JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURITY FRAMEWORK FOR AWS EC2

Kshitij Raj[1], A.S. Pandit[2], Aryan Bahtt [3], Prashik Arun Ate[4]

Department Of E&TC Eng., Smt. Kashibai Navale College of Engineering, SPPU, Pune, Maharashtra

Abstract*— As every service and business is going to cloud for better results. Cloud bring huge changes in the world of IT. AWS is one of the cloud largest cloud providers in the market. Many entertainments and other services are on AWS like Netflix, but this also contain threats as hacker around the world wants to exploit it. In recent times many cloud services got hacked and tons of data sensitive got the leak. So, this framework will help them to secure the cloud and service. It is capable for mitigate the flaws found and list out other underlying threats with its built-in scanner capabilities the system and help the user to stay protected from the threat. This report aims to elaborate and analyse the numerous unresolved issues threatening the Cloud computing adoption and diffusion affecting the various stake holders linked to it.

***Keywords*— Cloud Computing, Virtualization, Network analyser, Python, Bash, Cloud Security**

I. INTRODUCTION

Virtualization has been instrumental in the rapid rise of cloud computing. It involves creating a virtual environment that provides hardware-based services to end-users on personal computers. Server virtualization, storage virtualization, and network virtualization are the three forms of virtualization that have led to the evolution of cloud computing. However, with the growth in on-demand application usage and an ever-expanding user base, security and privacy issues have become more complex and widespread. Cyber-attacks are also becoming more sophisticated, and individual users' online identification information can be used for identity theft. This leads to the critical security risk , which can be harmful as well as data leak. A security framework for AWS EC2 should focus on securing and mitigating instances at the operating system level, as users may leave configuration errors or potential backdoors that can be exploited by attackers. The framework can be developed using Python and native scripting languages of different operating systems, such as PowerShell for Windows and Bash for Linux. Python can detect the instance's OS type and run the appropriate native scripting language to fix any configuration issues and display potential risks after scanning. Additionally, a network analyzer can be used to analyze the network and store its information in logs in a database for further analysis.

II. LITERATURE SURVEY

Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine." ICCSN '10 Proceeding of the 2010 Second International Conference on Communicatior Software and networks. IFEE Computer Society, USA. 2010 . Innovation is necessary to ride the inevitable tide of change. The buzzword of 2009 seems to be "cloud computing" which is a futuristic platform to provides dynamic resource pools, virtualization, and high availability and enables the sharing, selection and aggregation of geographically distributed heterogeneous resources for solving large-scale problems in science and engineering. But with this ever developing cloud concept, problems are arising from this ¿golden solution¿ in the enterprise arena. Preventing intruders from attacking the cloud infrastructure is the only realistic thing the staff, management and planners can foresee. [1]

Shilpi Mishra,Dr. Manish Kumar, Niharika Singh, Stuti Diwedi “A Survey on AWS Cloud Computing Security Challenges & Solutions” 2022 A better knowledge of cloud computing's security problems has been shown and the techniques and solutions which have been used by the cloud service sector have been highlighted in this article. The objective of this report is to shed light on immerging cloud services market and the different upcoming challenges like network issues. [2]

Beaulah A Navamani, Chuan Yue, and Xiaobo Zhou "An Analysis of Open Ports and Port Pairs in EC2 Instances 2017" Security communities, reports and surveys often state that port scans can be considered as precursors to an attack. In this paper, we performed an analysis pinpointing the risks of open ports in a cloud environment.[3]

Hanqian Wu Li Yao, Yi Ding, Chuck Winer, Li Yao Network "Security for Virtual Machine in Cloud Computing" 2010 In this paper, we focus on the security of virtual network in virtualized environment. First, we outline the security issues in virtual machines, and then security problems that exist in a virtual network are discussed and analyzed based on Xen platform.[4]

S. Narula, A. Jain and Prachi, "Cloud Computing Security: Amazon Web Service," 2015 Fifth International Conference on Advanced Computing & Communication Technologies . In this paper Secure Network Architecture is attained by the network devices such as firewall which manages and controls the boundary of network. Traffic flow policies, access control list (ACL), is generated to control the flow of informational is approved by Amazon Information Security. Secure Access Point indicates that AWS has limited number of access points so as to perform proper monitoring of communication. The access points of customers are called API endpoints. [5]

