Intrusion Detection and Prevention using Honeypot Network for Cloud Security

[1] AMIT SHUKLA, [2] Dr. NITA YADAV, HOD

[1, 2] Department of CSE, HBTU KANPUR, [1] AMITSHUKLA.12J@GMAIL.COM

Abstract: As the number of users grows quickly, so do problems with hardware failure, web hosting, and the allocation of space and memory for data. These problems are causing data loss, either directly or indirectly. We use cloud computing to provide services that are dependable, quick, and inexpensive. As this technology becomes better and better, it becomes more and more likely that bad people will be able to get beyond its protection. Honeypot is a mechanism to keep bad traffic from getting to systems. It is a huge plan that has made systems safer in certain ways. When installing Honeypot onto the servers of third-party cloud vendors, one can consider numerous legal challenges. Thus, the concept of Honeypot is applied to a file-sharing software that is rendered on a cloud server. This paper discusses the process of identifying threats in a cloud-based environment and the process of using Honey pot to defend it and implies how the two can be accomplished in an innovative way.

Index terms *– Detection, Honeypot, Cloud Computing, Honeyd, Honeynets, Cloud IDS*

1. INTRODUCTION

Mobile data traffic is exponentially increasing as more people are using smart phones and tablets; this has seen more applications being developed to support mobile operators. This has compelled the mobile networks to go under massive restructuring to meet the new demand. The analysis and projections indicate that beyond 2020, the mobile networks will be required to support traffic rates that are over a thousand times more than the current rates [1]. This growth comes with everything bundled like the need of additional capacity, need of higher data speeds, and larger numbers of connected devices. As well as, topics, such as, energy efficiency, system cost, latency, spectrum availability, and spectral efficiency, also play a role in terms of changes in radio access network over time [1]. The possible solution to these issues is the so-called Cloud Radio access network (C-RAN) or centralized RAN. This network transforms the method by which ordinary RANs are constructed. A comprehensive processing of baseband processing is performed in C-RAN by a so-called Background Unit (BBU), whereas sending and receiving of radio signals is left to so-called remote Radio units (RRUs) [2], [3]. The BBUs and the RRUs are related through fronthaul community and hence, they discover it simpler to change information. "In-section and Quadrature (IQ)" samples among the BBU and RRU are standardly packaged in the "not unusualplace Public Radio Interface (CPRI) and the Open Base Station structure Initiative (OBSAI)" [6], [7]. These requirements permit the electricity to be managed dynamically and this means that BBUs may be switched off or switched on primarily based totally on visitors load at some stage in the day [7]. C-RAN has some of benefits, inclusive of being greater

energy-efficient, safer, and capable of use state-of-the-art interference control strategies like "Coordinated MultiPoint (CoMP)" [6]. However, the fronthaul community has a large problem: it has to deal with a whole lot of visitors. The amount of IQ sampled information despatched through the fronthaul can be at the least 10 instances greater than the RF signal`s most bandwidth. This way that optical connections are wanted for transmission. [6], [7]. To help with this problem, researchers have been looking at IQ data compression methods that consume less bandwidth while yet keeping the advantages of a centralized design [8], [9]. Current compression ratios aren't enough for future radio access needs, but researchers are working to improve compression algorithms so that they can keep up with changing network needs. In conclusion, C-RAN is a potential way to meet the changing needs of mobile networks. However, problems like fronthaul traffic congestion mean that new ideas in compression methods and network design are always needed.

Cloud-based honeypots let you look into and study attacks that happen to regular people. With them, an expert may turn the IP addresses and malware being used into security material that can keep the cloud environment safe. There are benefits to using a cloud build. When you look at a cloud framework, a honey pot is like a regular honey pot in that it should be able to tell whether the cloud framework has been compromised or if someone tried to do so. Finally, they may just sit there and record all the activity that comes into the cloud site. Since this is what it's used for, almost any activity should be seen as immediately suspicious.

Honey pots may help make threats more clear and function as an early warning system. This provides a cloud company a more proactive approach to security instead of a reactive one. Any group that works with outside resources or places or cloud services should use cloud-based Honey pots.

The main goal of the suggested system is to change the way cloud-based file-sharing apps are secured by using a new method that combines Honeypot ideas.

