RB Journal of Lib & Information Science ISSN: 0972-2750
(UGC Care Group I Listed Journal) Vol-12 Issue-07 No.01: 2022

AN ENCROACHMENT PERCEPTION AND AVOID INTRUSION FOR CLOUD SECURITY USING HONEYPOT

M.Kavitha, Associate Professor, Sridevi Women's Engineering College, Hyderabad, E-mail:kavithareddy2414@gmail.com
Madireddy Akhila, B.Tech, Dept of Information Technology, Sridevi Women's Engineering College, Hyderabad, E-mail:madireddyakhila@gmail.com
Ramagiri Bindu Priya, B.Tech, Dept of Information Technology, Sridevi Women's Engineering College, Hyderabad,E-mail:ramagiribindupriya@gmail.com
Velpoor karrolla krithika, B.Tech, Dept of Information Technology, Sridevi Women's Engineering College, Hyderabad, E-mail:krithikavelpoor@gmail.com
Ramadugu Sahithya, B.Tech, Dept of Information Technology, Sridevi Women's Engineering College, Hyderabad, E-mail:sahithya7262@gmail.com

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.

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

1. INTRODUCTION

Cloud computing is a technique to store, share and access data anytime and anywhere with a device that is connected to a network, preferably the internet. Cloud computing consists of an expandable storage space with no physical storage space which is accessible from anywhere in the world using any device, by connecting it to the internet [1]. It contains large number of computing devices connected through a real-time communication (the internet) and has a common data storage area. The term “the cloud” is used as a metaphor for the Internet, based on the fact that a cloud like shape was used to indicate network telephone schematics, and later the Internet as an abstraction of underlying infrastructure it represents [4]. Honeypots are viewed as a successful technique to track programmer conduct and uplift the viability of security instruments. Honeypots are specifically designed to not only purposely engage and deceive hackers but also identify malicious activities performed over the Internet and can be counted as an effective method to track hacker behaviour [11]. Honeypots can be defined as systems or assets which are used to not only trap, monitor but to also identify erroneous requests present within a network. They vary in the interaction provided to the attackers, from low interaction to medium and high, each type has its advantages and disadvantages. Their aim is to analyze, understand, watch and track attacker’s behaviour in order to create systems that are not only secure but can also handle such traffic. It is a closely monitored computing resource that we want to be probed, attacked, or compromised. “More precisely, it is an information system resource whose value lies in unauthorized or illicit use of that resource.” [2].

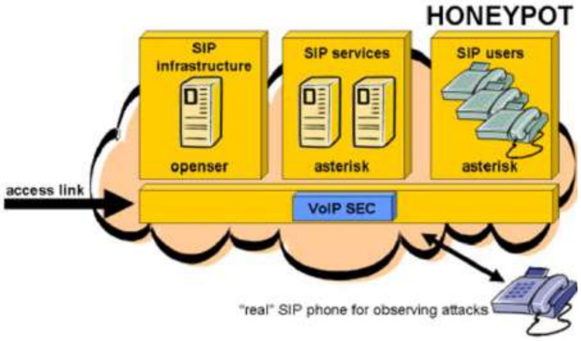


Fig.1 Honeypot.

Cloud-based Honeypots give the capacity to explore and examine assaults that hit ordinary customers [14] .Having them permits a specialist to interpret the IP locations and malware being utilized into security content that can ensure a normal cloud environment [20]. 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 [12]. 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.

2. LITERATURE REVIEW

Design of Privacy-Preserving Cloud Storage Framework

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

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

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 with Existing Vulnerabilities and Countermeasures

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 For Security Enhancement In Wireless Intrusion Detection System

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.

Performance Evaluation of Symmetric Encryption Algorithms:

Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Encryption algorithms play a main role in information security systems. On the other side, those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. This paper provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types ,battery power consumption, different key size and finally encryption/decryption speed. Simulation results are given to demonstrate the effectiveness of each algorithm.

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

The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. Cloud computing is the Concept Implemented to decipher the Daily Computing Problems, likes of Hardware Software and Resource Availability unhurried by Computer users. The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing. The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm.

3. IMPLEMENTATION

Existing system

Cloud 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 defence lessness output to discover a shortcoming in the system outline or vulnerabilities in programming that can be misused.

Limitations

- Less efficient and security

- Insecure Interface and APIs.
- Less Confidentiality and integrity.

Proposed work

In propose paper author designing Honeypot server which accept user request to upload, download and share file. While sharing file users will give sharing permission and password to genuine users and then share users can give password to download file. If any malicious user try to download file with fake password then Honeypot server will serve him fake file, which assure attacker that server has successfully hijack and he continue sending malicious activity which help Honeypot extract more information from him.

Advantages

- Proposes a new technique of protecting data in a cloud through Honeypot by implementing it through an application on the above mentioned infrastructure (Cloud Computing Environment).
- There are many restraints that need to be followed while implementing a Honeypot. The application makes it possible to store as well as share a document.
- Provides more security and authentication.

