International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 15th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 12

DOI: 10.48047/IJIEMR/V11/ISSUE 12/25

Title **INTRUSION DETECTION AND PREVENTION USING HONEYPOT NETWORK FOR CLOUD SECURITY**

Volume 11, ISSUE 12, Pages: 180-188

Paper Authors
Kandula Mounika, DR.V.UMA RANI

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

INTRUSION DETECTION AND PREVENTION USING HONEYPOT NETWORK FOR CLOUD SECURITY

1 Kandula Mounika, M.tech in software engineering (SE) SIT JNTUH
2 DR.V.UMA RANI, Professor of CSE

ABSTRACT: Due to the rapid growth in users, issues with hardware failure, web hosting, data space and memory allocation, and other issues are directly or indirectly contributing to data loss. We use cloud computing techniques to deliver services that are dependable, quick, and affordable. The likelihood of malevolent individuals compromising this technology's security is rising as a result of its enormous development. Using a honeypot is one approach to direct harmful traffic away from systems. It is a massive method that has improved system security in some ways. The possibility of Honeypot is applied in a document sharing project that is introduced on cloud servers, thinking about the numerous legitimate troubles one might experience while putting Honeypot on outsider cloud seller servers. This article covers how to identify assaults in a cloud-based environment and how to secure it using honeypots, while also suggesting a novel method for doing so.

Keywords: *detection, Honeypot, Cloud Computing, Honeyd, Honeynets, Cloud IDS.*

1. INTRODUCTION

Data in the cloud can be accessed, shared, and stored by any device connected to a network, typically the internet, at any time and from any location. A device can access an expanding storage space that has no physical storage and can be accessed from anywhere in the world when it is connected to the internet [1]. It features a huge number of processing units connected in real-time over the internet, as well as a shared data storage space. In view of the way that a cloud-like structure was utilized to signify network phone charts and thusly the Web as a deliberation of the basic framework it addresses, the expression "the cloud" is utilized as an illustration for the Web [4]. Honeypots are seen to be a successful method for monitoring programmer behaviour and enhancing the effectiveness of security tools. Honeypots are especially made to intentionally draw in and stunt programmers, yet additionally to recognize unlawful web-based movement and can be viewed as a productive method for checking programmer conduct [11]. A honeypot is a system or asset that is used to catch, monitor, and identify erroneous requests that are present in a network. Every sort enjoys benefits and downsides relying upon the degree of reach it offers the aggressors, going from little cooperation to medium and high. Their goal is to observe, monitor, and track the behaviour of attackers in order to develop systems that are both safe and able to manage such traffic. We wish to investigate, attack, or hack this carefully guarded computational resource. It is a data framework asset whose worth is determined through unlawful or unlawful utilization, to be more precise. [2].

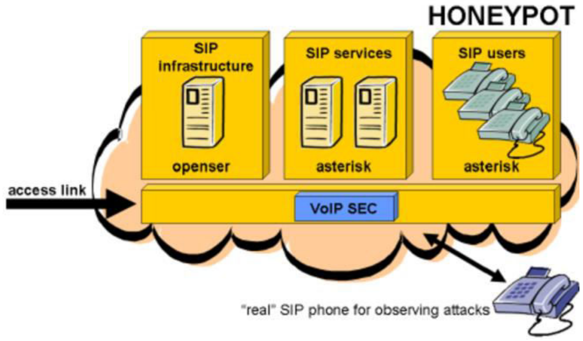


Fig.1 Honeypot.

Cloud-based Honeypots allow for the exploration and analysis of attacks that target common consumers [14]. Having them empowers a specialist to decipher the malware being utilized and IP areas into security material that can ensure a normal cloud climate [20]. When those IP addresses have been recognized, they will do a ping degree and vulnerable result to distinguish any blemishes in the plan of the framework or any risky code defects [12]. It is obvious yet true that bad people frequently seek the weakest goals [9]. Utilizing a cloud construct has benefits. The honeypot ought to have the option to decide if a cloud structure has been compromised or endeavors have been made to do as such, similar as conventional honeypots.

