#### JNANASANGAMA, BELGAVI -590018

Seminar Report On

#### “Data Fragmentation Analytics”

Submitted in partial fulfillment for the award of degree of MASTER OF COMPUTER APPLICATIONS

Submitted by

**PRABHANJAN SHRINIVAS PURANIK**

**USN No: 1IH19MCA11**

Under the Guidance of

### Prof. A.G.Vishwanath



**BANGALORE INSTITUTE OF TECHNOLOGY K R ROAD, V V PURA, BENGALURU – 560004 Department of MASTER OF COMPUTER APPLICATIONS**

### K R ROAD, V V PURA, BENGALURU – 560004

**Department of MASTER OF COMPUTER APPLICATIONS**



**CERTIFICATE**

This is to certify that, the Seminar on **Fragmentation analytics for Data** carried out by **Mr**. **PRABHANJAN SHRINIVAS PURANIK** with (USN: **1IH19MCA11**), of VI Semester MCA, **Bangalore Institute of Technology** is a bonafide work done in partial fulfilment of the Post graduate program of Visvesvaraya Technological University, Belagavi, during the academic year 2022.

**A G Vishwanath** Asst. Professor, Dept. of MCA BIT, Bengaluru.

**Prof. A M Shivaram** Asst. Professor, HOD, Dept. of MCA BIT, Bengaluru.



## Vision

**To establish and develop the Institute as a center of higher learning, ever abreast with expanding horizon of knowledge in the field of engineering and technology, with entrepreneurial thinking, leadership excellence for life-long success and solve societal problem**.

## Mission

### Provide high quality education in the engineering disciplines from the undergraduate through doctoral levels with creative academic and professional programs.

* **Develop the Institute as a leader in Science, Engineering, Technology and management, Research and apply knowledge for the benefit of society.**

### Establish mutual beneficial partnerships with industry, alumni, local, state and central governments by public service assistance and collaborative research.

* **Inculcate personality development through sports, cultural and extracurricular activities and engage in the social, economic and professional challenges.**

# Department of Master of Computer Applications



## Vision

**To transform young graduates into skilled professionals to meet Industrial and Societal needs.**

## Mission

### To enhance the Teaching learning process to meet quality education in the field of Computer applications

* **To impart the knowledge in current technologies to meet the industrial needs**

### To inculcate ethical values and leadership qualities for the betterment of society

**PEO’s**

### PEO1: To develop quality application software with innovative ideas to meet the industrial requirements

* **PEO2: To imbibe the current technologies and to adopt in computing profession as per the changing needs**
* **PEO3: To progress in their career with leadership qualities and ethical values that enhances self and societal growth**

## Program Outcomes (POs)

|  |  |
| --- | --- |
| **PO1** | **Apply knowledge of computing fundamentals, computing specialization, mathematics and domain knowledge appropriate for conceptualization of computing models as per the requirement** |
| **PO2** | **Identify, analyze systematize and solve computer application related problems using the principles of mathematics, computing sciences and relevant domain knowledge** |
| **PO3** | **Design, develop and evaluate software solution to solve complex problem with societal and environment concern.** |
| **PO4** | **Conduct investigations of complex computing problems using research based methods to provide valid conclusions.** |
| **PO5** | **Select, adapt and apply appropriate techniques, resources and modern tools for complex computing activities** |
| **PO6** | **Understand ethical responsibilities and cyber regulations to perform professionally.** |
| **PO7** | **Involve in independent learning for continual development as computing professionals** |
| **PO8** | **Apply and demonstrate the computing and management principle to manage projects in multidisciplinary environment as an individual or as a member in team.** |
| **PO9** | **Comprehend and write effective reports and make quality presentations about complex computing activities** |
| **PO10** | **Understand and assess the impact of computing practices and socio- environmental concern** |
| **PO11** | **Work as an individual and a member or a leader in multidisciplinary environment** |
| **PO12** | **Identify business opportunity and pursue using innovative ideas to create value and wealth for the betterment of society** |

**ACKNOWLEDGEMENT**

The satisfaction and happiness that accompany the successful completion of any task would be done but incomplete without mention of the people who made it possible, whose constant guidance and encouragement crowned our efforts with success.

I thank my parents for supporting me throughout the completion of the project

I consider this a privilege to express our gratitude to **Dr. Aswath M. U**, Principal, Bangalore Institute of Technology, Bengaluru who provided us all facilities needed for completing this project.

I offer my sincere thanks to **Prof. A.M. Shivaram**, HOD, Master of Computer Applications, Bangalore Institute of Technology, Bengaluru for his encouragement and guidance throughout my training.