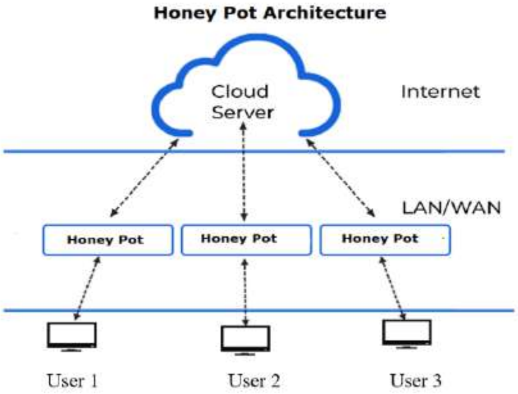


Fig.2: System architecture

There are Various of ways in the vision of possibility when talking about an attack on the system in order to discover some faults and vulnerabilities of that same target system so that some kind of advantage can be taken out of it[6]. Honeypot tends to perform as a surveillance tool and can also provide an early warning if required. It is a computer system or a site or an application that not only appears to be an isolated part of the network but usually also contains the information that is can be valuable attacking entity, which are highly trained to exploit the data to such an extent that it can harm the firm [8]. The following paper proposes a new technique of protecting data and resources in a cloud through Honeypot by implementing it through an application on the above mentioned infrastructure (Cloud Computing Environment). There are many restraints that need to be followed while implementing a Honeypot. The application makes it possible to store as well as share a document [5]. While sharing or uploading the document it is encrypted using a password. If the correct password is not given then no message would be displayed rather the attacker would be shown an empty file [7]. Since the actual working of a Honeypot involves silent detection, hence the application tracks the IP address of the user so that later the admin can review it and recognize the malicious entity.

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 [18]. 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 [11]. Any association with either outside resources/areas or cloud administrations ought to deploy cloud-based Honeypots.

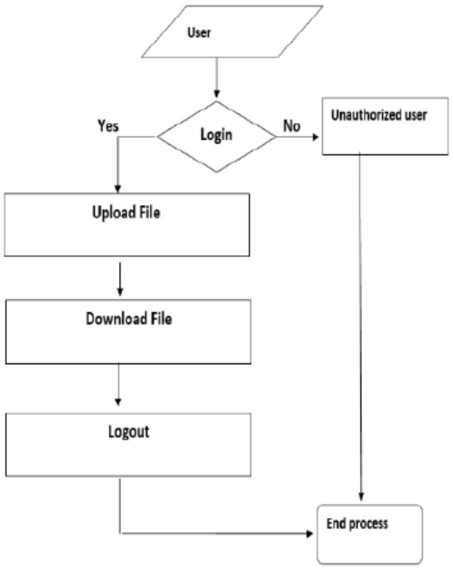


Fig.3: Dataflow diagram

MODULES:

- Users

Initially user Registers and Logins the Application by their user credentials.

- Honeypot Deployment

Honeypot in our work is deployed to detect, prevent and gives response to the intruders and also keep track of malicious activities done by the Hacker.

- Cloud Server

User can access services from the cloud server by storing and retrieving the files.

4. ALGORITHMS

Honey pots :

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. 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.

Types of Honeypots

Honeypots are divided mainly into two types:
1. lowinteraction
2. high-interaction Honeypots.

a) Low- Interaction Honeypot: Low-interaction Honeypots practice limited interaction. This is because the attacker activity is limited to the level of emulation by the Honeypot. Low-interaction Honeypot have a simple architecture and therefore they are easy to deploy. They are even easier on the maintenance side, offering minimal risk. Moreover, the attacker is never able to access an operating system in order to harm other systems. The main disadvantage of this type of Honeypot is that limited information is logged on the Honeypot database which also captures any unauthorized action. “It is also easier for an attacker to detect a lowinteraction Honeypot, no matter how good the emulation is, a skilled attacker can eventually detect their presence.”. Examples of low-interaction Honeypot include Specter, Honeyd, and KFSensor.

b) High- Interaction Honeypot: High-interaction Honeypots are usually complex in comparison to low interaction Honeypots, the reason of their complexity being: real time interaction with software and applications. Attackers are provided with real time systems and software. Extensive amounts of information can be captured in this type of Honeypot deployment and an open environment is provide that captures all activity. This allows high-interaction solutions to learn behaviour we would not expect .

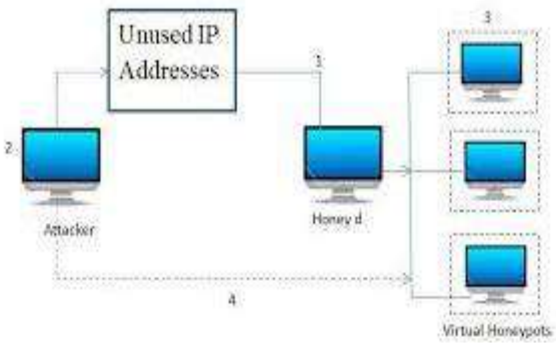


Fig.4: working diagram

5. EXPERIMENTAL RESULTS

Data sets are small as Honeypots collect the data about any malicious activity which includes attack or any kind of unauthorised act. Honeypots collect the data which can be easily managed and analyzed [15]. False Alarms about a attack are reduced when they capture unauthorized activity. Honeypots usually tend to make use of least possible number of resources.[10]. Even encrypted attacks can be captured by Honeypots.Some versions of Honeypot are easily deployed and hence can be easily maintained.