A. Ochani and N. Dongre, "Security issues in cloud computing," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) . In this paper the major concern on the number of user who store their personal information on cloud therefore service provider has to provide strong security by providing third party to prevent unauthorized access [6]

III. METHODOLOGY

The Security Framework for AWS EC2 is designed to identify potential issues within the operating system. Python is used to determine the type of OS on the instance and subsequently runs a native scripting language to rectify any identified issues or missing configurations.

In addition to the OS analysis, the project also includes a network analyzer. This analyzer scans the network and logs its findings in a database for further analysis. This database can be used by SOC to learn more about previous attacks or predict potential future attacks. The scripts used by the network analyzer will also scan for potential risks and threats, attempt to mitigate them, and check for brute force logins to the MySQL database.

In summary, this Security Framework for AWS EC2 uses Python to detect and resolve issues within the operating system, as well as a network analyzer to log and analyze network data for future threat detection and prevention.

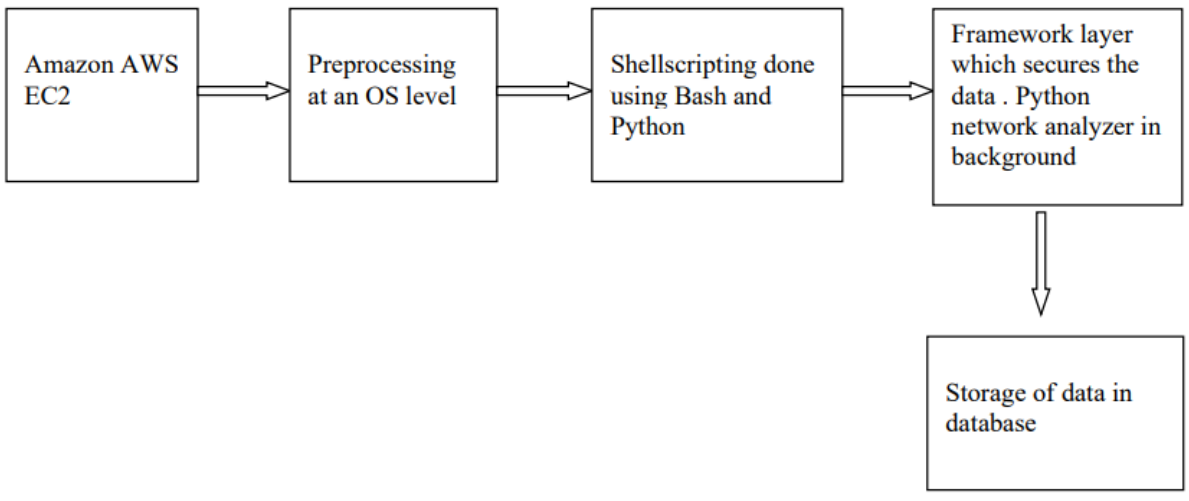

Fig.1 Block Diagram of the AWS EC2

Virtual Machine

This section is a virtual machine on which a cloud service provider provides service to the users all over the world whether it could be any computing services such as computing services, abstraction, network architecting etc. As cloud computing involves virtualization, the need of user authentication and control across the clouds is high. The existing solutions are not able to handle the case of multiple clouds. As multiple users' data are stored by a single hypervisor, specific segmentation measures are needed to overcome the potential weakness and flaws in hypervisor platform.

Pre-processing

Pre- processing is part where an initial python script is going to scan the OS for determining the type of OS distribution such as Windows and Linux, then it will execute the native script for the further scanning.

