INTRUSION DETECTION AND PREVENTION USING HONEYPOT NETWORK FOR CLOUD SECURITY

Mohammed Muzammil[1], Mohammed Mubashir[2], Mohammed Zahur Uddin[3], Mrs. L. Vaishnavi[4]
[1,2,3]B. E Student, Department of CSE, ISL College of Engineering, India.
[1]Assistant Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

ABSTRACT: 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 is directly or indirectly leading 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 a tremendous development in this technology, there is 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 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 which is deployed on cloud server. This paper discusses the detection attacks in a cloud-based environment as well as the use of Honeypot for its security, thereby proposing a new technique to do the same.

INTRODUCTION

The ability to store, distribute, and access data on a device that is linked to a network—preferably the internet—at any time and from any location is known as cloud computing. With cloud computing, you may use any device to access an expanded, physically-free storage space that is connected to the internet and available from anywhere in the world. It has a shared data storage space and a vast number of computer units linked in real time over the internet. Because a cloud-like form was first used to portray network telephone schematics and subsequently the Internet as an abstraction of the underlying infrastructure it represents, the phrase "the cloud" is used as a metaphor for the Internet. Honeypots are seen as an effective way to monitor the behavior of programmers and improve the efficacy of security tools. Honeypots are a useful tool for tracking hacker behavior since they are made expressly to not only lure and trick hackers, but also to detect harmful activity occurring online. Systems or assets that are used to catch, monitor, and detect erroneous requests inside a network are known as honeypots. They differ in the level of involvement they provide the attackers, ranging from minimal to medium and high. Each style has pros and cons of its own. Their goal is to build systems that are both safe and capable of managing this kind of traffic by analyzing, comprehending, observing, and tracking the behavior of attackers. We want to explore, attack, or hack this highly watched computational resource. "To be more specific, it is a resource within an information system whose value is derived from its unauthorized or illicit use."

Problem Statement:

Cloud-based Honeypots give the capacity to explore and examine assaults that hit ordinary customers.Having them permits a specialist to interpret the IP locations and malware being utilized into security content that can ensure a normal cloud environment. Once those IP addresses have been distinguished, they will then lead a ping scope and defencelessness output to discover a shortcoming in the system outline or vulnerabilities in programming that can be misused. It's conspicuous yet genuine; awful folks pursue the weakest focuses the most often [9]. There are upsides of utilizing a cloud construct Honeypot in light of a cloud framework is like customary Honeypots in that it ought to have the capacity to decide whether a cloud framework has been traded off or endeavours were made to do so.

At last, they can essentially sit and log all movement coming into the cloud site; and in light of the fact that it's utilized for this particular reason practically any action ought to be dealt with as instantly suspicious. Honeypots can serve to make dangers more obvious and go about as an early alert framework, which gives a cloud organization a more proactive way to deal with security instead of responsive. Any association with either outside resources/areas or cloud administrations ought to deploy cloud-based Honeypots.

LITERATURE SURVEY

Design of Privacy-Preserving Cloud Storage Framework

AUTHORS: RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui,

ABSTRACT: Privacy security is a key issue for cloud storage. To solve this problem, the paper proposes a privacy-preserving cloud storage framework, which includes the design of data organization structure, the generation and management of keys, the treatment of change of users' access right and dynamic operations of data, and the interaction between participants. We design an interactive protocol and an extirpation-based key derivation algorithm, which are combined with lazy revocation, multi-tree structure and symmetric encryption to form a privacy-preserving, efficient framework for cloud storage. A system is realized which is based on the framework. The paper analyzes the effectiveness of extirpation-based key derivation algorithm, the overhead of the system and the privacy security of the framework. Finally, we summarize our work and introduce our future research directions.

Scientific Cloud Computing: EarlyDefinition and Experience

AUHORS: Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W

ABSTRACT: Cloud computing emerges as a new computing paradigm which aims to provide reliable, customized and QoS guaranteed computing dynamic environments for end-users. This paper reviews recent advances of Cloud computing, identifies the concepts and characters of scientific Clouds, and finally presents an example of scientific Cloud for data centers.

Ensuring Data Storage Security in Cloud Computing

AUTHORS: Cong Wang, Qian Wang, KuiRen and Wenjing Lou,

ABSTRACT: Cloud computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel

controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Comparison of Symmetric and Asymmetric Cryptography withExisting Vulnerabilities and Countermeasures

AUTHORS: Yogesh Kumar, Rajiv Munjal and Harsh Sharma

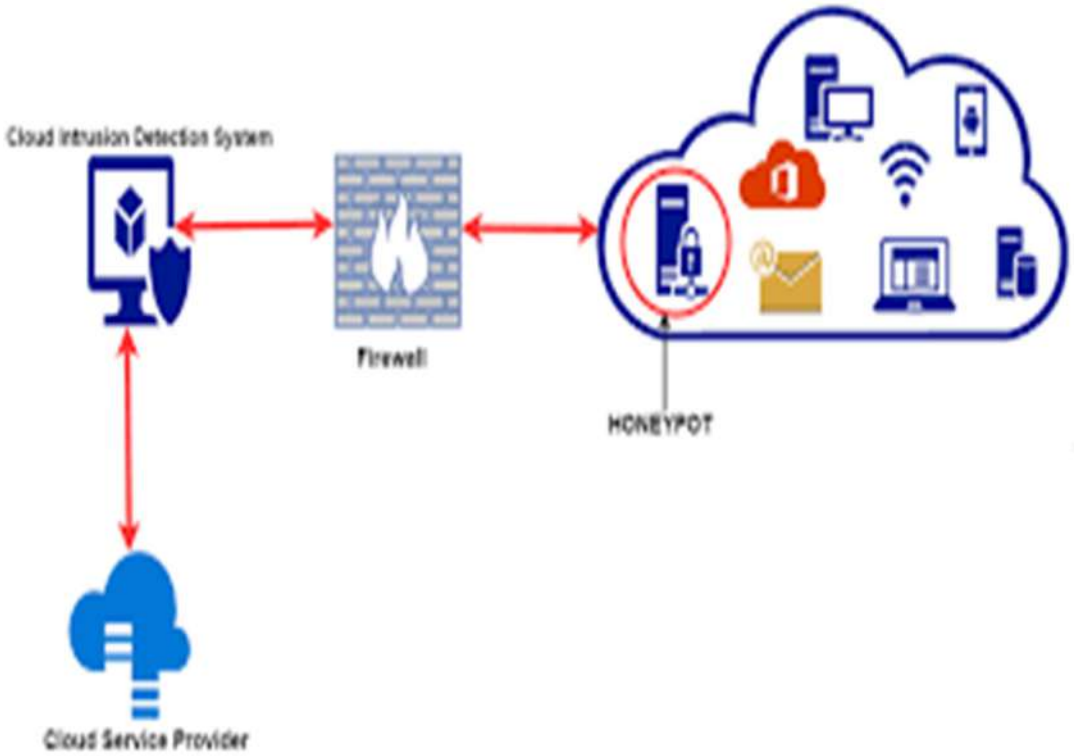
ABSTRACT: Internet and networks application are growing very fast, so the need to protect such application are increased by using cryptographic methods. The two widely accepted and used cryptographic methods are symmetric and asymmetric. The DES ideally belongs to the category of symmetric key cryptography and RSA belongs to the category of asymmetric key cryptography. This paper comprises of brief description of RSA and DES cryptography algorithms and their existing vulnerabilities along with their countermeasures. Besides this, there is a theoretical performance analysis and comparisons of symmetric and asymmetric cryptography.

