IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA SECURITY IN CLOUD COMPUTING

[1]Vinit Pereira, [2]Parul Sahare,

[1]M. Tech Scholar, [2]Assistant Professor,
[1]Electronics & Communication Engineering,
[1]Indian Institute of Information Technology, Nagpur, India

Abstract: Presently DWDM technology referring to transmission of multiple wavelengths into a single fiber is gaining importance. Optical transport network performs "**Digital Wrapping**" of all kinds of client signals for optimum utilization of Bandwidth with various data rate standards. Emphasis is laid on Modus operandi of Hackers to exploit all the possibilities to intrude into High Bandwidth systems in order to gain superiority. The study also refers to increasing trends and popularity of cloud computing due to flexibility in services offered by various firms. Irrespective of increasing demand the security concerns due to deliberate cyber-attacks cannot be negotiated. Cyber security issues, threats and attacks are well defined with its implications in this study. The means and measures to be undertaken to counter the cyber-attacks is challenging issue. However, thinking one step ahead of Hackers and attackers will certainly provide solution to safeguard Cloud services. The paper refers to Simulation of "**Data Security"** in Cloud Computing.

***Index Terms* – Digital Wrapping, Security Parameter, Security Level.**

I. INTRODUCTION

Cybercrime is a global problem dominating the world in Cyber angle. Crypto jacking threats are taking exponential rise in Cloud Computing, breaching the data security aspect with repeated attacks like Ransomware are on the rise. Attack techniques of Hackers evolving since Cloud Computing has become a way of life. There is a never-ending scope to counter such attacks on a real time basis to safeguard our systems. Common threats are Data loss, Insider threats etc.

1.1 Digital Wrapping in DWDM

Today's era demands high Bandwidth wherein a concept of DWDM technology consisting of digitally wrapped signals is being implemented. In order to safeguard such a huge architecture, security of data is of prime importance. Digital Wrapping starts with a client signal mapped into the OPU payload, with the OPU overhead providing information on the type of signal mapped into the payload and the mapping structure. Thereafter, ODU overhead adds optical path-level monitoring, alarm indication signals, automatic protection switching bytes and embedded data communications channels (GCC1/GCC2). The ODU is the basic payload that is electronically groomed and switched within an OTN network. The OTU overhead adds bytes to provide optical section layer PM, alarm indication, and the GCC0 data communications channel. The OTU represents a physical optical interface or port, such as OTU1 (2.5 Gbps), OTU2 (10 Gbps), OTU3 (40 Gbps) and OTU4 (100 Gbps). High Bandwidth is achieved by combining these Digitally wrapped signals and transmitting it on a Single fiber thus saving cost in Physical layer [1], [2].

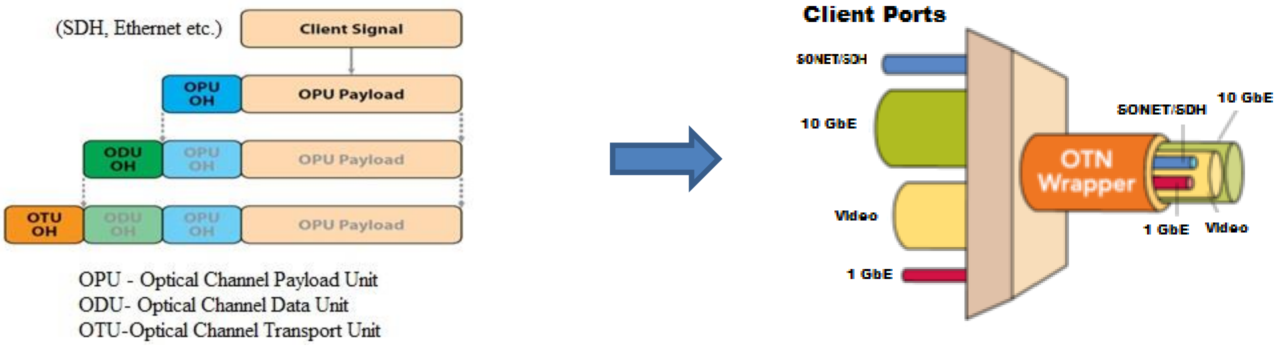

Figure 1.1: Digital Wrapping in DWDM

1.2 Modus operandi of Hacker

The aim of Hacker is to gain ascendancy into the system which could facilitate in financial gain. Various tactics followed by the attacker are collect information on Geographical locations by Geotagging, obtain call details through True caller, get root access of Mobile/ PC, obtain financial details of user etc.