Usually shells are interactive that mean, they accept command as input from users and execute them. However some time we want to execute a bunch of commands routinely, so we have type in all commands each time in terminal.
As shell can also take commands as input from file, we can write these commands in a file and can execute them in shell to avoid this repetitive work. These files are called Shell Scripts or Shell Programs. Shell scripts are similar to the batch file in MS-DOS and PowerShell script. Each shell script is saved with **.**sh file extension e.g., myscript.sh where the batch and PowerShell are saved with extension of .bat and .ps1

A shell script has syntax just like any other programming language. If you have any prior experience with any programming language like Python, C/C++ etc. it would be very easy to get started with it.

A shell script comprises following elements –

Shell Keywords – if, else, break etc.
Shell commands – cd, ls, echo, pwd, touch etc. Functions
Control flow – if. then. else, case and shell loops etc.

Framework layer which secures the data and Network Analyser

After Pre-processing, scripting will analyse the potential threat, scan for any mis configuration in the system, check for brute forcing of databases and suggest possible mitigations. In this framework we added a network analyser and native scripting languages to scan and fix so level issue with better overview and grasp. A network analyser which will run actively in background and store all the information a database for further analysis, this analyser is developed with python and using mongo db. for storing the data

Storage of data on the cloud

The framework layer will store the network database on the cloud and will be preserved for further usage by the user and will have all the flaws fixed without any hassles the user will get a secure and user attractive interface which could be used by any organization a network security in their database or in a data warehouse

IV. EXPERIMENTATION

Our model is divided into two parts, firstly detecting the operating system which operating system it is running windows or Linux using python script. Then it will call the native so scripting language like PowerShell or bash script. It will tweak configurations and OS level settings also allow to list about possible threats and issue through its inbuilt scanner. The second part is of network analyser which will run in background and store in database for further analysis