Cryptography Algorithm Compaison ForSecurity Enhancement In Wireless Intrusion Detection System

AUTHORS: Mr. Gurjeevan Singh, Mr. AshwaniSingla and Mr. K S Sandha

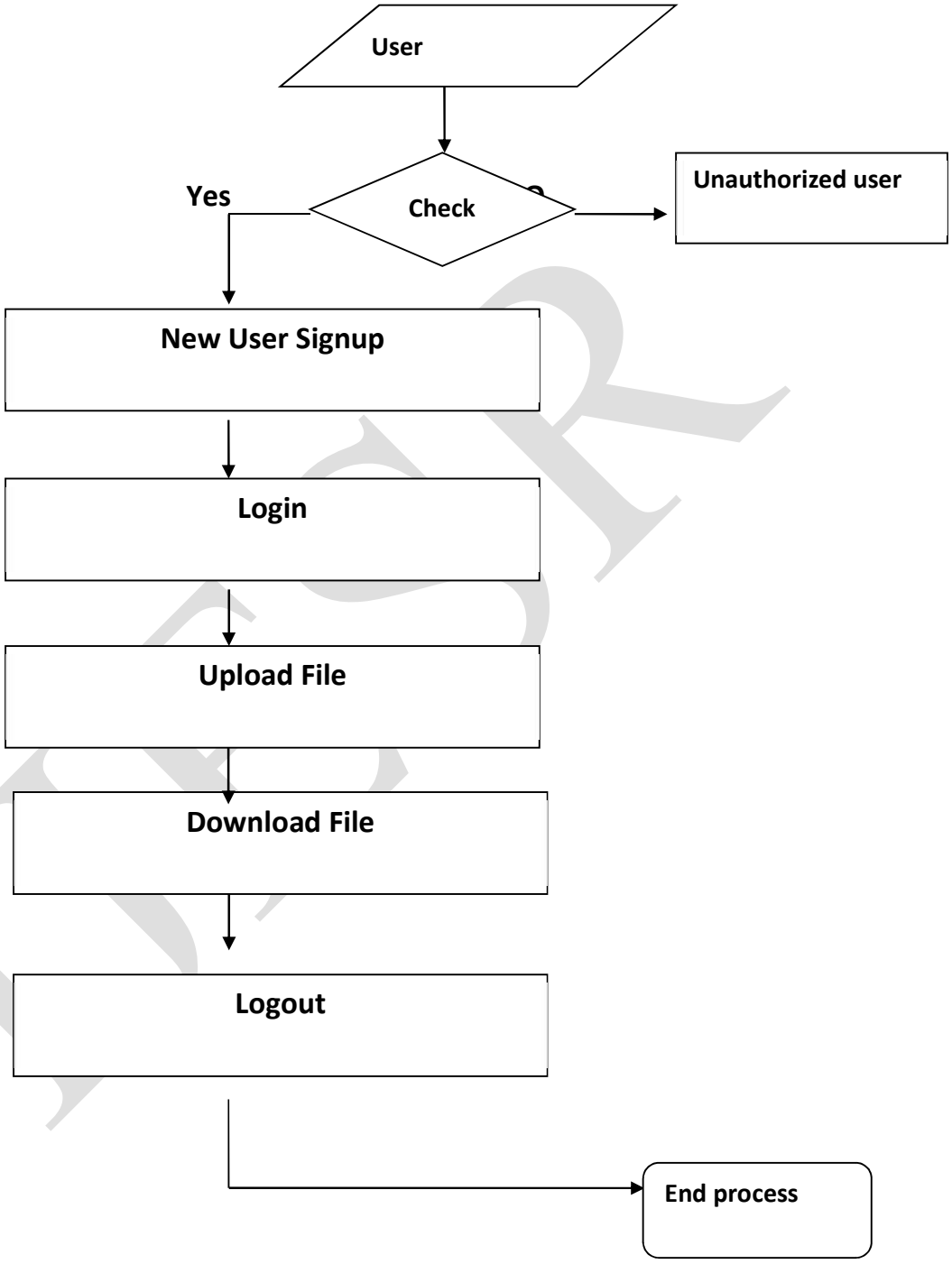
ABSTRACT: Wireless Networks are growing very fast and admiring day by day, due to its ease in setup and economical aspect. Security is major concern in wireless networks. Because of the threats in Wireless Network Systems, there is always risk in breach of network security. This study reveals the intrusion detection systems for wireless networks and various types of threats for them like DoS, Jamming the Network, Junk Transmission, Teardrop, Ping-Of-Death (POD), and Man-inthe-middle. Wireless Intrusion Detection System (WIDS) is a tool used to detect unauthorized access to a network. An IDS usually performs this task in one of the two ways, with either anomaly based detection or signature-based detection. Encryption algorithms play a major role in the information security systems. On the other side, these algorithms put additional CPU load and consume battery fast. This paper provides the evaluation of encryption algorithms like AES, DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms and Blowfish is found to be the best encryption algorithm.

SYSTEM ARCHITECTURE:



DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



SYSTEM TEST

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Test Cases

USER REQUIREMENTS:

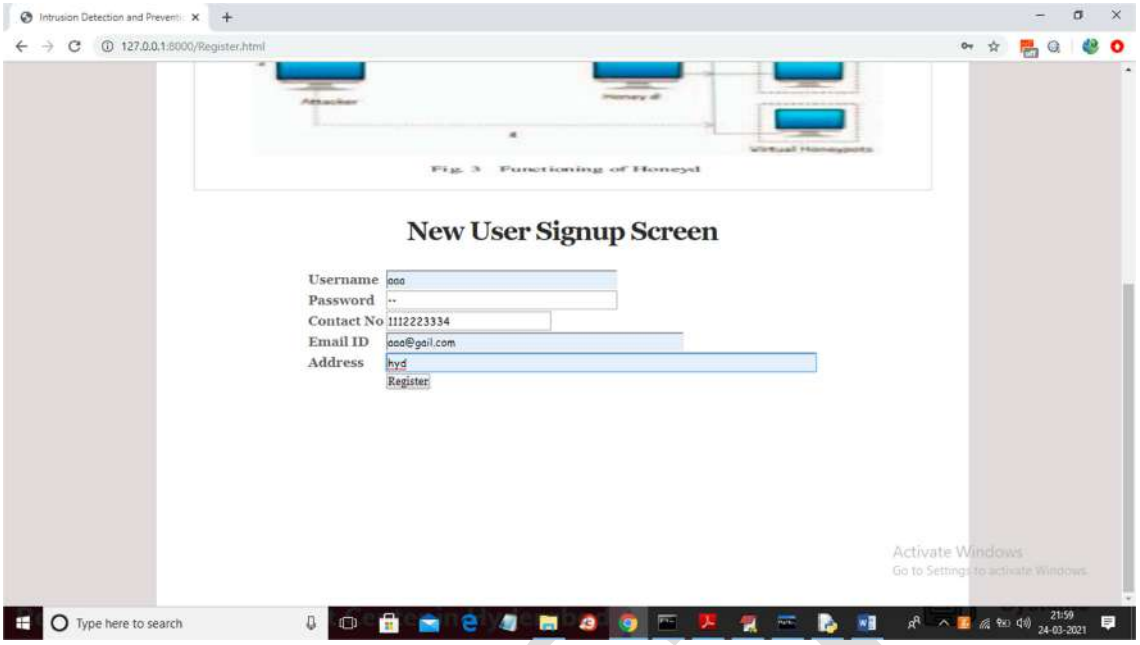
1. Home

Use case ID	Intrusion Detection and Prevention using Honey pot Network for Cloud Security
Use case Name	Home button
Description	Display home page of application
Primary actor	User
Precondition	User must open application
Post condition	Display the Home Page of an application
Frequency of Use case	Many times
Alternative use case	N/A
Use case Diagrams	
Attachments	N/A