2. LITERATURE REVIEW

Design of Privacy-Preserving Cloud Storage Framework

Concerns regarding privacy and security are essential for cloud storage. The study proposes a framework for privacy-preserving cloud storage that takes into account participant engagement, the creation and administration of keys, the structure of the data organization, and modifications to users' access rights. We give an intuitive convention, an extirpation-based key age method, slow repudiation, a multi-tree structure, and symmetric encryption to make a viable and confidential distributed storage system. The acknowledgment of a framework based on the structure. The productivity of the extirpation-based key age procedure, the framework above, and the structure's protection security are undeniably analyzed in this review. At long last, we present a rundown of our discoveries and framework our next research plans.

Scientific Cloud Computing: EarlyDefinition and Experience

Determined to give end clients reliable, customized, and QoS guaranteed registering dynamic settings, distributed computing is arising as another worldview in processing. This exposition examinations current improvements in distributed computing, characterizes the thoughts and characteristics of logical mists, and afterward gives a representation of a logical cloud for server farms.

Ensuring Data Storage Security in Cloud Computing

As the arranged cutting edge design for IT organizations, distributed computing. Distributed computing sends the application programming and data sets to the enormous server farms, where the organization of the information and administrations may not be totally dependable, rather than regular arrangements, where the IT administrations are under sufficient physical, coherent, and individuals controls. Nonetheless, this particular quality presents various novel security gives that are minimal perceived. Here, we put an extraordinary accentuation on cloud information capacity security, which has forever been a significant part of administration quality. In spite of its progenitors, we give a productive and versatile circulated design with two prominent elements to get the exactness of clients' information in the cloud. Our technique coordinates capacity exactness protection and information issue localisation, i.e., the location of acting mischievously servers, by utilizing the homomorphic token with circulated confirmation of eradication coded information (s). As opposed to most of before research, the new methodology likewise gives effective and secure powerful procedure on information blocks, for example, information update, erase, and add. The recommended procedure is incredibly successful and sturdy against Byzantine disappointment, malevolent information adjustment attacks, and even server agreement assaults, as per broad security and execution studies.

Comparison of Symmetric and Asymmetric Cryptography withExisting Vulnerabilities and Countermeasures

Since applications for the internet and networks are expanding quickly, it is more important than ever to safeguard them using cryptographic techniques. Symmetric and asymmetric encryption techniques are the two that are most often used and recognised. Ideally, RSA and DES belong to the category of asymmetric key cryptography and symmetric key cryptography, respectively. The RSA and DES cryptographic algorithms are briefly described in this document, along with any current weaknesses and workarounds. In addition, theoretical performance analyses and symmetric and asymmetric cryptography comparisons are included.

Cryptography Algorithm Compaison ForSecurity Enhancement In Wireless Intrusion Detection System

Because of how simple they are to set up and how affordable they are, wireless networks are expanding quickly and gaining popularity daily. The main worry with wireless networks is security. There is always a chance that network security will be breached due to attacks in Wireless Network Systems. This paper describes intrusion detection systems for wireless networks as well as numerous threats to them, including DoS, jamming the network, junk transmission, teardrop, ping-of-death (POD), and man-in-the-middle attacks. The Wireless Intrusion Detection System (WIDS) is a device for spotting illegal network access. This task is often carried out by an IDS using either anomaly-based detection or signature-based detection. The information security systems heavily rely on encryption methods. On the other hand, these methods increase CPU burden and quickly deplete battery. In this study, encryption methods including AES, DES, 3DES, RC2, Blowfish, and RC6 are evaluated. Blowfish was deemed to be the best encryption algorithm after comparisons were done for those algorithms.

Performance Evaluation of SymmetricEncryption Algorithms:

Applications for the internet and networks are expanding quickly, thus there is a greater need to defend these applications. In information security systems, encryption methods are crucial. On the other hand, those methods need a lot of computational resources, including memory, CPU time, and battery power. AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6 are six of the most used encryption algorithms that are evaluated in this study. These encryption techniques have been compared at several parameters for each algorithm, including various data kinds, data block sizes, battery power consumption, different key sizes, and encryption/decryption performance. To illustrate each algorithm's efficacy, simulation results are provided.

Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security ofCloud in Cloud Computing:

The cloud is a platform of the future that offers virtualization, high availability, and dynamic resource pools. The procedure of "distributed computing" permits us to utilize adaptable, circulated processing conditions inside the limits of the Web today. Distributed computing was incorporated to address regular PC issues such clients' absence of admittance to equipment, programming, and assets. A straightforward and powerful answer for day to day processing is presented by distributed computing. Cloud security and the legitimate execution of the cover over the organization are the central concerns with distributed computing. By executing a computerized signature utilizing the RSA strategy, we have endeavored to assess the Distributed storage Procedure and Information Security in the Cloud in this Exploration Paper.

3. IMPLEMENTATION

Attacks that target common consumers can be explored and examined using cloud-based honeypots. Having them empowers a specialist to decipher the malware being utilized and IP areas into security material that can ensure an ordinary cloud climate. When those IP addresses have been distinguished, they will do a ping degree and helplessness result to recognize any blemishes in the plan of the framework or possibly perilous code.

Disadvantages:

- Denial of Service, malicious insiders, insecure interfaces and APIs, traffic hijacking, and others.

The author of the proposed article has created a honeypot server that accepts user requests for file uploads, downloads, and sharing. When sharing files, users will grant passwords and sharing rights to trustworthy users, and after sharing, users can provide passwords for file downloads. Any malignant client who endeavors to download a document with a misleading secret word will be sent a clear page by the honeypot server. On the off chance that we give the aggressor a clear page in the proposed paper, he will rapidly understand that the honeypot is offering him no response, so, all in all he will stop all further activity. In order to overcome this issue, Honeypot serves phoney files in place of empty responses. This assures the attacker that the server has been effectively hijacked, allowing him to continue delivering harmful activities that aids Honeypot in gathering further information from him.

Advantages:

- Frames an original technique for getting information and assets in a cloud utilizing Honeypot and proposes how to utilize it utilizing an application on the previously mentioned framework (Distributed computing Climate).
- There are sure limitations that should be stuck to while utilizing a Honeypot. A report might be shared and put away utilizing the program.

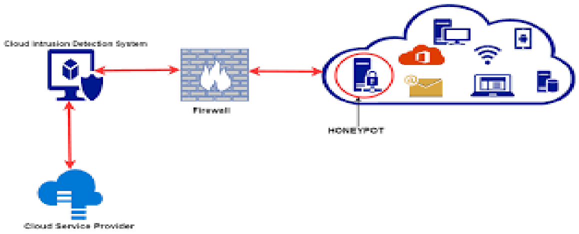


Fig.2: System architecture

While examining an attack on a framework to find blemishes and shortcomings of a similar objective framework so that some type of benefit might be gotten from it, there are various procedures in the domain of possibility[6]. A honeypot frequently fills in as a reconnaissance device and, if essential, can give an early admonition. It is a PC framework, site, or application that not just gives the impression of being a different substance from the remainder of the organization yet additionally much of the time approaches delicate information that can be utilized against the client or the organization [8]. In the going with study, an original strategy for shielding information and assets in a cloud utilizing Honeypot is proposed. It is carried out utilizing an application on the previously mentioned foundation (Cloud Computing Environment). While implementing a Honeypot, there are several restrictions that must be adhered to. A document may be shared and stored using the programme [5]. The document is password-encrypted when shared or uploaded. If the right password is not entered, no message but an empty file will be presented to the attacker [7]. Since a Honeypot's operation includes quiet detection, the programme logs the user's IP address so that the administrator may later analyse it and identify the malicious party.

Finally, they may effectively sit and log every activity that enters the cloud site. Since it is used for this specific purpose, almost every action should be seen as immediately suspect [18]. Honeypots may be used to highlight threats and operate as an early warning system, giving a cloud company a more proactive approach to security rather than a reactive one [11]. Any connection to external systems or resources or to cloud-based management systems should use cloud-based honeypots.