The primary goal is to ensure a seamless augmentation of the file-sharing program with HoneyPot capabilities and deploy decoy systems in the best positions to locate and prevent misdemeanor.

With inclusion of Honeypots in the application design, the system is optimistic that they would make the system resistant to a broad variety of cyber attacks, including mere unauthorized access and other sophisticated attacks.

Put in Honeypot functions to the file-sharing application in a way that it can redirect and discover bad activities easily. The integration offers a method of safeguarding potential security threats ahead of time.

The proposed solution will help to shift the thinking of cloud-based file sharing applications with regard to security. The aim of the system is to offer an active, robust and scalable defense system against the dynamic world of cyber threats in cloud computing environment with new security controls and strategic objectives.

2. LITERATURE SURVEY

The distribution of computer resources and services has taken the most favored mode, which is cloud computing. Considering the security of the records in cloud environment, it has gained a lot of significance

as numerous industries have now taken benefit of it. The literature review will serve as an overview of works conducted to enhance the security of the data storage and encryption in cloud computing.

The early definition and experience of scientific cloud computing is presented in the book Scientific Cloud Computing: Early Definition and experience [2] by Lizhe Wang et al. The article discusses the characteristics, make-up and issues cloud computing poses to scientific research. The gist of this article is the discussion on how the concept of cloud computing can be applied in the scientific field; however, it also highlights the importance of addressing concerns on security to safeguard valuable research data.

In their paper, Cong Wang et al. (2015) discuss methods of ensuring the security of data stored in cloud computing environments, or, to be more precise, how to assure the safety of such kind of data (Cong Wang et al., 2015). The article discusses numerous security issues that arise in cloud storage systems as the privacy of data, its safety, and availability. It recommends such measures as cryptographic techniques and access systems in an attempt to make such issues not so of a problem, and enhancing data security. This research takes part in the on-going efforts to secure data in the cloud, emphasizing the imperativeness of effective security solutions.

Atish Jain et al. The paper entitled enhancing the security of Caesar Cipher Substitution method using a Randomized approach to make the communication more secure is on how to make the Caesar cipher substitution technique more secure by applying random approach. According to the research, a novel method was proposed to strengthen the encryption procedure and ensure secure communication ties. The suggested solution makes cryptographic systems more resistant to different types of assaults by adding randomization to the encryption process. This study adds to the larger conversation on encryption methods and how they might help keep communication channels safe in cloud computing settings.

Yogesh Kumar et al.'s paper, "comparison of Symmetric and uneven Cryptography with present Vulnerabilities and Countermeasures [7]," gives a full comparison of symmetric and asymmetric encryption methods. The thing talks approximately the pros and cons of each cryptography methods and appears at the flaws that are already there and the ways to restore them. This examine enables humans pick the proper cryptographic techniques for protective records in cloud computing settings with the aid of showing the exchange-offs among security and pace.

Jaime Raigoza et al.'s comparing performance of Symmetric Encryption techniques [12] looks at how well symmetric encryption techniques work. The study looks at several symmetric encryption methods and compares them based on speed, complexity, and security. This study helps people choose the best encryption methods for cloud computing settings by looking at how well various encryption algorithms work.

Generally, the literature we have reviewed demonstrate the importance of employing advanced security and encryption algorithms to maintain data confidential, security, and available in the cloud computing environments. Through these research works, the cloud computing systems can become

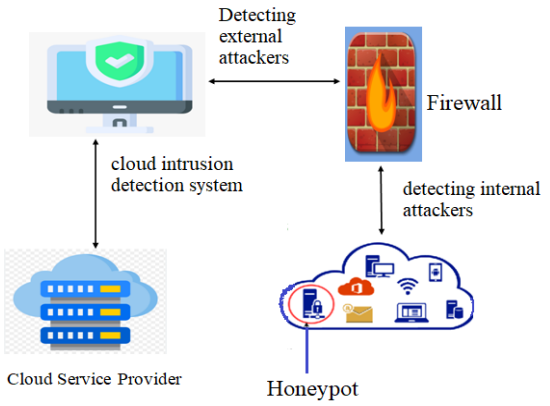
safer as they investigate the encryption methods and address security complications.