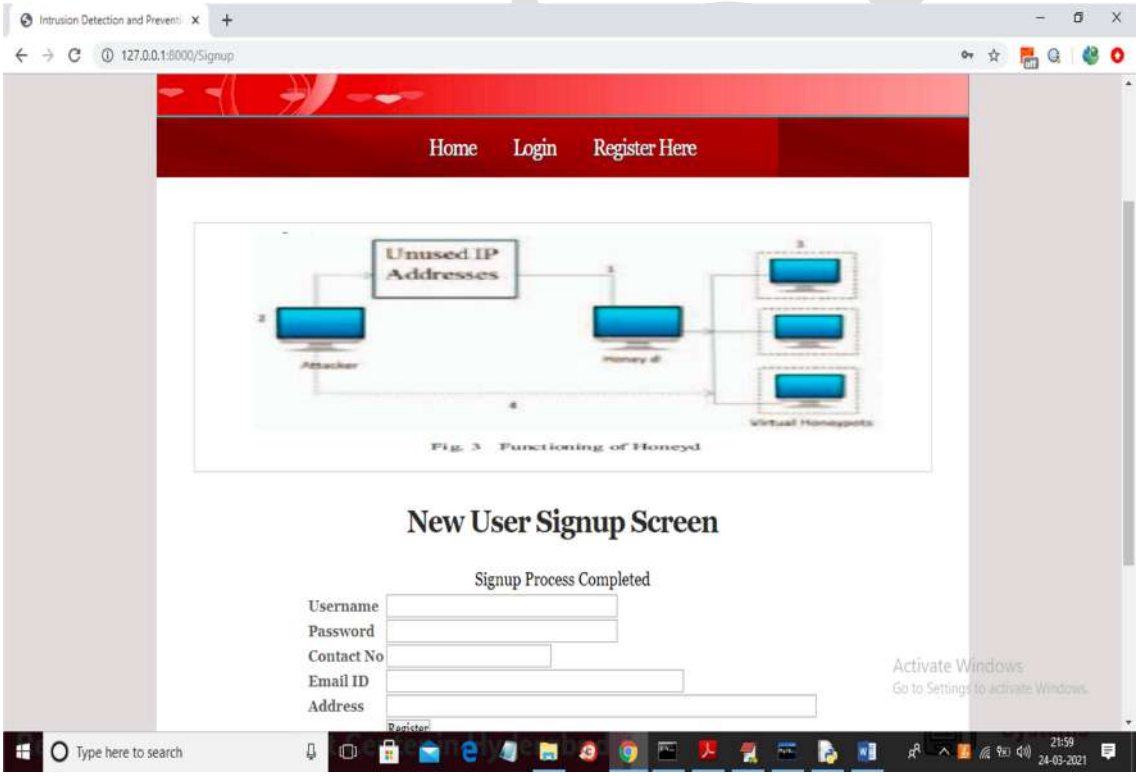
Results

To run project install MYSQL, python 3.7 and DJANGO server and then deploy app on DJANGO and start server and run in browser to get below output.

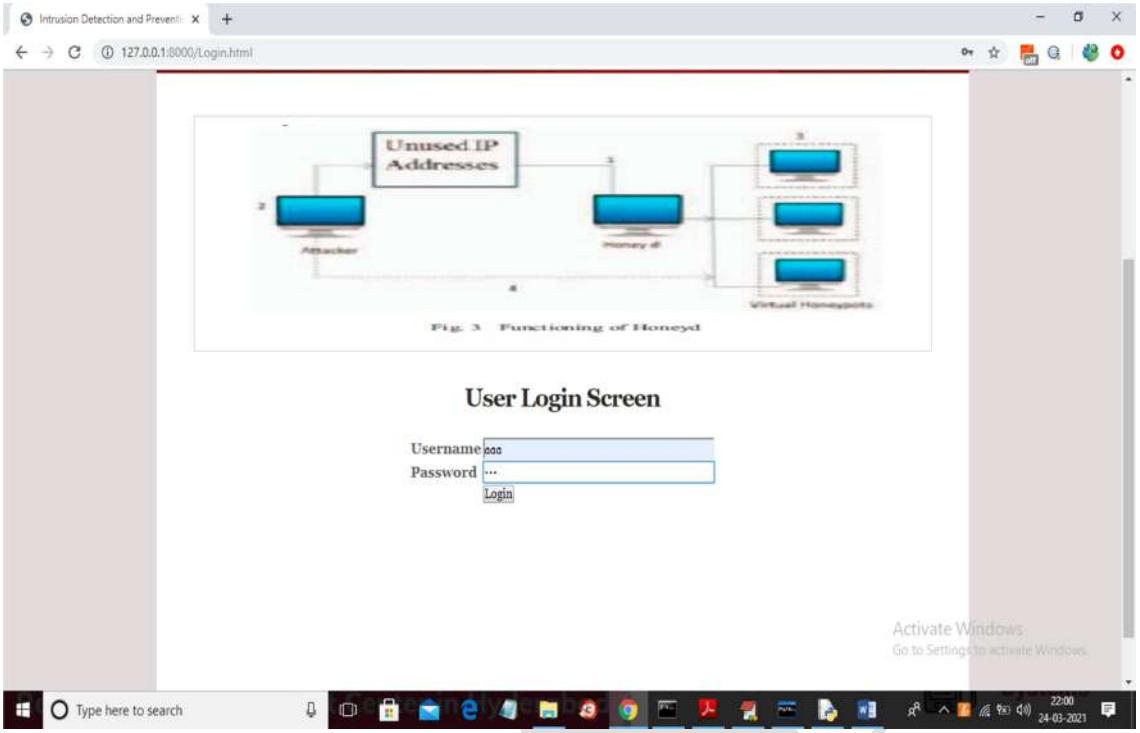
In above screen click on 'Register Here' link and register some users