II. CLOUD BASICS

2.1 Cloud Characteristics

IT resources are delivered to the users as per their demands. Cloud computing provides solutions of higher security with lower cost. Cloud provides flexibility in various characteristics like On-demand self-services, Broad network access, Rapid elasticity, Resource pooling, Measured service etc. [3].

2.2 Cloud Service Models

SaaS, PaaS and IaaS are three main Cloud service models offered to users. SaaS provides a complete software solution that you purchase on **a** pay-as-you-go basis from a cloud service provider. The SaaS applications are also called as Web-based software, on-demand software, or hosted software. PaaS services are hosted in the cloud and where in users simply access through their web browser. A PaaS provider hosts the hardware and software on its own infrastructure. IaaS is a service where infrastructure is provided as outsourcing to enterprises such as networking equipment, devices, database, web servers etc. IaaS service is also known **as** Hardware as a Service. Customers here pay on a per-user basis, typically by the hour, week, or month [3], [4].

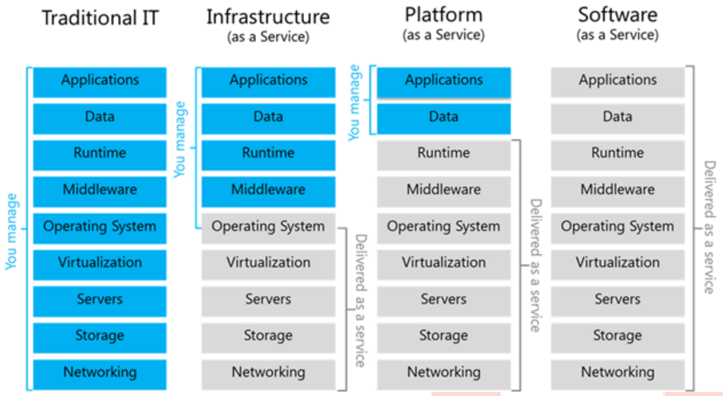

Figure 1.2: Cloud Service Models

2.3 Cloud Deployment Models

There are mainly four cloud deployment models viz Public cloud, Private cloud, Hybrid cloud and Community cloud. In public cloud, anybody can access systems and services and hence, it is less secure. In private cloud, hardware is not shared and refers to the ability to access systems and services within a given organization. In hybrid cloud, organizations can move data and applications between different clouds using a combination of two or more cloud deployment methods, depending on their needs. In community cloud, systems and services are accessed by a group of organizations [4].

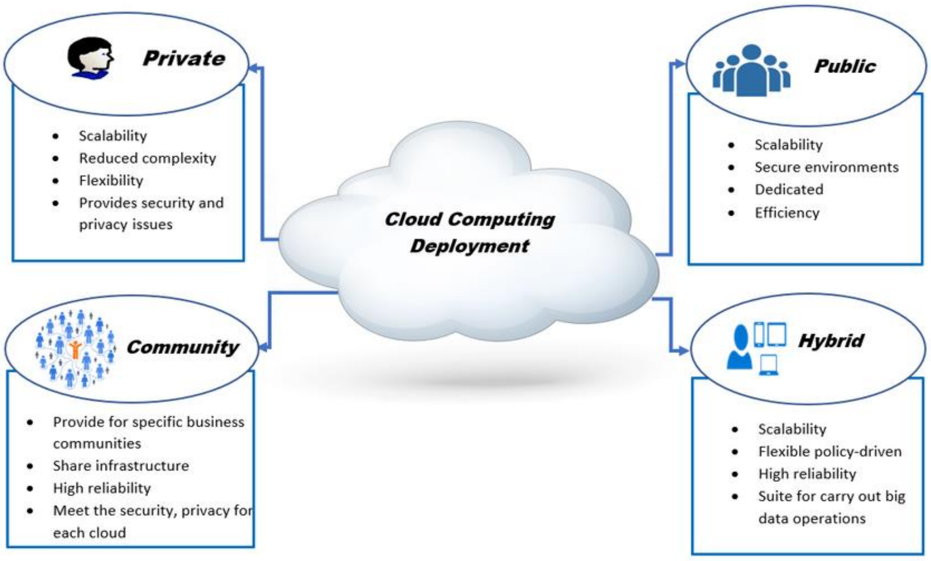

Figure 1.3: Cloud Deployment Models

III. Cloud Security Threats & Attacks [5], [6]

3.1 Data Breach/ Loss

Data breach may result due to deletion, modification and stealing of information without any backup of the existing data and loss of an Encryption keys. Data loss may result due to absence of authorization, authentication, weak encryption algorithms, access control, absence of disaster recovery etc.