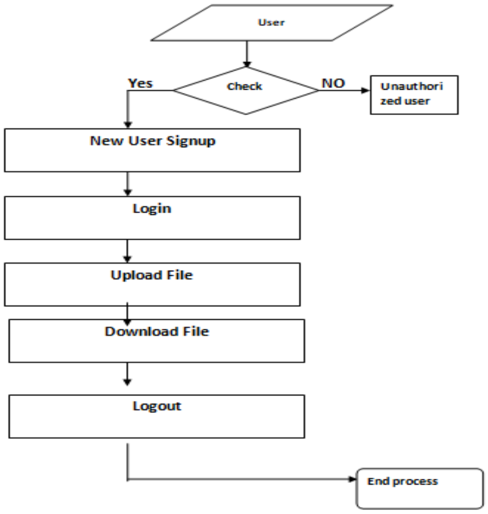


Fig.3: Dataflow diagram

MODULES:

- Register New User
The user will register in this module.
- Login
The user will login in this module.
- Upload File Users will upload files in this module.
- Save the file
The user will download a file from this module.
- Logout
The user will log out of this module.

4. ALGORITHMS

Honey pots :

Attacks that target common consumers can be explored and examined using cloud-based honeypots. Having them empowers an expert to interpret the infection utilization and IP areas into security material that can ensure an ordinary cloud climate. When such IP addresses have been recognized, they will next incite a ping extension and vulnerability result to distinguish any programming defects or shortcomings that may be taken advantage of. It's obvious yet true that bad people frequently seek the weakest goals. Using a cloud build has benefits. The honeypot ought to have the option to decide if a cloud system has been compromised or endeavors have been made to do as such, similar as conventional honeypots.

Types of Honeypots

Generally speaking, there are two sorts of honeypots:

Honeypots with low and high engagement.

a) Low- Interaction Honeypot: Low-interaction Limited interaction is used in honeypots. This is so that the activity of the attackers is constrained to the Honeypot's level of emulation. Low-interaction honeypots are simple to deploy because of their straightforward architecture. They pose little risk and are much simpler to maintain. Additionally, the attacker never has access to an operating system from which to damage other computers. The biggest drawback of this kind of honeypot is that it only logs a limited amount of information on its database, which also records any unlawful activity. Regardless of how brilliant the copying is, a prepared aggressor can eventually distinguish the presence of a low-connection Honeypot, thus it is likewise more straightforward for an assailant to recognize them. Ghost, Honeyd, and KFSensor are a couple of instances of low-connection honeypots.

b) High- Interaction Honeypot: When contrasted with low cooperation honeypots, high connection honeypots are ordinarily more refined because of continuous programming and application association. Aggressors are given admittance to ongoing programming and frameworks. This kind of honeypot deployment allows for the collection of large quantities of data and offers an open environment that records every activities. High-interaction solutions can develop behaviours we wouldn't anticipate because to this.

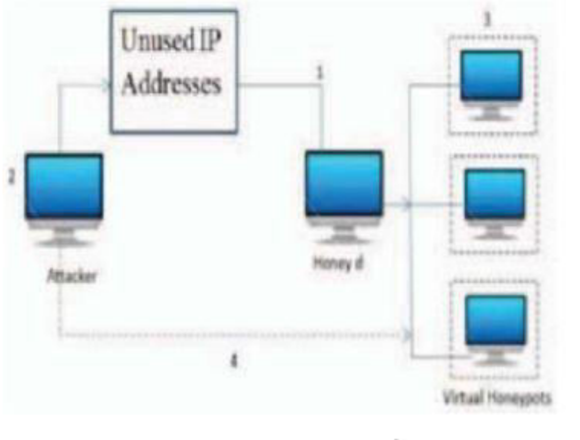
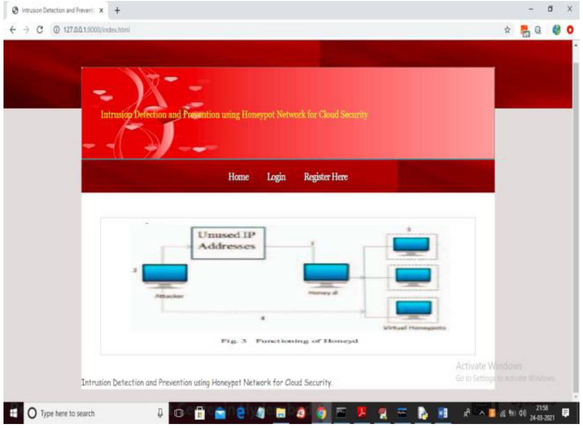