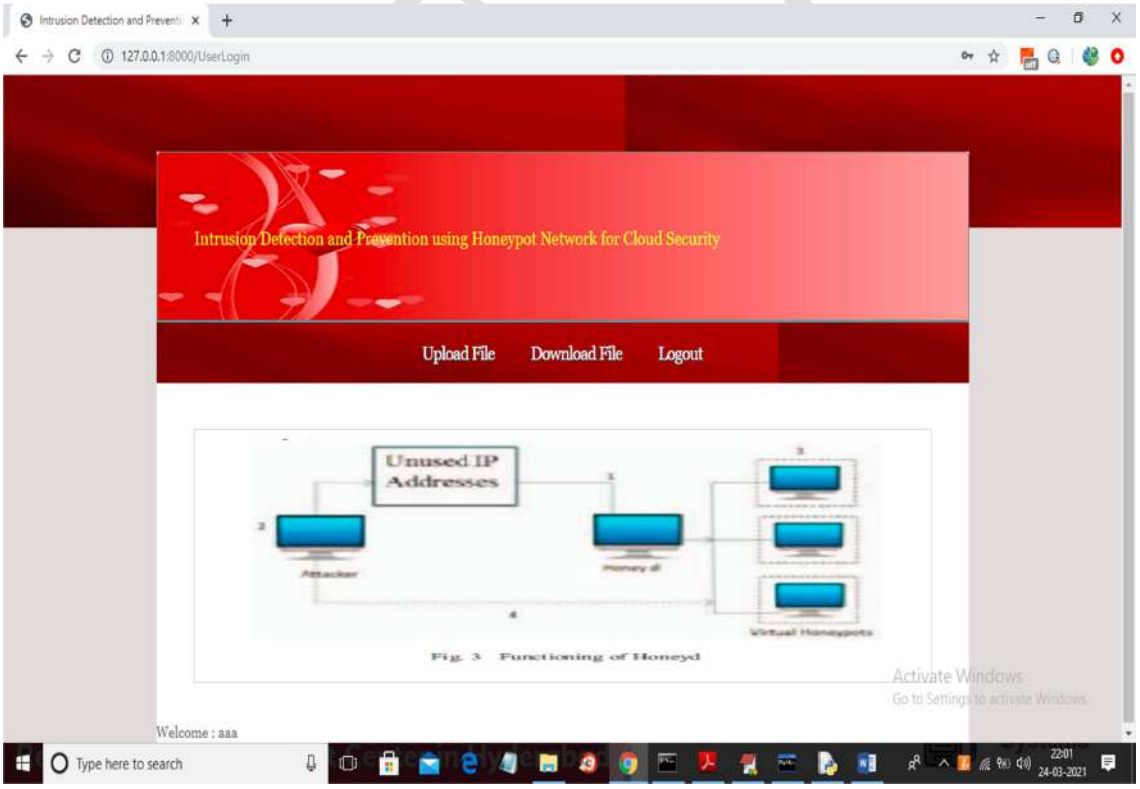
In above screen adding one user and then click on 'Register' button to get below screen



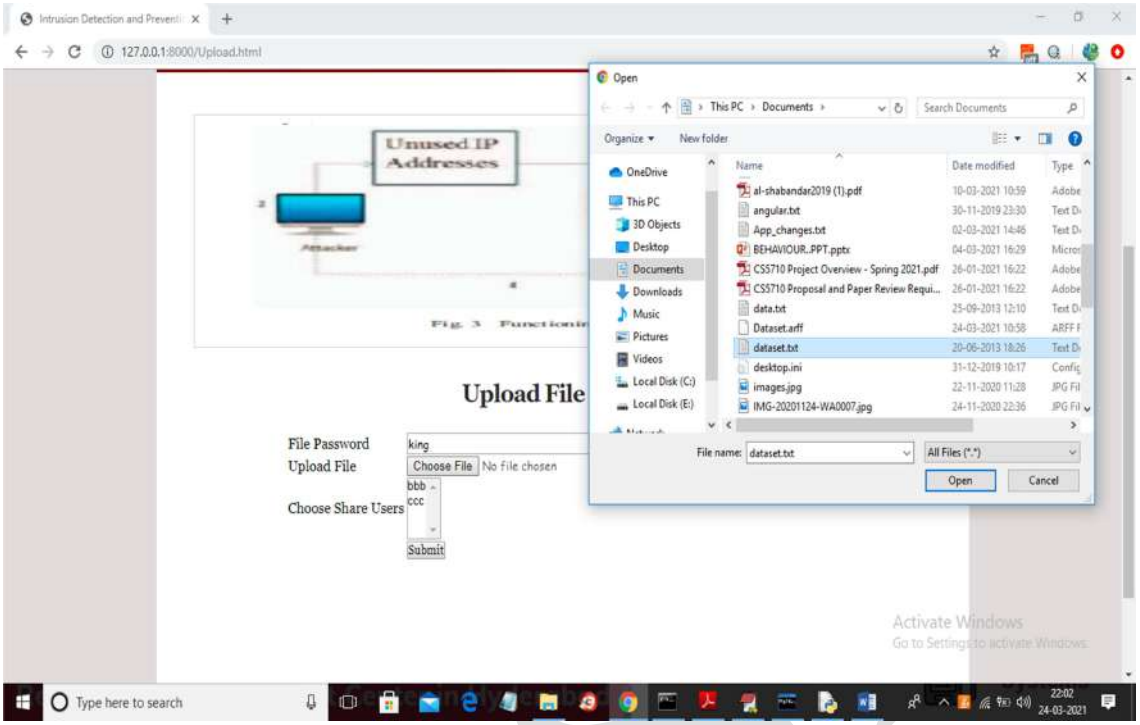
In above screen user signup process completed and similarly you can add many more users and now click on 'Login' link to get below login screen



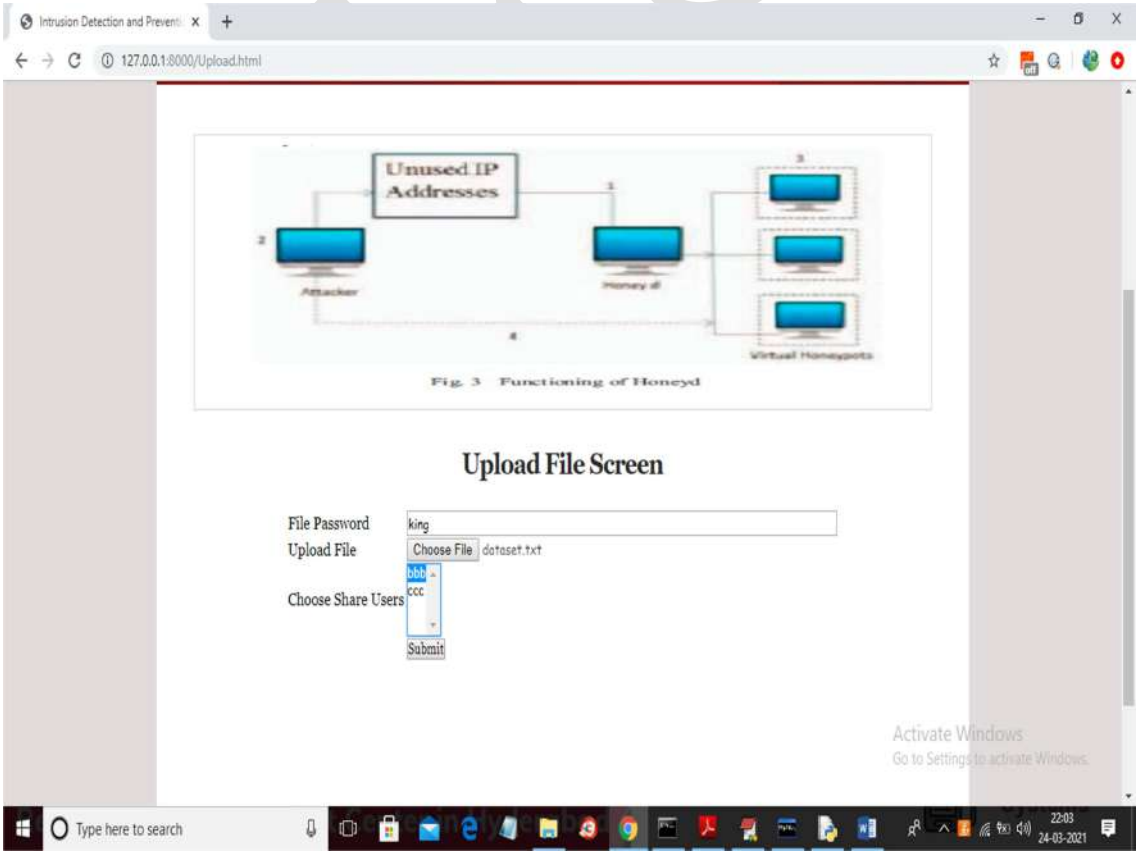
In above screen user ‘aaa’ is logged in and after login will get below screen