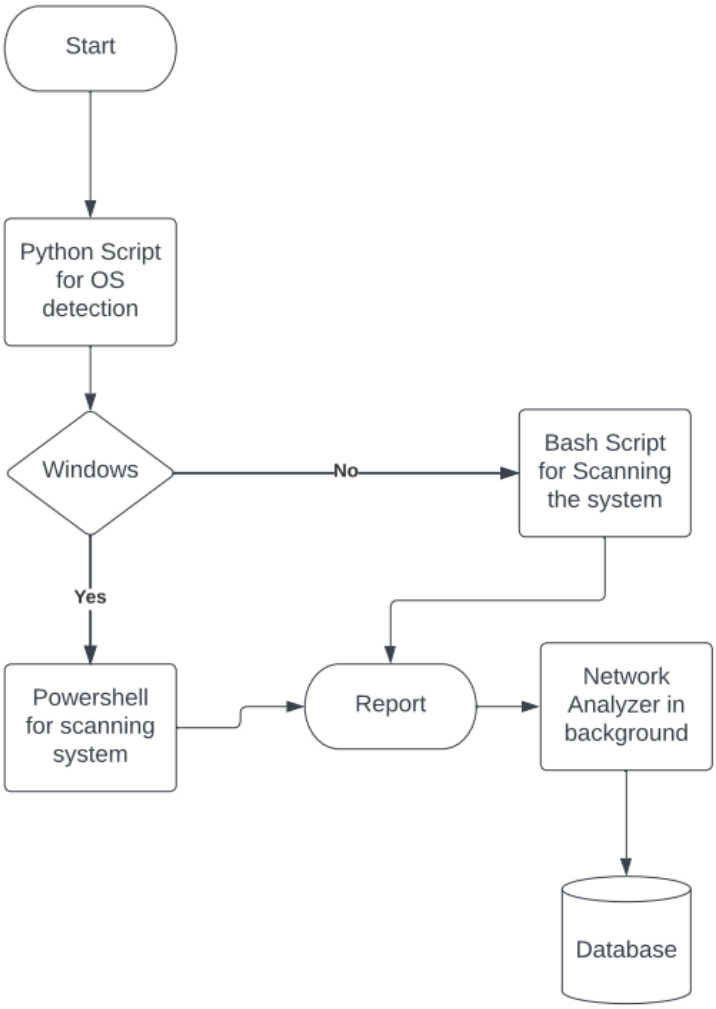

Fig.2 Flowchart of overall system

It will scan the scan the whole operating system and check for flaws and other vulnerability which damage the security of the system and mitigate the flaws of the system fix and alert according to scan, and also check for brute force login attempt in MySQL and also analyses network in background using inbuilt feature for network scanning and storing data in mongo dB for further analysis. Important Parameters to be checked Detection of OS. Script executes according to the native OS also checks for firewall and save all the rules. Checks for suspicious process and backdoor files. Leaked cloud credentials. MySQL brute force and no pass login. Display all routes and IP in hosts. Network analyser store data of the network in background. Our model is divided into two parts, firstly detecting the operating system on which its server is running and second part is about the network analyser which will analyse network. After that it will store data in the database for further analysis by the server admin.

V. RESULTS AND DISCUSSION

After the scanning is finished the script will detect the system operating system and the under lying system using built in libraries or command specific to the programming language or operating system.