Fig.4: working diagram

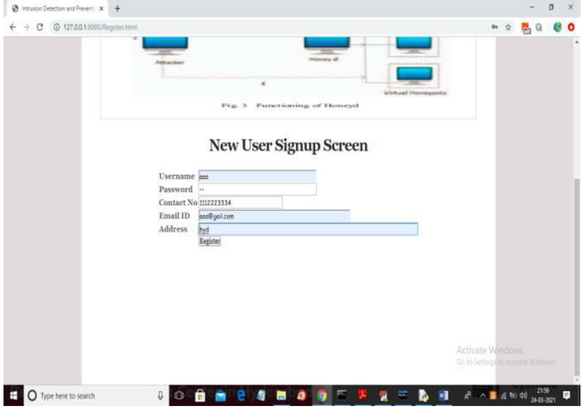
5. EXPERIMENTAL RESULTS

Data sets are minimal since honeypots only record harmful activities, such as attacks and other unauthorised acts. Data that is simple to handle and analyse is collected by honeypots [15]. Assault-related false alarms are decreased when unlawful conduct is recorded. The least amount of resources are generally used by honeypots. [10]. Honeypots can record even encrypted assaults. Some Honeypot versions are simple to deploy and, thus, simple to maintain.


Intrusion Detection and Prevention using Honeypot Network for Cloud Security

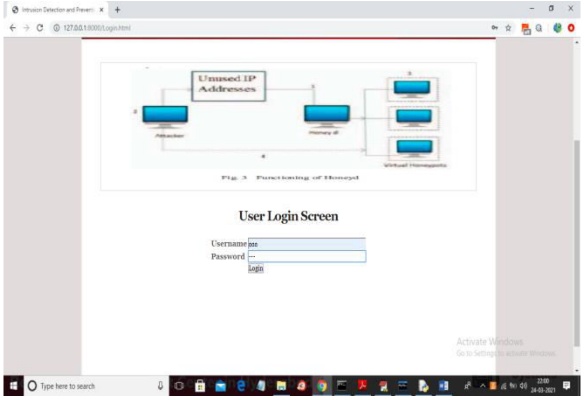
Intrusion Detection and Prevention using Honeypot Network for Cloud Security.

Fig.5: Home screen


New User Signup Screen

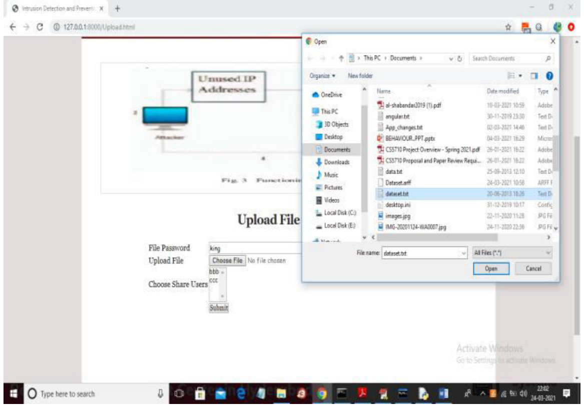
Username ooo
Password ··
Contact No 1112223334
Email ID ooo@gail.com
Address hyd