3. METHODOLOGY

i) Proposed Work:

The proposed solution is an addition of a Honeypot server to a file-sharing program which operates on cloud servers to secure settings in the clouds. This program allows one to upload, download and share files. It also enables the user to allocate sharing rights and give password to authentic individuals to allow them to view shared files. In case an evil user attempts to down load a file using a fake password, the Honeypot server intercepts and provides them with a fake file. Besides preventing unnecessary access, this step may gather valuable data on the suspected threats as well. The HoneyPot server will also move very proactive since the IP address of bad users is banned permanently and they will not attempt to re-gain entry. The recommended solution will solve the security issues which are already present in the file-sharing program because trapping the malicious traffic using Honeypot ideas will allow securing cloud-based configurations, preventing the leakage of sensitive data and reducing the risks of bad actors.

ii) System Architecture:



"Fig 1 Proposed Architecture"

iii) Modules:

"We have created the following modules to carry out this project: you may register, log in, upload a file, and download a file. A short explanation is provided below:"

a) Register:

The registry module makes it easier to register users to the cloud environment. This is an important step in setting up the user's authentication and access control. When people register, they provide important information such as their name and credentials that are used to confirm their identity and provide them with the right to access certain areas. The sturdy registration method may be very essential to make certain that handiest actual customers can get into the system. This protects in opposition to unauthorized technique and any violation of security. The registration module enables preserve the cloud surroundings secure and personal series and checking the person records correctly. This creates self assurance and duty among customers. This method additionally lays down the segment for adopting strict regulations on get admission to and authentication techniques that enhance standard protection and

decrease the dangers that include unlawful tries to get admission to or negative cloud behavior.

b) Login:

The login module is an essential a part of the device protection as it lets in simplest legal customers to the cloud environment. This module tests the identification of customers or entities and makes positive that simplest the ones who've get right of entry to to the device can do so. Verification normally method checking person login data, which includes usernames and passwords, towards information which are already recorded withinside the device database. Also extra complicated authentication techniques, such multi -issue verification, also can be used for even higher protection. Once the person has been efficiently verified, he can get right of entry to the device and use his / her features consistent with the rights and permissions furnished to them. The login module could be very essential for keeping steady data, preventing unlawful technique and keeping the general integrity of the device protection. It does the proper law of who has get right of entry to to the cloud environment. Following the person`s get right of entry to and pastime tries also can offer you with beneficial records for tracking and audit and make sure that everybody adheres to protection guidelines and principles.

c) Upload File:

The record recording module permits you to securely add documents to the cloud and deliver them the choice to feature passwords or encryption keys for similarly protection. This characteristic enables save you negative conduct through permitting customers to maintain their facts secure from others who need to now no longer get entry to it. The machine can take a look at that recording is real, and ensure that best folks who are allowed to peer the documents which have been uploaded ask customers for encryption keys or passwords in the course of the add process. This module may consist of verification exams that prevent recording documents that might be risky or harmful, which might be an excellent more secure cloud environment. In general, the add record module may be very essential to keep facts protection withinside the cloud environment. It permits customers to securely update and keep your documents whilst decreasing the threat of negative conduct.

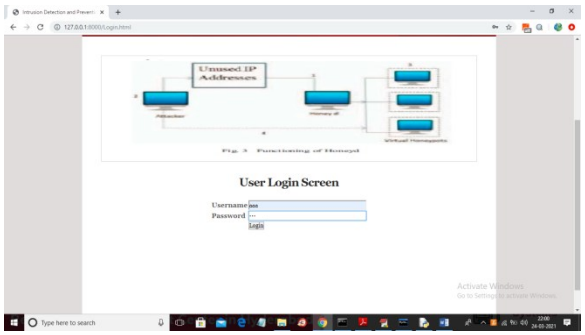
d) Download File:

The download module allows you to download users who have logged into tightening files from the cloud, but must provide the file for the file. When people share files, the uploader gives real users sharing rights and passwords. If someone tries to download the file using a bogus password, the Honeypot server stops them by showing them a blank page. This proactive step stops anyone from trying to get into the system without permission, which protects the system's integrity and prevents possible security breaches.

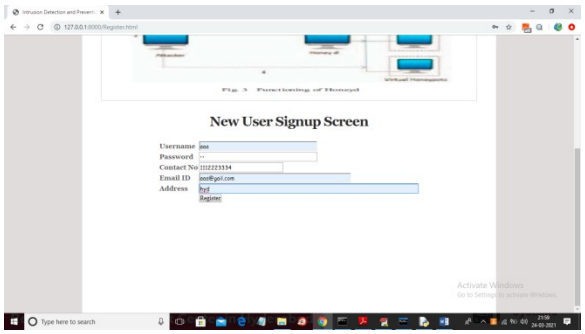
4. EXPERIMENTAL RESULTS

“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.”