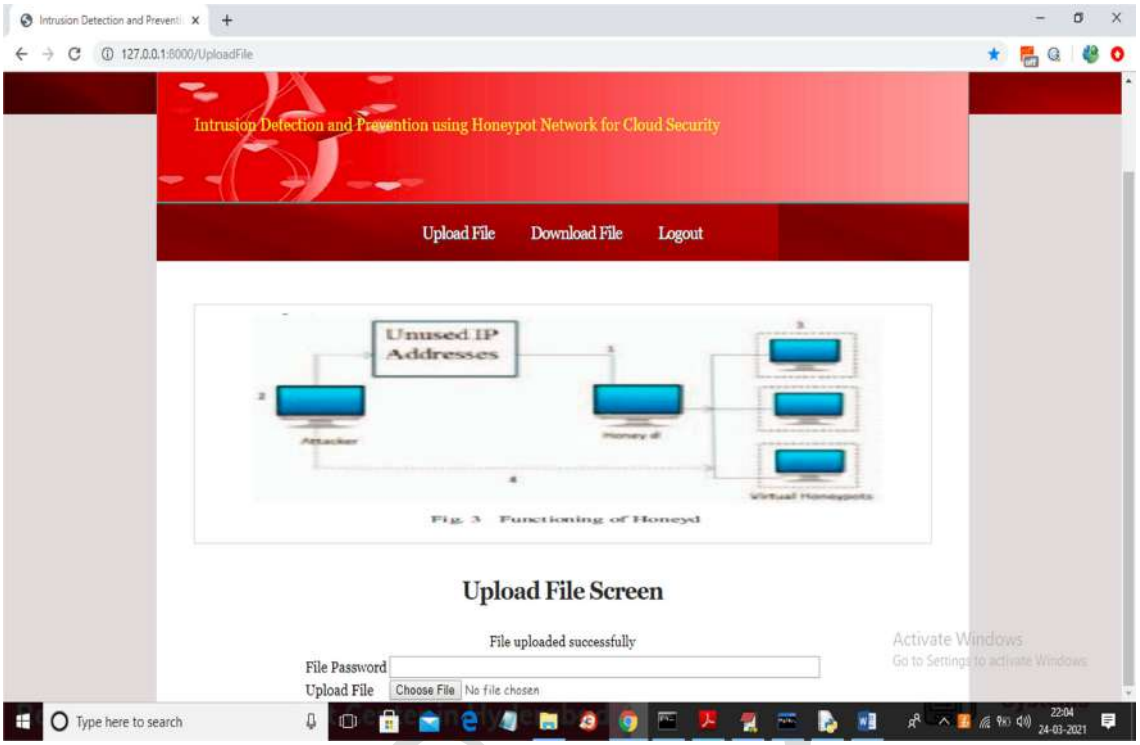
In above screen now user can click on ‘Upload File’ link to upload files



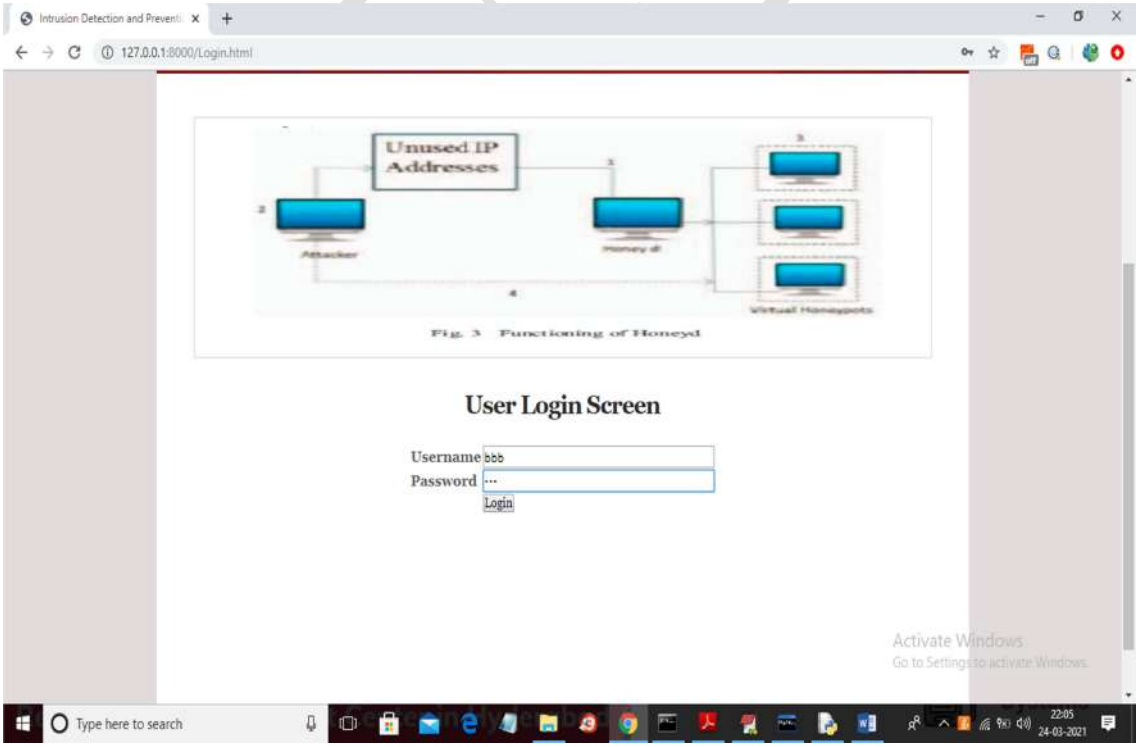
In above screen in first field we need to enter file password and then click on 'Choose File' button to select any file and then select require users with whom you want to share file and you can select multiple users by holding CTRL key from keyboard



In above screen user aaa is sharing file with bbb and now click on 'Submit' button to upload file

