybersecurity strategy utilizing honeypots and SHA256 hashing presents a proactive approach to mitigating the risks associated with data breaches. By mimicking a target for hackers, the honeypot system serves not only to divert and distract attackers but also to provide valuable insights into their tactics and methods. The integration of SHA256 hashing on piece-wise data enhances the system's capability to detect and respond to unauthorized changes, thereby fortifying the overall security posture. The potential benefits of this strategy include a reduction in successful cyber-attacks, early detection of threats, and a deeper understanding of the evolving landscape of cybercriminal activities. By leveraging computer science aptitude and smart application of these technologies, organizations can not only bolster their defenses but also gain a proactive understanding of potential security threats.
It is crucial to continuously assess and adapt cybersecurity measures based on the evolving nature of cyber threats. Regular monitoring, feedback from security professionals, and iterative improvements contribute to the overall effectiveness of the implemented strategy. While no security solution can offer absolute guarantees, the combination of honeypots and SHA256 hashing represents a proactive and dynamic defense mechanism against unauthorized access and potential data breaches.
In essence, this cybersecurity strategy is a valuable tool in the ongoing battle to secure sensitive and confidential information, providing organizations with the means to not

only prevent but also to learn from and respond to cyber threats effectively.

VII. FUTURE SCOPE

1. Use an SSH connection to access the data instead of MongoDB. (looks more close to reality)
2. To optimize for cost, it is not recommended to keep these decoy systems scaled up all the time, they should spawn only when an attacker crosses a certain level of control measures.

VIII. ACKNOWLEDGEMENT

We take this opportunity to thank our teachers and friends who helped us throughout the project.
First and foremost I would like to thank my guide for the project (Vanshika Gupta, Supervisor, and CSE) for her/his valuable advice and time during development of project.
We would also like to thank Dr. Vijai Singh (HoD, Computer Science Department) for his constant support during the development of the project

IX. REFERENCES

[1]. Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).

[2]. Intrusion Detection and Prevention using Honeypot Network for Cloud Security 10th International Conference on Cloud Computing, Data Science &Engineering(Confluence).

[3]. Honeypot-based intrusion detection system: A performance analysis, Published in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).

[4]. Why you need honeypots in the cloud: L. Spitzner, “The Value of Honeypots”, 10thJan, 2003. (A guidehttps://www.developer-tech.com/news/2020sep/02/why-you-need-honeypots-in-the-cloud-a-guide/)

[5]. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Kar l W., “Scientific Cloud Computing: EarlyDefinition and Experience,” 10th IEEE Int. Conference onHigh Performance Computing andCommunications, pp. 825- 830, Dalian, China , Sep. 2008 .

[6]. SQL Injection Avoidance for Protected Database with ASCII using SNORT and Honeypot, 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[7]. Karthik Sadasivam, Banuprasad Samudrala, T. Andrew Yang. “Designof Network Security Projects using Honeypots”, University of Houston.

[8]. A Highly Interactive Honeypot-Based Approach to Network Threat Management Future Internet 2023

[9]. Gurpreet Singh, SupriyaKinger”Integrating AES, DES, and 3 -DES Encryption Algorithms for Enhanced DataSecurity “International Journal of Scientific &EngineeringResearch, Volume 4, Issue 7, july-2013.

[10]. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied CryptographyCRC Press.

[11]. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.

[12]. A Study on Advancement in Honeypot-based Network Security Model, Published in 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)