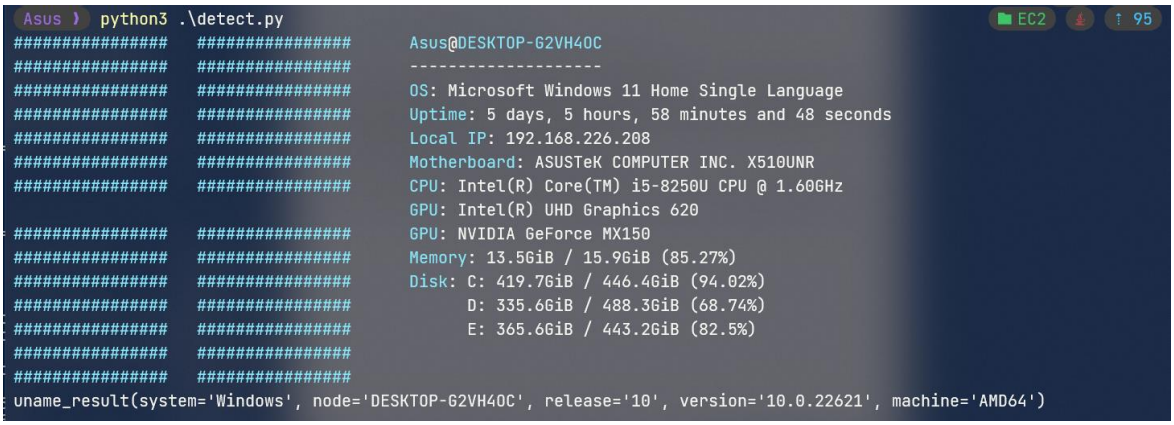

Fig.3 Python script OS detection

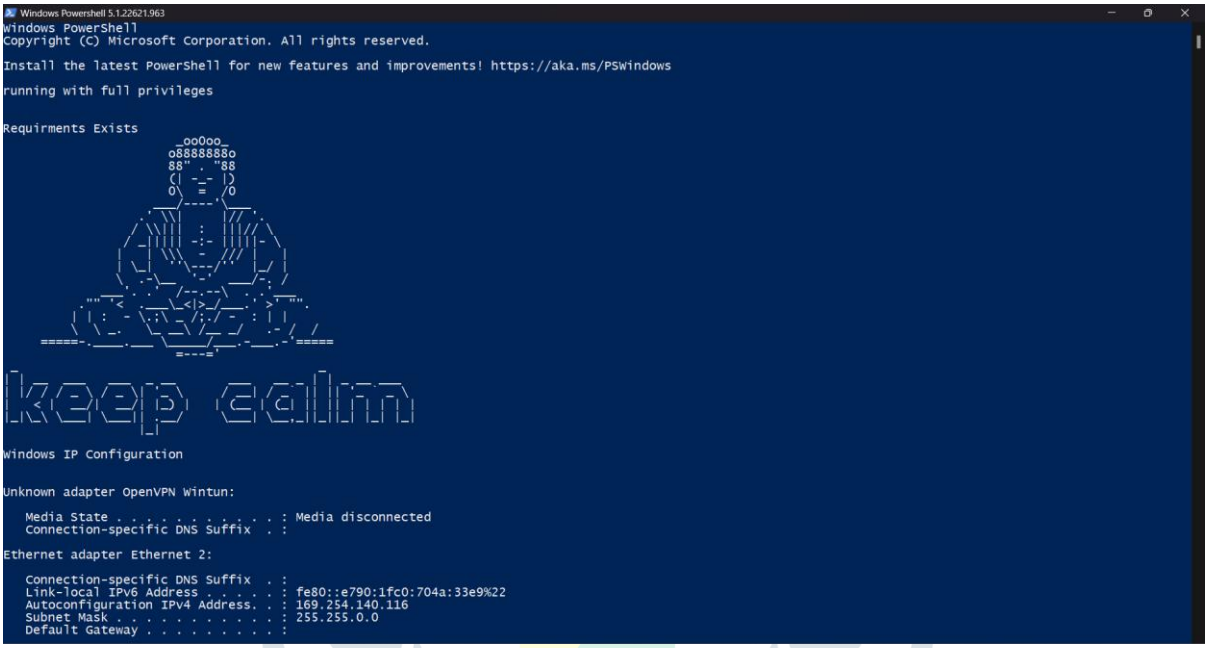

Fig.4 PowerShell Script

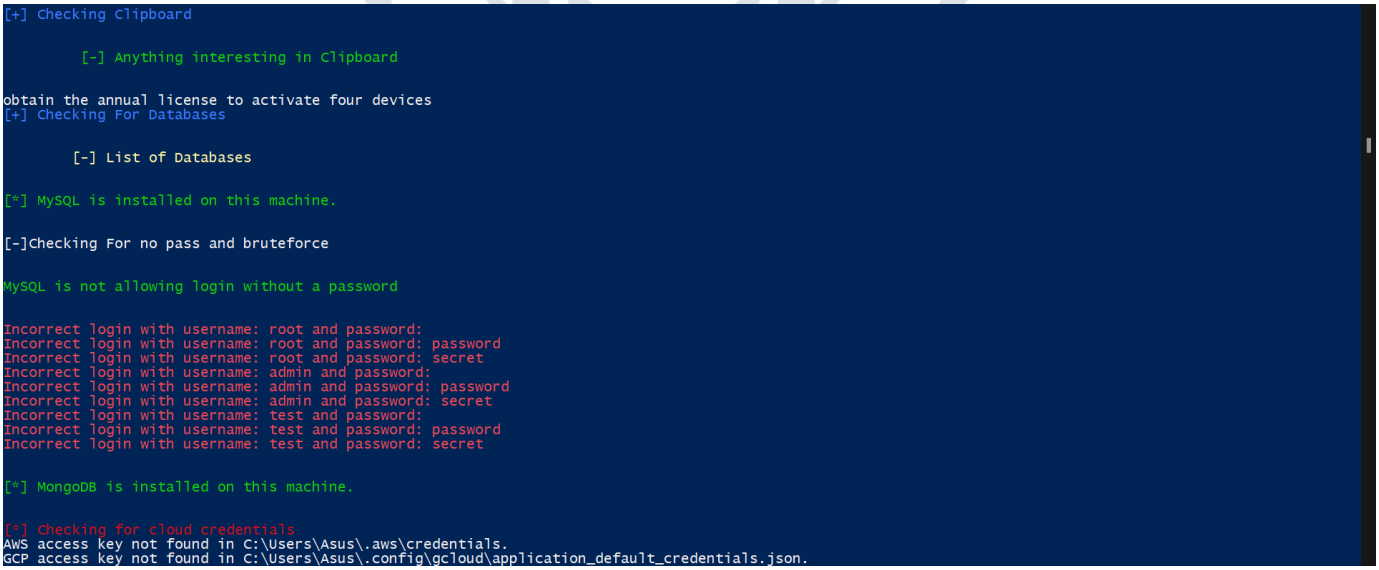

Fig.5 Checking sensitive information

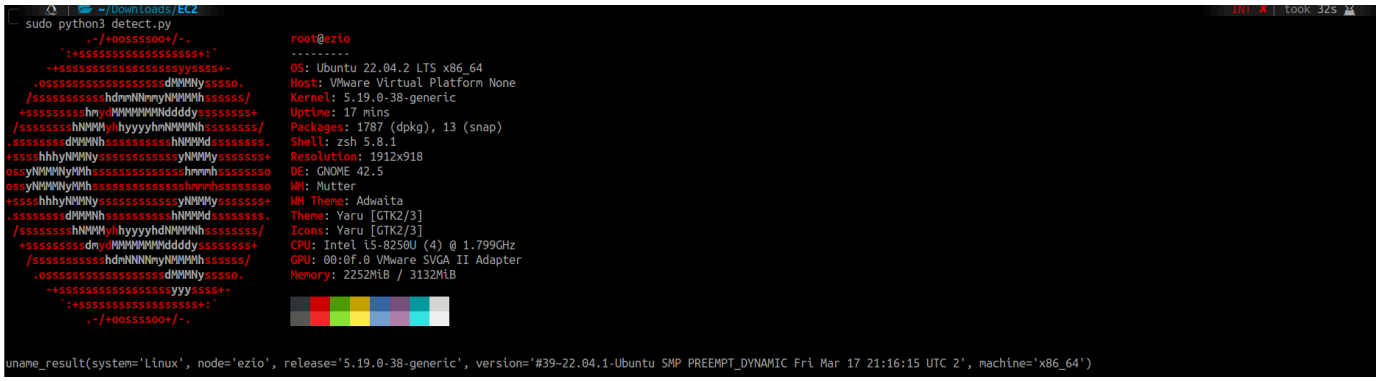

Fig.6 Detected Linux

Fig.7 Bash Script

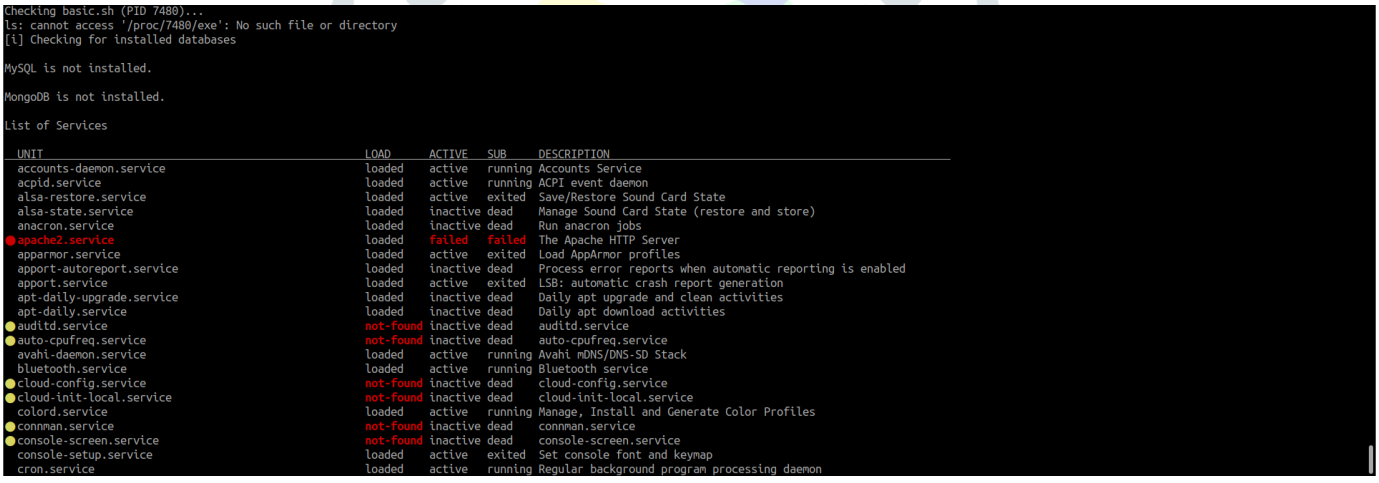

Fig.8 List of services

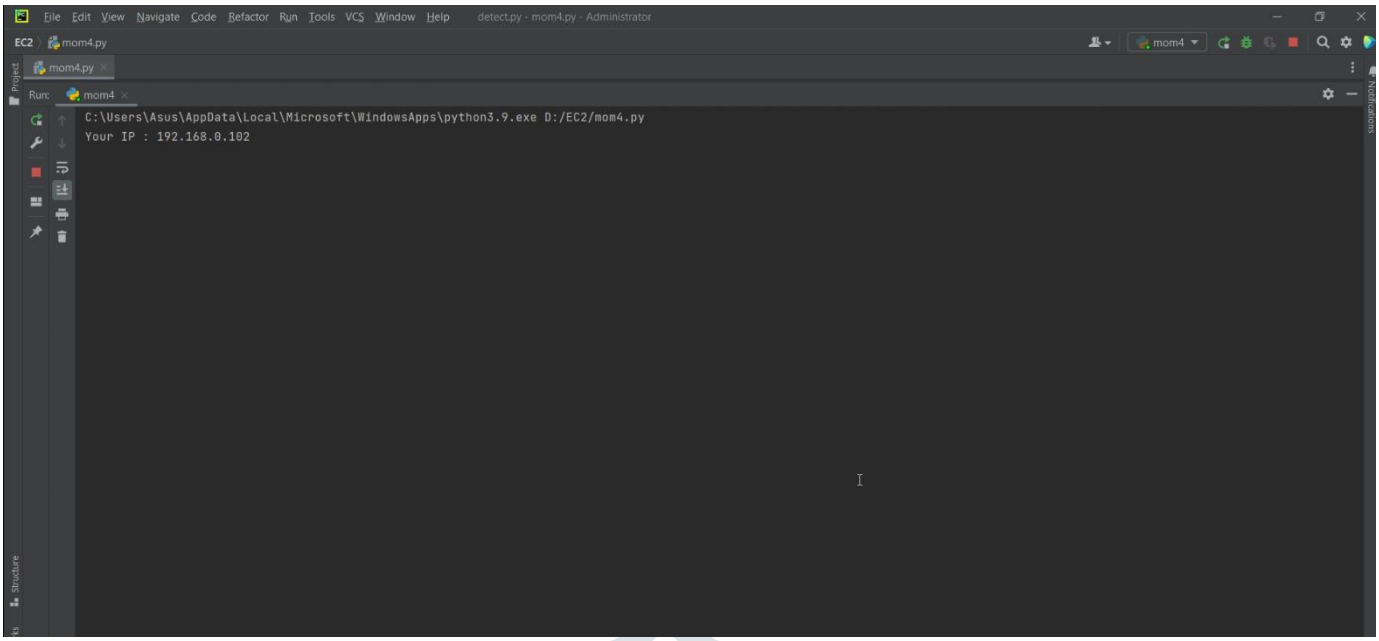

Fig.9 Network Analyzer

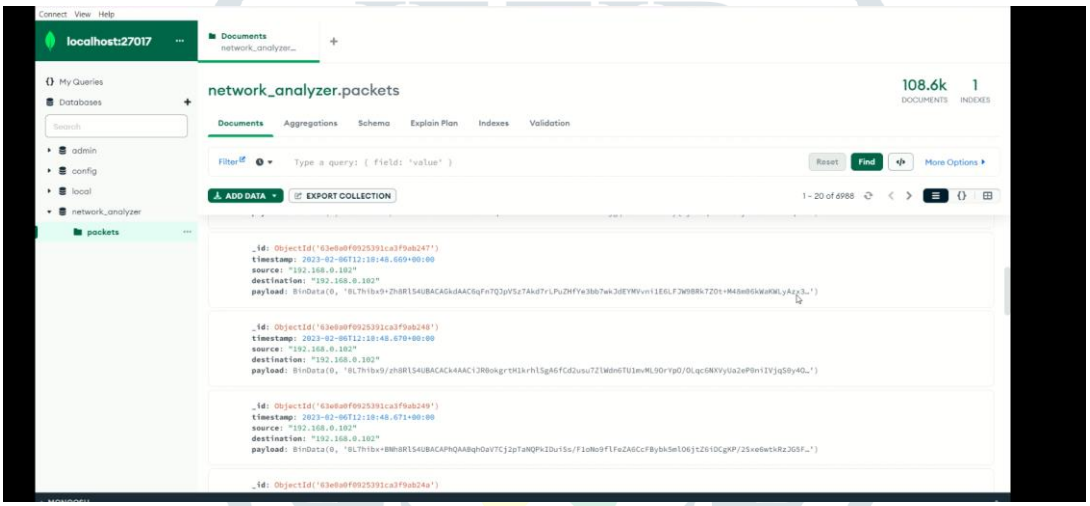

Fig.10 Mongo db stored data

VI. CONCLUSIONS AND FUTURE SCOPE

Cloud Computing, envisioned as the next generation architecture of its enterprise is a talk of the town these days. Although it has revolutionized the computing world, it is prone to manifold security threats varying from network level threats to application-level threats. in order to keep the cloud secure, these security threats need to be controlled. moreover data residing in the cloud is also prone to a number of threats and various issues like confidentiality and integrity of data should be considered while buying storage services from a cloud service provider. auditing of the cloud at regular intervals