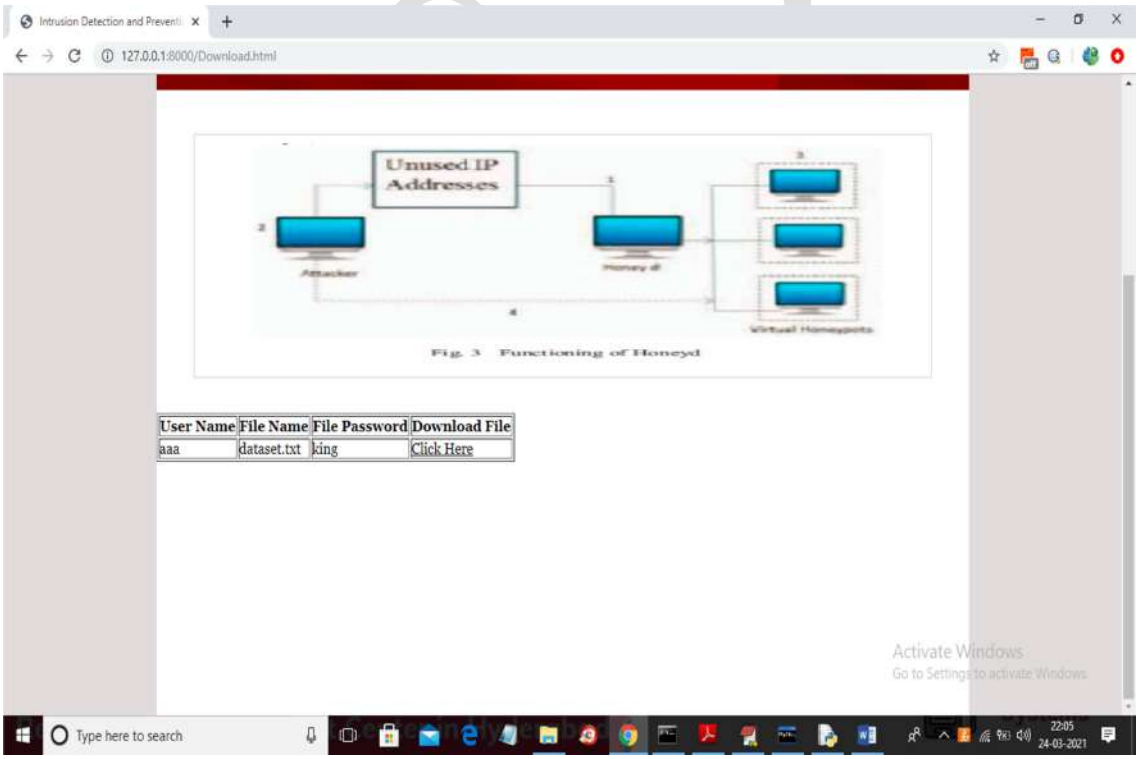


In above screen file is uploaded and now logout and login as user bbb to download file

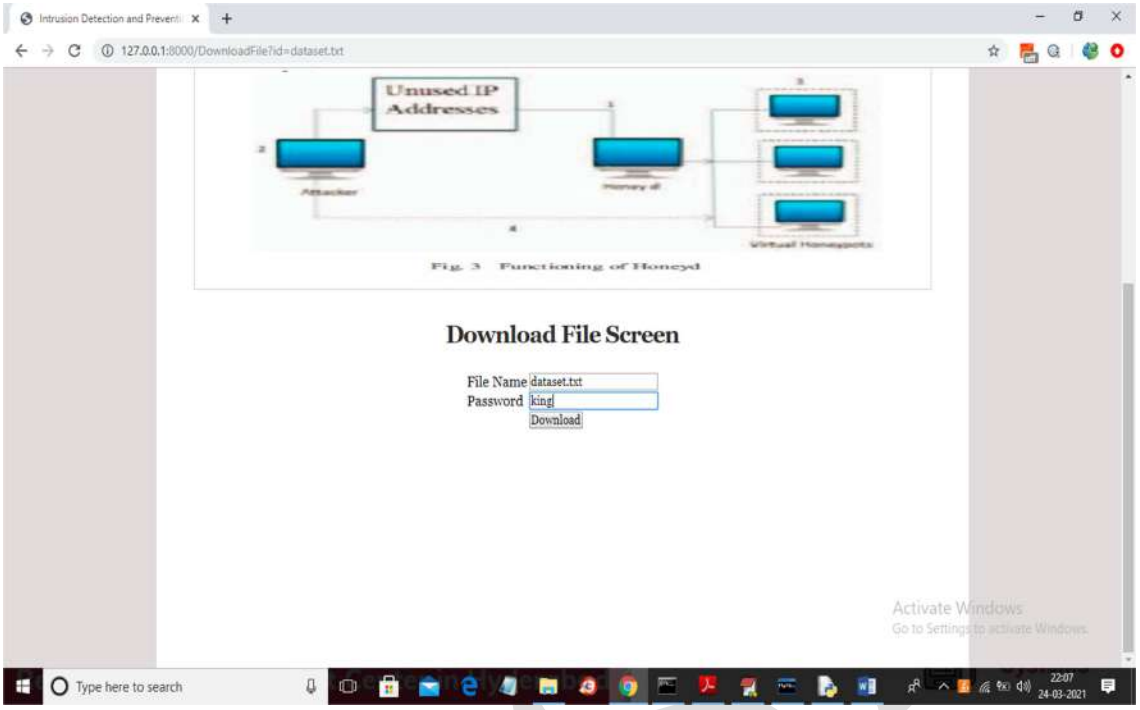


In above screen user bbb is login and after login will get below screen

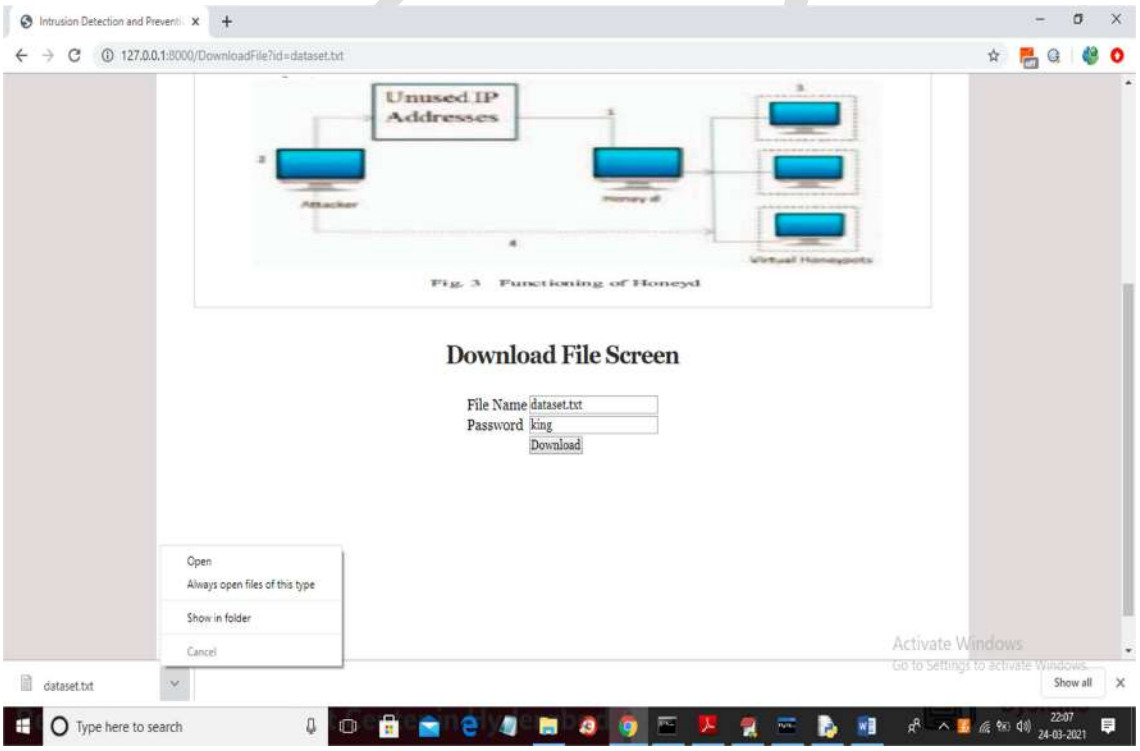
Now click on 'Download File' link to get below screen