3.2 Abuse and Nefarious use of Cloud services

This kind of threat refers to attackers generating unauthorized access into cloud platform by password cracking, CAPTCHA-solving, initiate dynamic attacks, hosting malign data, Botnet command, DDoS, etc.

3.3 Inadequate Infrastructure Design and Planning

Cloud service providers may fail to satisfy the rapid rise due to shortage of resources or weak network design known as inadequate infrastructure design and planning giving rise to network latency.

3.4 Malicious Insiders

Malicious insiders refer to employees, contractors or other business partners having authorized access to cloud resources wherein they compromise the integrity, availability or confidentiality of the organization’s data resulting in loss of productivity, and financial theft.

3.5 Illegal Access to the Cloud

Confidential and critical data is compromised due to weak authentication and authorization controls leading to unlawful access of data.

3.6 Isolation Failure

Due to failure in compartmentalization of routing, reputation, storage, memory etc., hackers gain illegal access to the data.

3.7 Network Management

Network congestion, misconnection, misconfiguration etc., affects services and security due to poor network management.

3.8 Authentication Attacks

Attackers gain unauthorized access to cloud computing systems due to weak authentication and limitations of one-factor authentication.

3.9 Loss of Encryption Keys

Attackers intrude into the systems due to poor management of keys and poor key generation techniques resulting in loss of Encryption keys.

3.10 Denial of Service (DoS) attack

The attack occurs due to flooding of traffic into the system. Large organizations such as banking sector, government sector, etc. are affected wherein huge amount of data is lost due to DoS attacks.

IV. Research Methodology

MATLAB, a popular programming language for numerical computing and data analysis, providing various built-in functions and tools is used for implementing data security measures in cloud computing. It's important to note that while MATLAB provides tools and functions for data security, it's also essential to follow best practices for data security, such as using strong encryption algorithms, properly managing encryption keys, and implementing multifactor authentication etc.

4.1 Simulation Procedure

The MATLAB code is simulated for a cloud environment with 100 servers and 1,00,00,00,000 clients using the cloud. The simulation runs for 100 seconds, and the data stored on the cloud is generated randomly. The security level of the data is calculated based on the average value of the data stored on each server. If the security level is below a threshold i.e.0.5, noise is added to the data to increase the security level [7], [8]. Finally, average security level over time is plotted to get results.

4.2 Mathematical Equations

Initially, parameters i.e. number of servers, number of clients and time for simulation are defined for simulation. Security parameter Alpha is defined between 0 and 1. The formula for Security parameter is as follows;

$$\text{alpha} = 0.5 \qquad (4.1)$$

Thereafter, random data is generated and stored on cloud. The formula for generation of random data is as follows;

$$\text{data} = \text{rand}(n, T) \qquad (4.2)$$

Simulation for defined time duration is carried out for data stored on cloud. Security level of data is calculated based on the equation given below;

security_level = alpha*sum(data(:,t))/n (4.3)

If the security level is too low then noise is added to the data. The formula for addition of noise is as follows;

data(:,t) = data(:,t) + noise (4.4)

Finally, average security level is calculated for each client based on formula given below;

avg_security=mean(data,1) (4.5)

V. Results and discussion

Considering 100 servers and 1,00,00,00,000 clients in cloud environment, results are plotted by varying Security parameter from 0.5 to 0.9. Thereafter, keeping the Security parameter as 0.9 constant with 1,00,00,00,000 clients, results are plotted by increasing number of Servers in cloud environment.