It is my privilege to express my sincerest regards to my internal guide, **A G Vishwanath**, for his valuable inputs, guidance, encouragement, whole-hearted cooperation for making the report.

I thank all of my teaching and non-teaching staff of the department of MCA, who has helped me in completing my mini project successfully during this pandemic situation.

**PRABHANJAN SHRINIVAS PURANIK**

**(1IH19MCA11)**

## CONTENTS

|  |  |  |
| --- | --- | --- |
| **SL NO.** | **TOPICS** | **PAGE NO.** |
| 1 | TITLE | 1 |
|  | INTRODUCTION | 2 |
|  | 1.1 DEFINITION | 2 |
|  | 1.2 Why Cloud security is Important | 2-4 |
|  | 1.3 cloud service type | 4-6 |
|  | 1.4 Advantages of Cloud Security | 7 |
|  | 1.5 Disadvantages of Cloud Security | 8 |
| 2 | DESCRIPTION | 4 |
|  | 2.1 HISTORY OF ARTIFICIAL INTELLIGENCE | 4-5 |
|  | 2.2 APPLICATIONS OF ARTIFICIAL INTELLIGENCE | 6-8 |
| 3 | RESEARCH PAPER | 9-14 |
| 4 | CONCLUSION | 15 |
| 5 | REFERENCE | 16 |

**Fragmentation analytics for Data**

## CHAPTER 1 INTRODUCTION

* 1. **Definition:** Cloud security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business. The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and provider
  2. **Why is cloud security important?**

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

Cloud security offers many benefits, including:

**Centralized security**: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with [**shadow IT**](https://www.forcepoint.com/cyber-edu/shadow-it) or [**BYOD**](https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod). Managing these entities centrally enhances traffic analysis and [**web filtering**](https://www.forcepoint.com/product/url-filtering), streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.

**Reduced costs**: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

**Reduced Administration**: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.

**Reliability**: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

More and more organizations are realizing the many business benefits of moving their systems to the cloud. Cloud computing allows organizations to operate at scale, reduce technology costs and use agile systems that give them the competitive edge. However, it is essential that organizations have complete confidence in their cloud computing security and that all data, systems and applications are protected from data theft, leakage, corruption and deletion.

All cloud models are susceptible to threats. IT departments are naturally cautious about moving mission-critical systems to the cloud and it is essential the right security provisions are in place, whether you are running a native cloud, hybrid or on-premise environment. Cloud security offers all the functionality of traditional IT security, and allows businesses to harness the many advantages of cloud computing while remaining secure and also ensure that data privacy and compliance requirements are met.

**Secure Data in the cloud:** Cloud data security becomes increasingly important as we move our devices, data centers, business processes, and more to the cloud. Ensuring quality cloud data security is achieved through comprehensive security policies, an organizational culture of security, and cloud security solutions.

Selecting the right cloud security solution for your business is imperative if you want to get the best from the cloud and ensure your organization is protected from unauthorized access, data breaches and other threats. [**Forcepoint Cloud Access Security Broker (CASB)**](https://www.forcepoint.com/product/casb-cloud-access-security-broker) is a complete cloud security solution that protects cloud apps and cloud data, prevents compromised accounts and allows you to set security policies on a per-device basis.

**1.3 Cloud service types** are offered by third-party providers as modules used to create the cloud environment. Depending on the type of service, you may manage a different degree of the components within the service:

* **The core of any third-party cloud service** involves the provider managing the physical network, data storage, data servers, and computer virtualization frameworks. The service is stored on the provider’s servers and virtualized via their internally managed network to be delivered to clients to be accessed remotely. This offloads hardware and other infrastructure costs to give clients access to their computing needs from anywhere via internet connectivity.
* **Software-as-a-Service (SaaS)** cloud services provide clients access to applications that are purely hosted and run on the provider's servers. Providers manage the applications, data, runtime, middleware, and operating system. Clients are only tasked with getting their applications. SaaS examples include Google Drive, Slack, Salesforce, Microsoft 365, Cisco WebEx, Evernote.
* **Platform-as-a-Service** cloud services provide clients a host for developing their own applications, which are run within a client’s own “sandboxed” space on provider servers. Providers manage the runtime, middleware, operating system. Clients are tasked with managing their applications, data, user access, end-user devices, and end-user networks. PaaS examples include Google App Engine, Windows Azure.
* **Infrastructure-as-a-Service (IaaS)** cloud services offer clients the hardware and remote connectivity frameworks to house the bulk of their computing, down to the operating system. Providers only manage core cloud services. Clients are tasked with securing all that gets stacked atop an operating system, including applications, data, runtimes, middleware, and the OS itself. In addition, clients need to manage user access, end-user devices, and end-user networks. IaaS examples include Microsoft Azure, Google Compute Engine (GCE), Amazon Web Services (AWS).