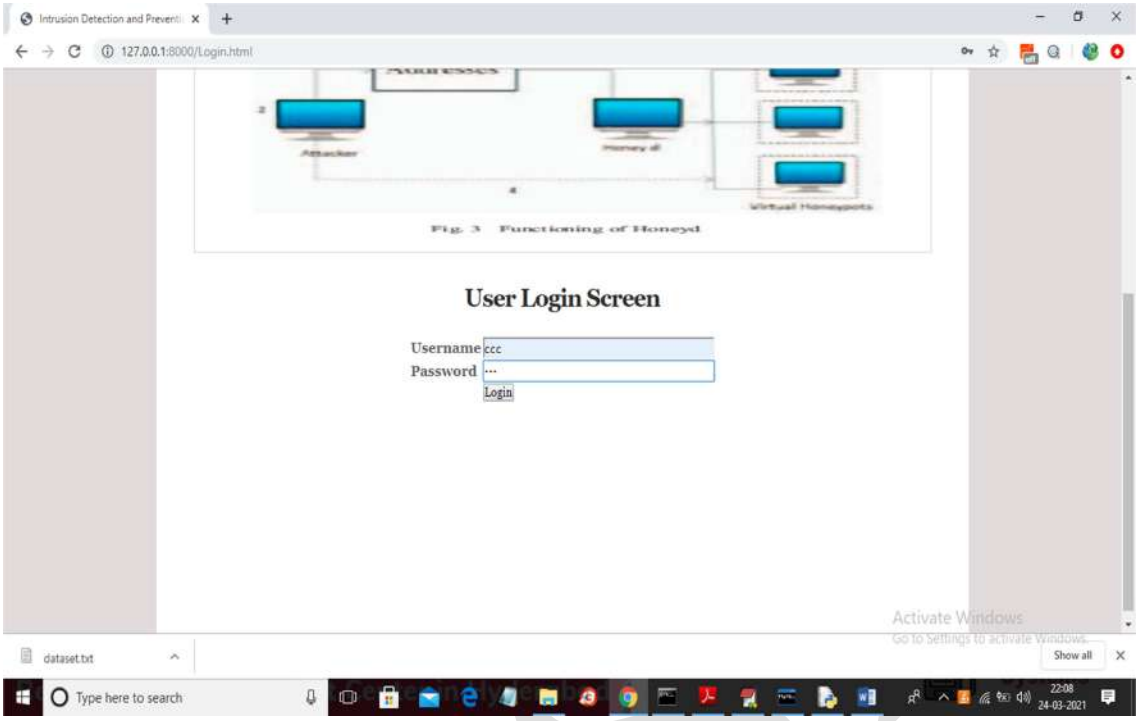
In above screen bbb user can see all files list shared by other user and password of file also will be visible to him as user aaa has given share permission to him. now any time bbb user can click on 'Click Here' link to download file and to get below screen



In above screen user bbb entered password as 'king' and its correct password and file will be downloaded in browser status bar

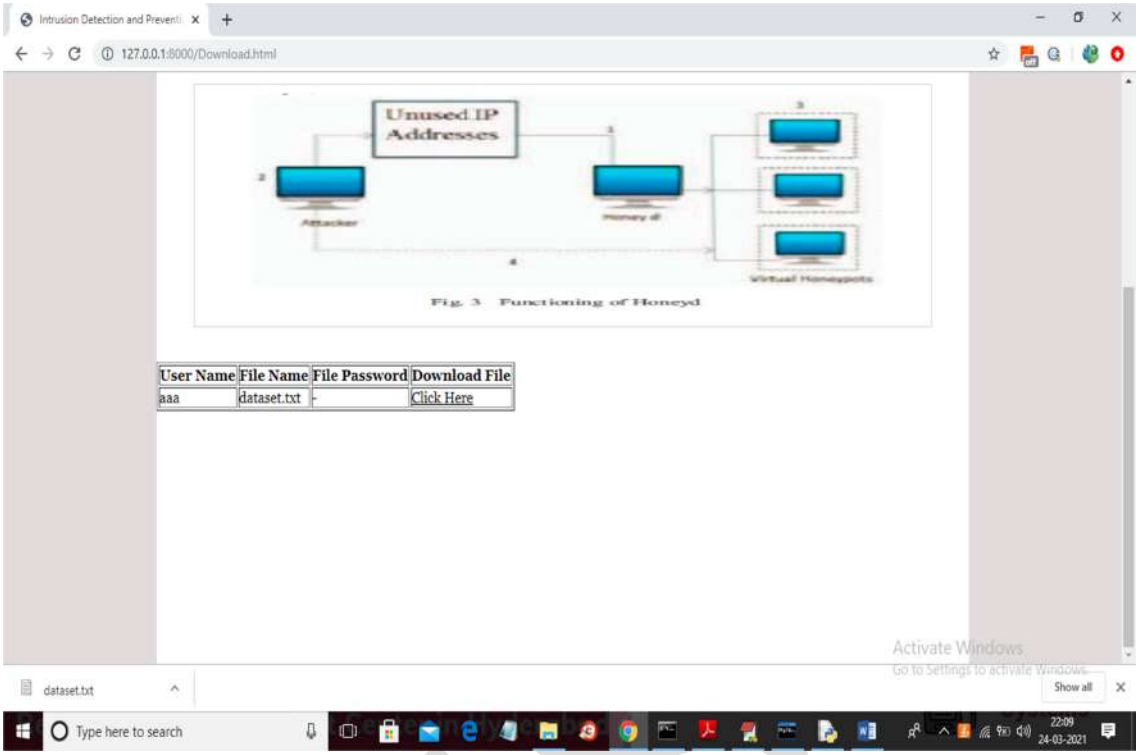


In above screen in status bar file is downloaded and now logout and login as user ccc who don't have share permission