5.1 Improvisation by increasing Security parameter

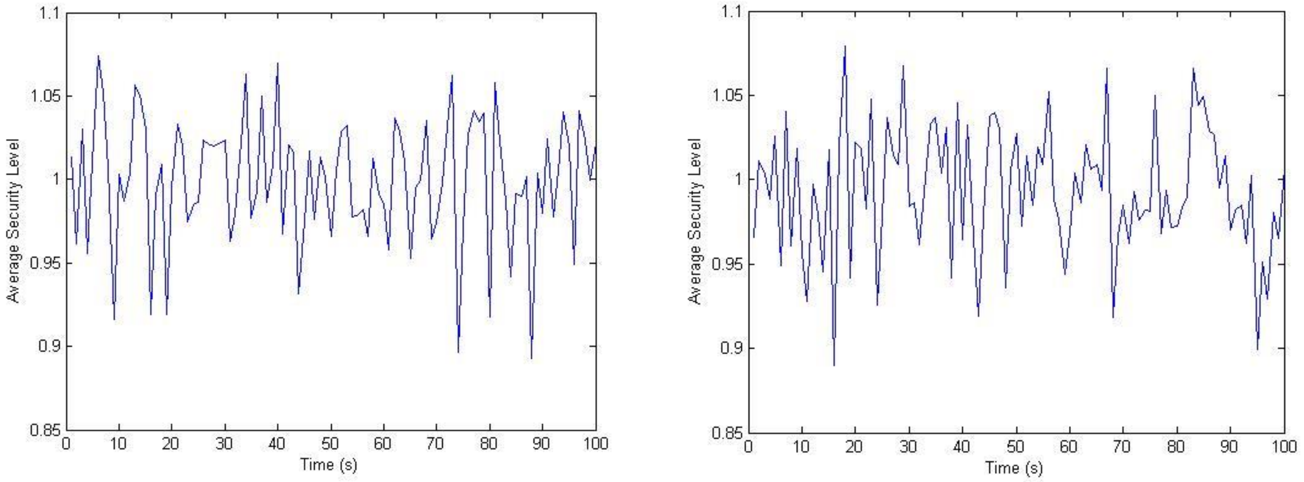

Figure 5.1: Average Security level vs Time for Security parameter 0.5

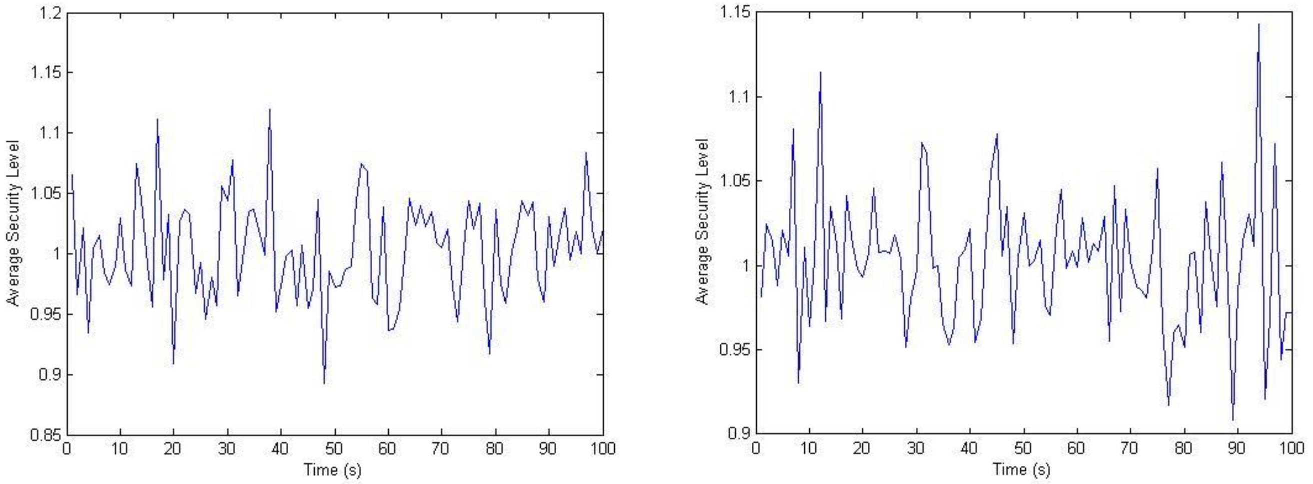

Figure 5.2: Average Security level vs Time for Security parameter 0.7

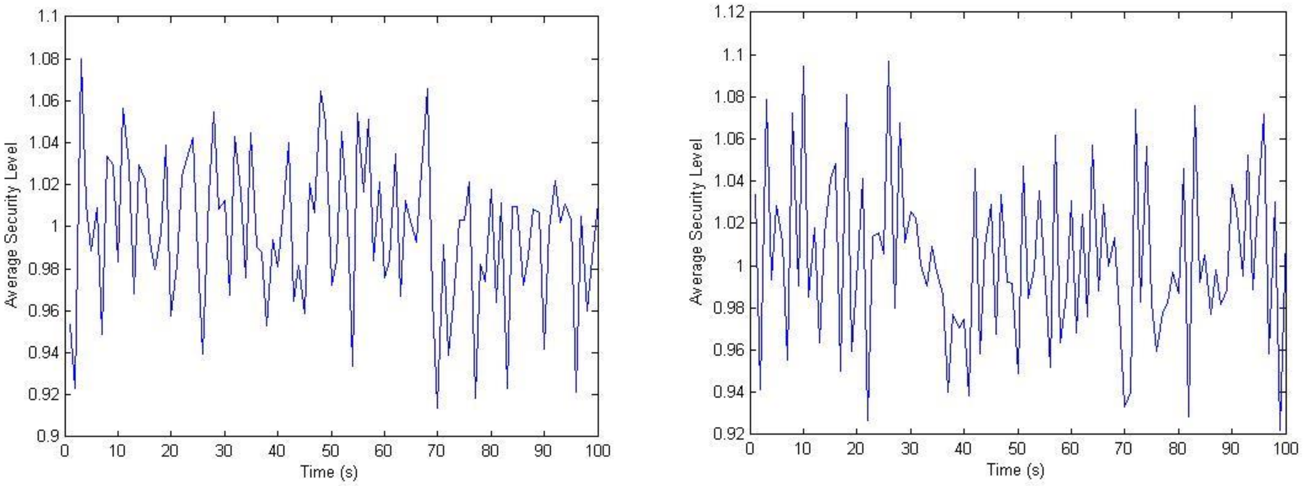

Figure 5.3: Average Security level vs Time for Security parameter 0.9

5.2 Improvisation by increasing number of Servers in Cloud

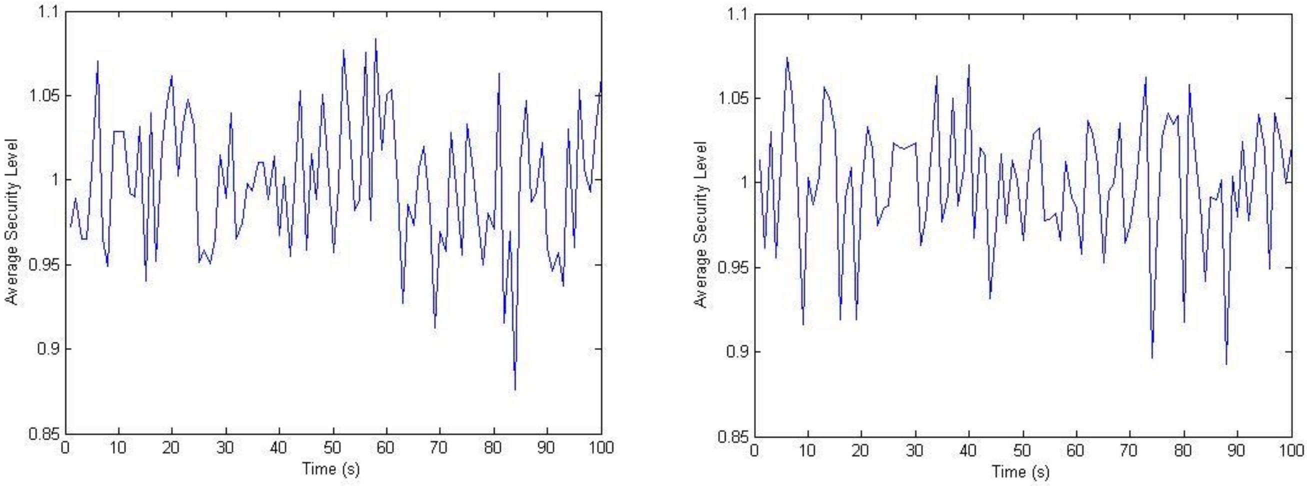

Figure 5.4: Average Security level vs Time with 100 Servers

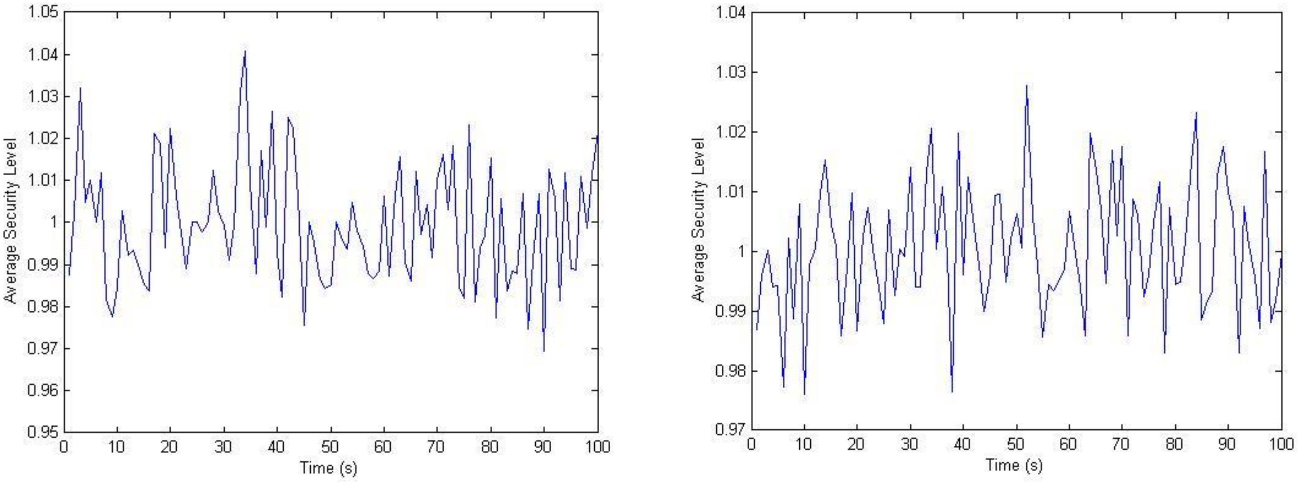

Figure 5.5: Average Security level vs Time with 1000 Servers

Initially, the MATLAB code is simulated by taking Security parameter as 0.5. Subsequently, various simulations are carried out by increasing Security parameter up to 0.9. It is seen that the Security level of data corresponds to Security parameter. The more the Security parameter the greater the