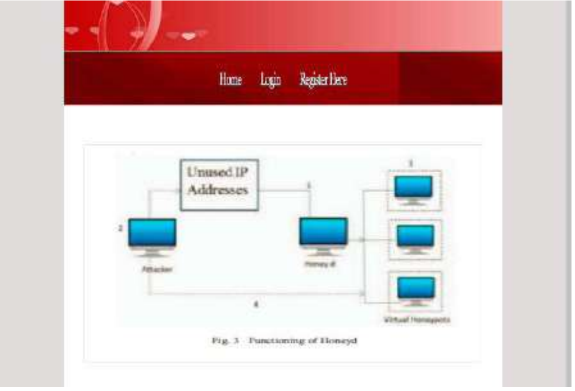
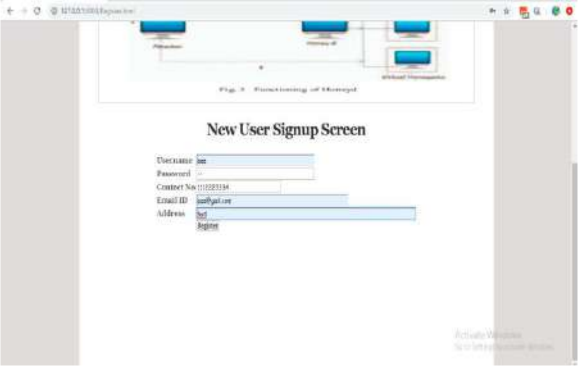


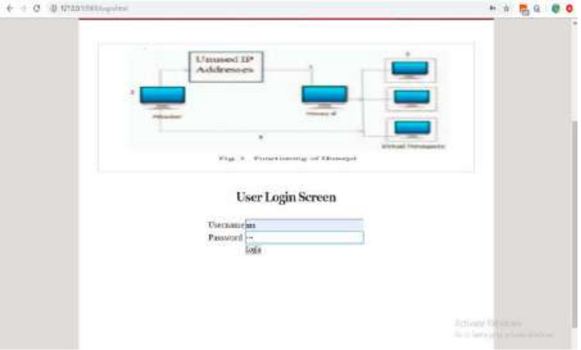
Fig.5: Home screen



New User Signup Screen

Username [illegible]
Password
Contact No 1112223334
Email ID [illegible]
Address [illegible]
Register

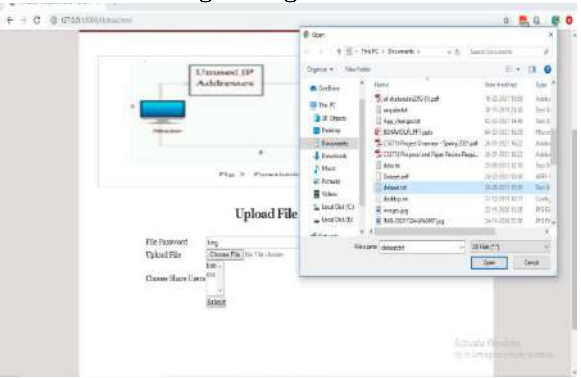
Fig.6: Registration screen



User Login Screen

Username aa
Password ••

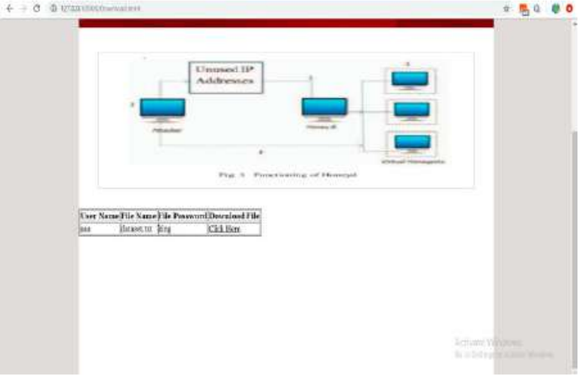
Fig.7: Login screen



Upload File

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

Fig.8: Upload file



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

Fig.9: Downloads Fake file for the   unauthorized user.

6. 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.

7. FUTURE SCOPE

Cloud is one of the few technologies that can bring about a major change, hence it is very necessary to make security of cloud more strong. In this paper we present a way to tackle malicious users using Honeypot. Organizations can prefer using Honeypot for detection of rogue elements. One can easily understand the behavior of an attacker by implementing it. Since risks are increasing day by day in Information. Technology extra efforts are required to be put in. Honeynet ensures extra security and detection feature which can be further increased in standard as the technology advances.

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.