**1.3.2. Cloud environments** are deployment models in which one or more cloud services create a system for the end-users and organizations. These segments the management responsibilities — including security — between clients and providers.

The currently used cloud environments are:

* **Public** **cloud environments** are composed of multi-tenant cloud services where a client shares a provider’s servers with other clients, like an office building or coworking space. These are third-party services run by the provider to give clients access via the web.
* **Private** **third-party cloud environments** are based on the use of a cloud service that provides the client with exclusive use of their own cloud. These single-tenant environments are normally owned, managed, and operated offsite by an external provider.
* **Private in-house cloud environments** also composed of single-tenant cloud service servers but operated from their own private data center. In this case, this cloud environment is run by the business themselves to allow full configuration and setup of every element.
* **Multi-cloud environments** include the use of two or more cloud services from separate providers. These can be any blend of public and/or private cloud services.
* **Hybrid** **cloud environments** consist of using a blend of private third-party cloud and/or onsite private cloud data center with one or more public clouds.

By framing it from this perspective, we can understand that cloud-based security can be a bit different based on the type of cloud space users are working in. But the effects are felt by both individual and organizational clients alike.

## 1.3.3. How does cloud security work?

Every cloud security measure works to accomplish one or more of the following:

* Enable data recovery in case of data loss
* Protect storage and networks against malicious data theft
* Deter human error or negligence that causes data leaks
* Reduce the impact of any data or system compromise

**Data security** is an aspect of cloud security that involves the technical end of threat prevention. Tools and technologies allow providers and clients to insert barriers between the access and visibility of sensitive data. Among these, encryption is one of the most powerful tools available. Encryption scrambles your data so that it's only readable by someone who has the encryption key. If your data is lost or stolen, it will be effectively unreadable and meaningless. Data transit protections like virtual private networks (VPNs) are also emphasized in cloud networks.

**Identity and access management (IAM)** pertains to the accessibility privileges offered to user accounts. Managing authentication and authorization of user accounts also apply here. Access controls are pivotal to restrict users — both legitimate and malicious — from entering and compromising sensitive data and systems. [Password management](https://www.kaspersky.com/password-manager), multi-factor authentication, and other methods fall in the scope of IAM.

**Governance** focuses on policies for threat prevention, detection, and mitigation. With SMB and enterprises, aspects like threat intel can help with tracking and prioritizing threats to keep essential systems guarded carefully. However, even individual cloud clients could benefit from valuing safe user behavior policies and training. These apply mostly in organizational environments, but rules for safe use and response to threats can be helpful to any user.

**Data retention (DR) and business continuity (BC) planning** involve technical disaster recovery measures in case of data loss. Central to any DR and BC plan are methods for data redundancy such as backups. Additionally, having technical systems for ensuring uninterrupted operations can help. Frameworks for testing the validity of backups and detailed employee recovery instructions are just as valuable for a thorough BC plan.

**Legal compliance** revolves around protecting user privacy as set by legislative bodies. Governments have taken up the importance of protecting private user information from being exploited for profit. As such, organizations must follow regulations to abide by these policies. One approach is the use of data masking, which obscures identity within data via encryption methods

.

### Advantages of Cloud Security

Following are some main advantages of Cloud Security:

1. **Efficient recovery –**  
   Cloud computing conveys quicker and more exact recoveries of applications and information. With less downtime, it is foremost productive recuperation arrange.
2. **Openness –**  
   Get to your data wherever, at whatever point. A Web cloud framework increases benefit and commerce capability by ensuring that your application is constantly accessible. This takes under consideration basic participation and sharing between clients in different regions.
3. **No material required –**  
   Since everything will be encouraged within cloud, a physical stockpiling community is never once more critical. In any case, it might justify considering a support in case of a calamity that seem moderate down your business’ effectiveness.
4. **Preferred position –**  
   Straightforward execution – Cloud encouraging grants an organization to keep up comparative applications and trade shapes without managing with specialized parts of back-end. Easily managed over Web, a cloud establishment is viably and quickly accessible to organizations.
5. **Cost per head –**  
   Advancement overhead is kept to a base with cloud encouraging organizations, allowing organizations to utilize additional time and resources to make strides trade system. Versatility for improvement. The cloud is successfully versatile with objective that organizations can include or subtract resources as demonstrated by their necessities. As organizations create, their system will development with them.