Fig.6: Registration screen


User Login Screen

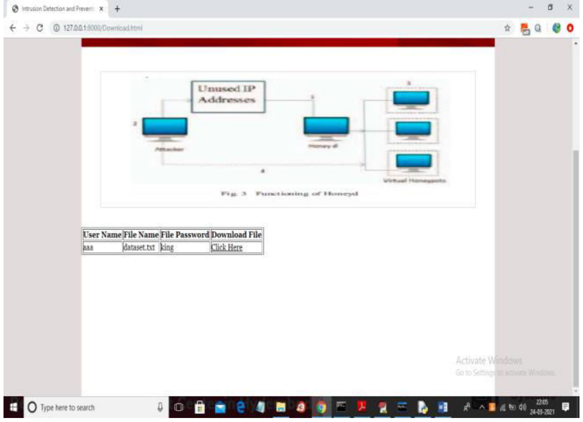
Username ooo
Password ···

Fig.6: Login screen


Upload File

File Password king
Upload File No file chosen
Choose Share Users bbb ccc

Fig.7: Upload file


Intrusion Detection and Prevent
127.0.0.1:8000/Download.html
Unused IP Addresses
Attacker
Honey d
Virtual Honeypots
Fig. 3 Functioning of Honeyd
Activate Windows
Go to Settings to activate Windows.
Type here to search
22:05
24-03-2021

User Name	File Name	File Password	Download File
aaa	dataset.txt	king	Click Here

Fig.8: Download file

5. CONCLUSION

Any association or business that utilizations cloud organizations or outside assets/regions ought to set up cloud-based honeypots. The IT group could be important to set up the honeypots, yet the security groups' character checking for vindictive action ought to truly decide the plan. Any association taking care of delicate information in the cloud should lean toward Honeypots, and they will likewise require gifted framework directors to survey the logs and answer the data. Honeypot monitoring and log collection can now be aided by incredible open-source tools. Obviously, the cloud stage itself is a factor. "Amazon EC2's ideal Honeypot will be in contrast to Microsoft Azure or IBM's cloud." Because they frequently imitate more conventional desktop and server operating systems, typical Honeypots are not perfect. However, when appropriate security professionals are constantly verifying and analyzing, their communication is most effective. The added use of human participation adds an extra layer of protection, and a professional may see a dangerous or harmful attack that had never been observed, thus watching programmes would have no learning. To start over is one of the greatest pieces of best practise advice. Bad actors will be well-versed in the default settings of honeypot technology due to its open source nature, and they will be on the lookout for these early warning signs of a trap. These technologies need to be set up in a way that cares about its customers and wants to give its cloud-based platform an extra layer of protection.

6. FUTURE SCOPE

It is absolutely necessary to improve cloud security because the cloud is one of the few technologies that has the potential to bring about a significant shift. In this work, we outline a Honeypot-based strategy for dealing with rogue users. For the purpose of identifying rogue elements, organisations may favour employing Honeypot. By using it, one may quickly comprehend an attacker's conduct. Additional measures must be made since information technology dangers are rising daily. The additional security and detection features provided by honeypots may be upgraded as technology develops.

REFERENCES

[1] RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui, "Design of PrivacyPreserving 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] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security ofCloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC- 2010).

[12] ChitraRajagopalan. P,TanupriyaChoudhury,Praveen Kumar, A Proposal and Implementation of Algorithm to enhance the security of the cloud", 5th Fifth International Conference on System Modeling & Advancement in Research Trends,IEEE,2016.

[13] BhaskarMandal,Tanupriya Choudhury," A Key Agreement Scheme for Smart Cards Using Biometrics.", IEEE International Conference (Published in IEEE) ICCCA 2016 ,Galgotias University,2016.

[14] Bhaskar Mandal ,Tanupriya Choudhury, "A Secure Biometric Image Encryption Scheme using Chaos and Wavelet Transformations", International Journal of Advanced Security in Data Analytics and Networks (Special Issue for Recent Advances in Communications and Networking Technology),2016.

[15] Karthik Sadasivam, Banuprasad Samudrala, T. Andrew Yang. "Design of Network Security Projects using Honeypots", University of Houston.