Security level of data can be achieved. Moreover, improvisation is also carried out with respect to number of servers on Cloud for 1,00,00,00,000 Clients. The Security level of data increases as the number of servers increase in Cloud environment. Cloud Computing is expanding day-by-day in the market and will see brighter and more secure Cloud future.

REFERENCES

[1] Qiong Wang, Gao Ying, “OTN for the Future Transmission Network”, Electronic and Information school, Liaoning University of Technology, Liaoning Jinzhou, China.

[2] Hong Ju Kim, Hyun Jae Lee, Bheom Soon Joo, Jong Hyun Lee, “Modular and Flexible Architecture od Wavelength-OTN-Packet Converged Platform”, Optical Internet Research Department, Electronics and Telecommunication Research Institute, Daejeon, Korea.

[3] Zaigham Mahmood, “Cloud Computing: Characteristics and Deployment Approaches”, School of Computing & Mathematics, University of Derby, UK.

[4] Amit Gyandev Prajapati, Shankarlal Jayantilal Sharma, Vishal Sahabrao Badgujar, “All About Cloud: A Systematic Survey”, Department of Information Technology, A P Shah Institute of Technology, Thane, India.

[5] Manoj Kumar Sasubilli, Venkateswarlu R, “Cloud Computing Security Challenges, Threats and Vulnerabilities”, 6th International Conference on Inventive Computation Technologies (ICICT), Jan 2021.

[6] Aditi Patel, Nisarg Shah, Dipak Ramoliya, Amit Nayak, “A detailed review of Cloud Security: Issues, Threats & Attacks”, 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA-2020).

[7] Kato Mivule, “Utilizing Noise Addition for Data Privacy, an Overview”, Computer Science Department, Bowie State University.

[8] Prachee Atmapoojya, Utkarsh Saini, Rohit Patidar, Rishabh Gupta, Sakshi Chhabra, Ashutosh Kumar Singh “Data Privacy Preservation Model using Noise Concept in Cloud”, International Journal of Engineering Research & Technology (IJERT), Vol. 11 Issue 03, March-2022.