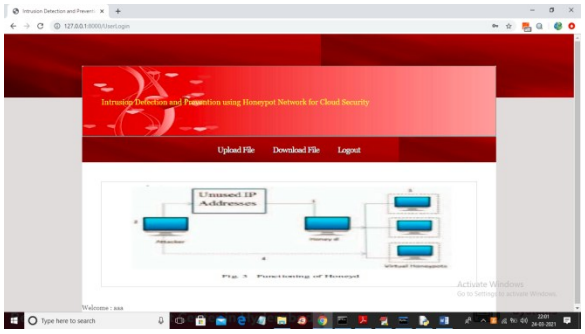
"In above screen click on 'Register Here' link and register some users"



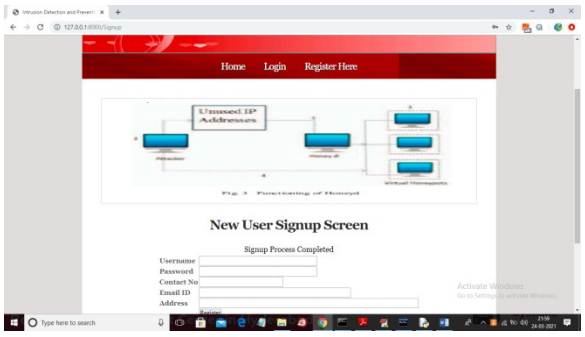
"In above screen user 'aaa' is logged in and after login will get below screen"



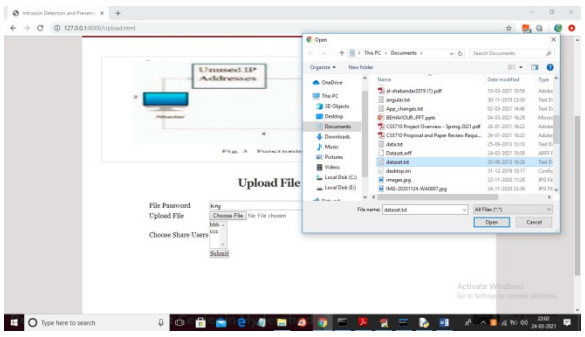
"In above screen adding one user and then click on 'Register' button to get below screen"



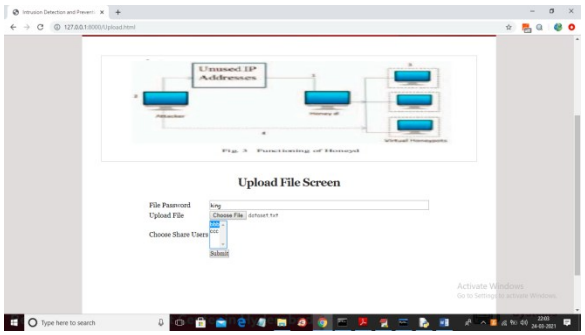
"In above screen now user can click on 'Upload File' link to upload files"



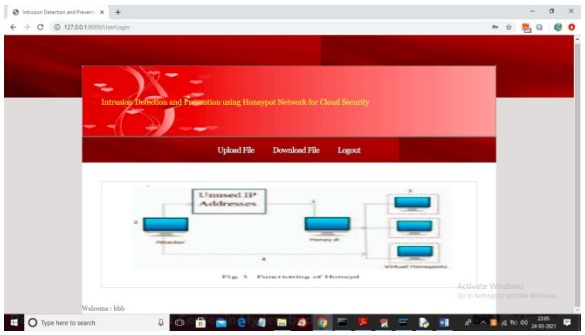
"In above screen user signup process completed and similarly you can add many more users and now click on 'Login' link to get below login screen"