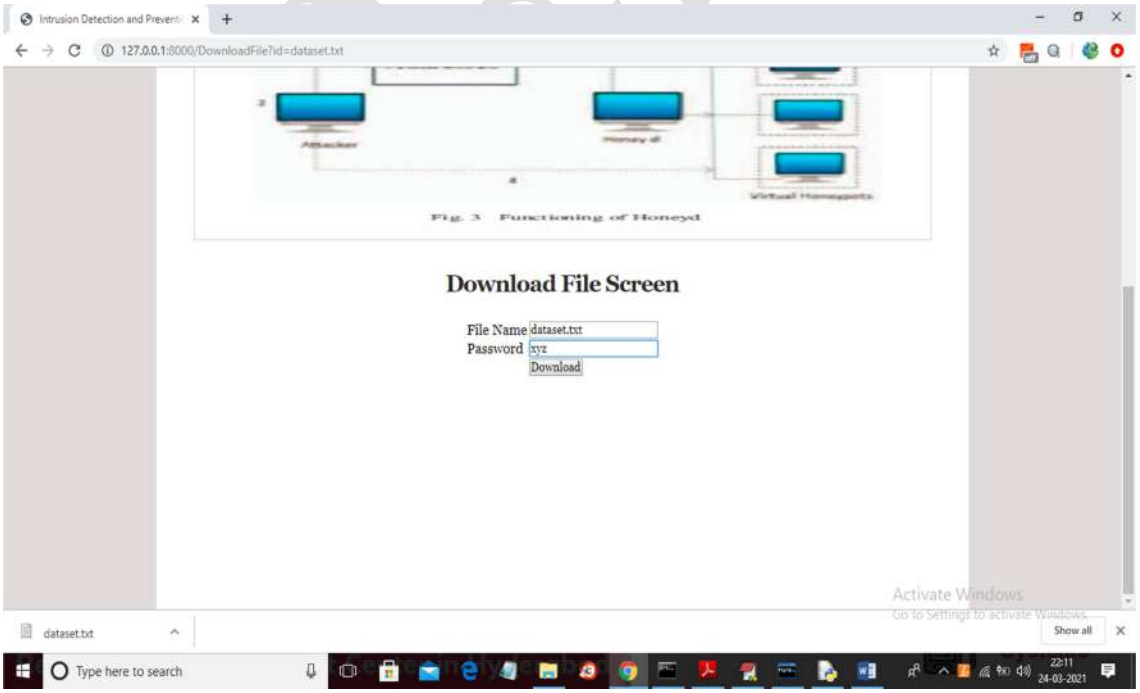


In above screen user ccc is login and after login will get below screen

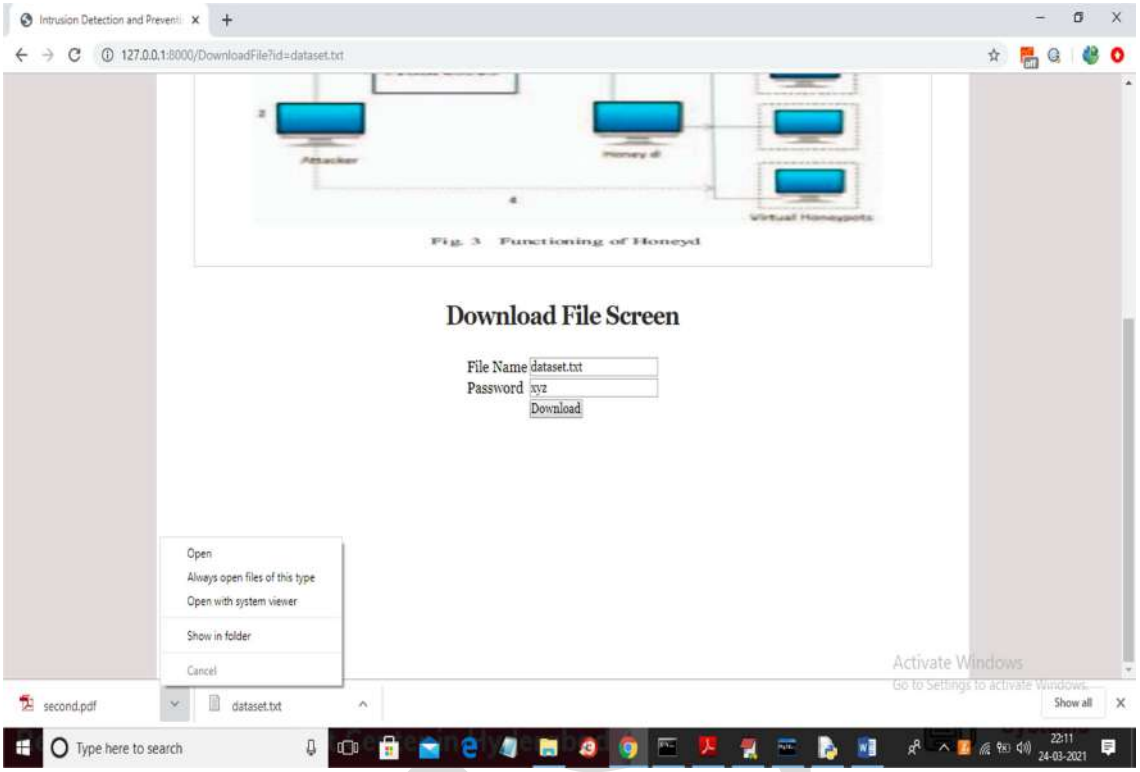
In above screen now user can click on 'Download File' link to get below screen of file list



In above screen ccc user also got file list but he don't have share permission so file password is disabled and now if he want he try to download file with fake password and then Honeypot detect him and serve fake response



In above screen ccc user try to download file with fake password and then will get below response from Honeypot



In above screen in status bar we can see Honeypot serve ccc user fake file called 'second.pdf' instead of original file 'dataset.txt'. In the same way Honeypot serve fake response to gather information from attacker

CONCLUSION

Any Organization or firm with either outside resources/areas or cloud administrations ought to deploy cloud-based Honeypots. The IT staff might be required to arrange the Honeypots, yet the genuine outline ought to be driven by the security groups will's identity observing for vindictive movement. Any association managing delicate information in the cloud must prefer Honeypots, and they will likewise require talented system heads to screen the logs and respond to the information. There are some incredible open source apparatuses that have been created to help with the observing and log gathering of Honeypots. It clearly relies on the cloud stage itself. "The perfect Honeypot for Amazon EC2 will contrast from Microsoft's Azure or IBM's cloud". In some ways, the customary Honeypots are not perfect as they tend to reflect the more conventional desktop and server working frameworks. They are, be that as it may, definitely best conveyed where fitting security experts are likewise checking and breaking down at all circumstances. The supplementary utilization of human collaboration gives that additional layer of security and the expert may distinguish a potential or hurtful assault that had never been seen and henceforth observing programming would have no learning." One of the best bits of best practice counsel is to redo from the get go. Honeypot innovation is open source thus the awful folks will be exceptionally acquainted with default settings and will screen for these early signs of a trap. These systems must be setup in an environment which care about their customers and want an extra edge in security in their cloud based platform.

REFERENCES

1. RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui, "Design of Privacy-Preserving Cloud Storage Framework 2010 Ninth International Conference on Grid and Cloud Computing.
2. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: EarlyDefinition and Experience," 10th IEEE Int. Conference onHigh Performance Computing and Communications, pp. 825- 830, Dalian, China, Sep. 2008
3. Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", InQuality of Service, 2009. 17th International Workshop on, page 19, 2009.
4. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.
5. Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "Cloud security issues" In ServicesComputing, 2009. IEEE International Conference on, page 517520, 2009.
6. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," *Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023
7. Md. Zainlabuddin, "*Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction*", Journal of Sensor, Volume2023.
8. Md. Zainlabuddin, "*Security Enhancement in Data Propagation for Wireless Network*", Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).
9. Dr MD Zainlabuddin, "*CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS*", Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)
10. Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies", Industrial Engineering Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022
11. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
12. Ijteba Sultana, Mohd Abdul Bari and Sanjay," *Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks*", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021
13. M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*", in 3rd International Conference ICCIDM, Springer - 978- 981-10-3874-7_3 Dec (2016)
14. Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017

15. Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022
16. Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7
17. Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.
18. Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.
19. Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10
20. Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.
21. Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.
22. Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017
23. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "*Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering"*, JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;
24. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
25. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021
26. Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
27. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6

28. .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011
29. Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253
30. Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)
31. Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)
32. Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486
33. Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016
34. Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)
35. Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)