needs to be done to safeguard the cloud against external threats . In addition to this, cloud service providers must ensure that all the SLAs are met and human errors on their part should be minimized, enabling smooth functioning. in this paper various security concerns for cloud computing environment from multiple perspective and the solutions to prevent them have been presented compared and classified. it will help to secure the EC2 for threats and attacks from the network side, securing the deployed services and EC2 on the platform, minimize the attack vector for the system in the future work, method may be implemented as a simulation of the framework for the use of end users or the developers which will be developing or deploying the applications without worrying about the hackers or network attackers.

ACKNOWLEDGMENT

Efforts and perspiration alone do not contribute to the success of any project. As we have realized the importance of human factor in any constructive efforts, many people apart from project team members contributed essentially to the project's success. We wish to thank Mr. Sahil Gaikwad, (Director & Founder, Secure Era Pvt. Ltd.) and all researcher's and authors for sharing their valuable work in our cyber community. We take this opportunity to express our special thanks to all the professors of our department for their valuable guidance. Last but not the least; we would like to thank our parents for being constant source of inspiration and all our friends who have helped us directly or indirectly.

REFERENCES

[1] A. Bakshi and Y. B. Dujodwala, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," *2010 Second International Conference on Communication Software and Networks*, Singapore, 2010, pp. 260-264, doi: 10.1109/ICCSN.2010.56.

[2] Mishra, Shilpi & Kumar, Manish & Singh, Niharika & Dwivedi, Stuti. (2022). A Survey on AWS Cloud Computing Security Challenges & Solutions. 614-617. 10.1109/ICICCS53718.2022.9788254.

[3] B. A. Navamani, C. Yue and X. Zhou, "An Analysis of Open Ports and Port Pairs in EC2 Instances," 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honololu, HI, USA, 2017, pp. 790-793, doi: 10.1109/CLOUD.2017.116.

[4] Hanqian Wu, Yi Ding, C. Winer and Li Yao, "Network security for virtual machine in cloud computing," 5th International Conference on Computer Sciences and Convergence Information Technology, Seoul, 2010, pp. 18-21, doi: 10.1109/ICCIT.2010.5711022.

[5] S. Narula, A. Jain and Prachi, "Cloud Computing Security: Amazon Web Service," 2015 Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, India, 2015, pp. 501-505, doi: 10.1109/ACCT.2015.20.

[6] A. Ochani and N. Dongre, "Security issues in cloud computing," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 783-787, doi: 10.1109/I-SMAC.2017.8058286.

[7] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource allocation for security services in mobile cloud computing," in Proc. IEEE INFOCOM'11, Machine-to-Machine Communications and Networking (M2MCN), pp. 191-195, April 10-15, 2011, Shanghai, China.

[8] Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011

[9] Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu, "SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environment," Sixth International Conference on Natural Computation, ICNC 2010, pp. 2935-2939, IEEE, Yantai, Shandong, China, 2010. ISBN: 978-1-4244-5958-2.

[10] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.