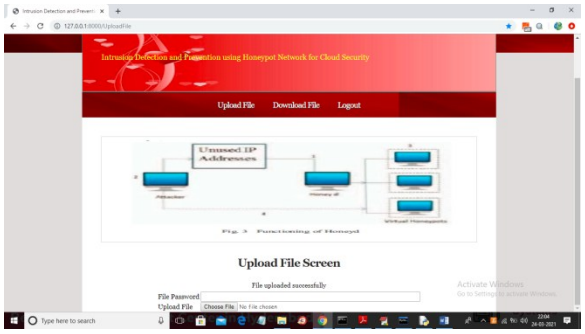
"In above screen in first field we need to enter file password and then click on 'Choose File' button to select any file and then select require users with whom you want to share file and you can select multiple users by holding CTRL key from keyboard"



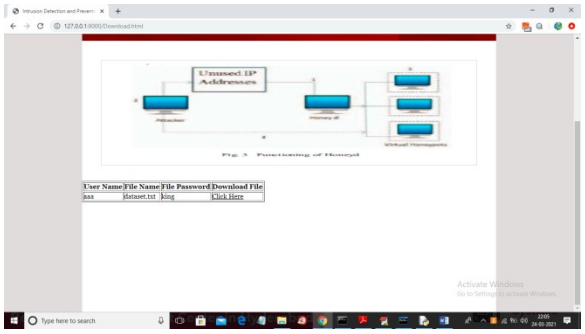
"In above screen user aaa is sharing file with bbb and now click on 'Submit' button to upload file"



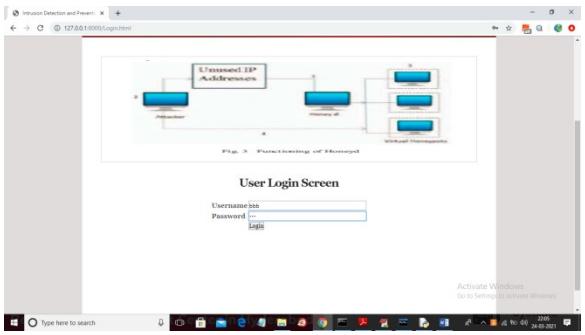
"Now click on 'Download File' link to get below screen"



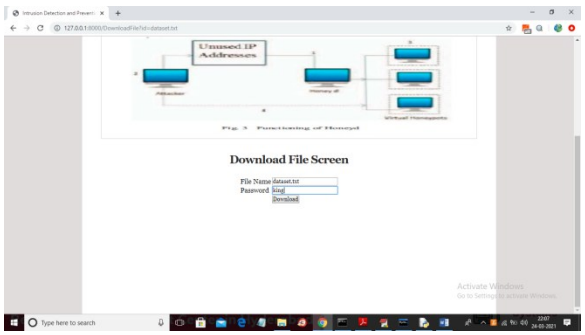
"In above screen file is uploaded and now logout and login as user bbb to download file"



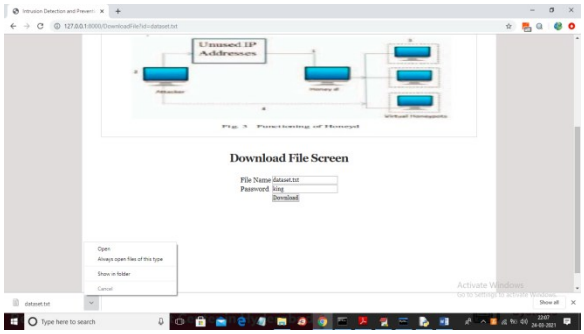
"In above screen bbb user can see all files list shared by other user and password of file also will be visible to him as user aaa has given share permission to him. now any time bbb user can click on 'Click Here' link to download file and to get below screen"



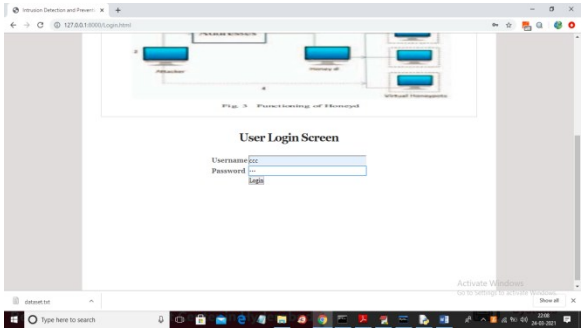
"In above screen user bbb is login and after login will get below screen"



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

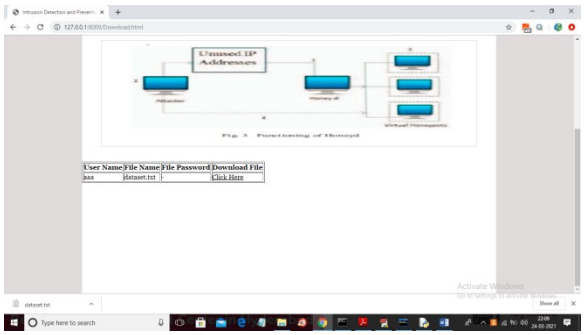


"In above screen in status bar file is downloaded and now logout and login as user ccc who don't have share permission"

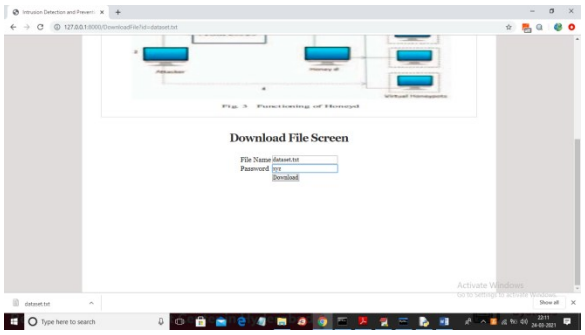


"In above screen user ccc is login and after login will get below screen"

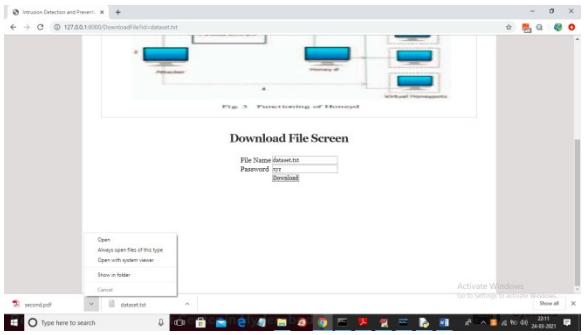
"In above screen now user can click on 'Download File' link to get below screen of file list"



"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"

5. CONCLUSION

Finally, companies and organizations who depend on outside resources, cloud services, or handle sensitive data in the cloud must use cloud-based honeypots. IT workers can set up Honeypots, but security teams who are always on the lookout for bad behavior should be in charge of the strategic design. Using open-source tools for monitoring and collecting logs makes Honeypots work better, but they need to be customized for each cloud platform, such as Amazon EC2, Microsoft's Azure, or IBM's cloud. Even while traditional honeypots don't always operate exactly like cloud settings, they give an extra degree of protection when used with professional network administrators. Best practice is that you should customize your settings early on so that enemies who know the default settings won't be able to find you. In the end, Honeypot technology is a proactive and flexible way to find possible dangers in cloud-based platforms when used in a security-conscious setting.

6. FUTURE SCOPE

Cloud is one of the few technologies that can really transform things. It is highly important to make the cloud's security stronger. We show how to utilize Honeypot to deal with bad users. Companies may choose to use Honeypot to find rogue components. By doing that, you can readily grasp how an attacker acts. Because threats are growing every day in information. More technology and work are needed. Honeypot adds an added layer of protection and detection, and as technology improves, these features may be made even better.

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] Kashish Goyal, SupriyaKinger" Modified Caesar Cipher for Better Security Enhancement" International Journal ofComputer Applications (0975– 8887) Volume 73– No.3, July 2013.

[7] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography withExisting Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and ManagementStudies, Vol. 11, Issue 03, Oct 2011.

[8] Mr. Gurjeevan Singh, Mr. AshwaniSingla and Mr. K S Sandha " Cryptography Algorithm Compaison ForSecurity Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary ResearchVol.1 Issue 4, August 2011.

[9] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of SymmetricEncryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[10] Gurpreet Singh, SupriyaKinger"Integrating AES, DES, and 3 -DES Encryption Algorithms for Enhanced DataSecurity "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[11] Atish Jain, Ronak Dedhia, Abhijit Patil , et. al., "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication" published in research gate open Access, available at https://www.researchgate.net/publication/284160169.

[12] Jaime Raigoza; Kapil Jituri, et. al., "Evaluating Performance of Symmetric Encryption Algorithms" published in ieee open Access, available at https://ieeexplore.ieee.org/document/7881551.