### Disadvantages of Artificial Intelligence

Every technology has some disadvantages, and the same goes for Artificial intelligence. Being so advantageous technology still, it has some disadvantages which we need to keep in our mind while creating an AI system. Following are the disadvantages of AI:

1. **Bandwidth issues –**  
   For perfect execution, clients need to arrange in like manner and not pack expansive sums of servers and capacity gadgets into a little set of information centres.
2. **Without excess –**  
   A cloud server is not one or another overabundance nor reinforced. Since development can bomb to a awesome degree, go without from getting seared by buying an overabundance course of action. Whereas this can be an additional cost, much of time it is defended, in spite of all inconvenience.
3. **Data transfer capacity issues –**  
   For idealize execution, clients ought to plan moreover and not gather colossal amounts of servers and capacity contraptions in a small course of action of server ranches.
4. **More control –**  
   At the point once you move organizations to cloud, you move your data and information. For organizations with insides IT staff, they won’t have choice to bargain with issues all alone. Be that because it may, Stratosphere Systems has an all day, each day live helpline that can address any issue right absent.
5. **No Redundancy –**  
   A cloud server isn’t excess nor is it supported up. As innovation may fall flat here and there, maintain a strategic distance from getting burned by obtaining a excess arrange. In spite of fact that it is an additional taken a toll, in most cases it’ll be well worth it.

## CHAPTER 2 DESCRIPTION

### Data Fragmentation using Different methods

Artificial Intelligence is not a new word and not a new technology for researchers. This technology is much older than you would imagine. Even there are the myths of Mechanical men in Ancient Greek and Egyptian Myths. Following are some milestones in the history of AI which defines the journey from the AI generation to till date development.

**Abstract:**

### Data Fragmentation in Cloud for Optimal Performance and Security that collectively approaches the security and performance issues. In this methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-colouring to prohibit an attacker of guessing the locations of the fragments. Furthermore, this methodology does not rely on the traditional Cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of this methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

**Keyword:** Random number Generation, Deduplication, optimal performance, chunk data, coloring.

**INTRODUCTION:**

Cloud storage propositions an abstraction of unlimited storage space for clients to host data, in a compensation as- you-go way [2]. For instance, a data sharing website, video sharing websites chose to host terabytes of data. In this manner, rather than self-keeping up data centers, endeavors would now be able to redistribute the storage of a mass measure of digitized content to that outsider distributed storage suppliers to spare the budgetary overhead in management of data. To ensure redistribute data clear approach is to apply cryptographic encryption onto touchy data with a lot of encryption keys, yet keeping up and securing such encryption keys will make one more security problem. One explicit issue is files deletion requests.

Cloud storage providers may not totally expel all duplicates files (e.g., Cloud storage providers may make different record reinforcement duplicates and disperse them over the cloud for dependability and customers don't have a clue about the number or even the presence of these reinforcement duplicates) and inevitably have the data uncovered if the encryption keys are obtained unexpectedly, also by mishaps or by harmful assaults. In this manner, we look to accomplish a significant security objective by dividing the data into skimpy pieces and these parts will be put away on various hubs in the cloud.

Fragmentation of data takes place based on the pseudo random number [4], Random numbers are numbers which occur by satisfying two conditions (1) the numbers distributed uniformly within the given interval or set (2) it is unable to predict the successor number by knowing the previous numbers in other words the random numbers have no relation with among them.

From the last many years there are numerous methods are evolved to generate random numbers.Many mathematicians have given few acceptable random generation algorithms.

Let us describe the meaning of random number with the well-known descriptive examples such as rolling a dice, tossing a coin etc. The actual definition of random can be stated as: A set of random number comprises numbers distributed uniformly over all of the probable values and each one is independent of the numbers which are generated already. Random numbers are numbers which occur by satisfying two conditions (1) the numbers distributed uniformly within the given interval or set (2) it is unable to predict the successor number by knowing the previous numbers in other words the random numbers have no relation with among them.

Various sorts of random number generators exist [4] among them are broadly categorized into (i) True and (ii) Pseudo random number generators. In this paper we are using pseudo random number.

In cloud different types of files, with different size will be stored, for dividing such data files there are different techniques are used [8][9]. For instance, the data file fragmentation threshold determined to be created through the file proprietor. The file owner of the file can indicate fragmentation threshold concerning either the number and size or percentage of various fragments [8]. The fragmentation threshold percentage, for example, can direct that individual fragment will be of 5% size of the total size of the file.

On the other hand, the proprietor may produce distinct file encompassing information about size and number of the fragment, for example, the size of fragments one and two is 5,000 and 8,749 Bytes respectively. We contend that the proprietor of the file isn't the one appropriate to produce fragmentation threshold since as a proprietor probably might not be having enough technical acquaintance to predict the number of fragments hence in this paper, we are using unique random number generation algorithm. In the proposed approach care is taken that no fragment contains any useful information.

**System Implementation**

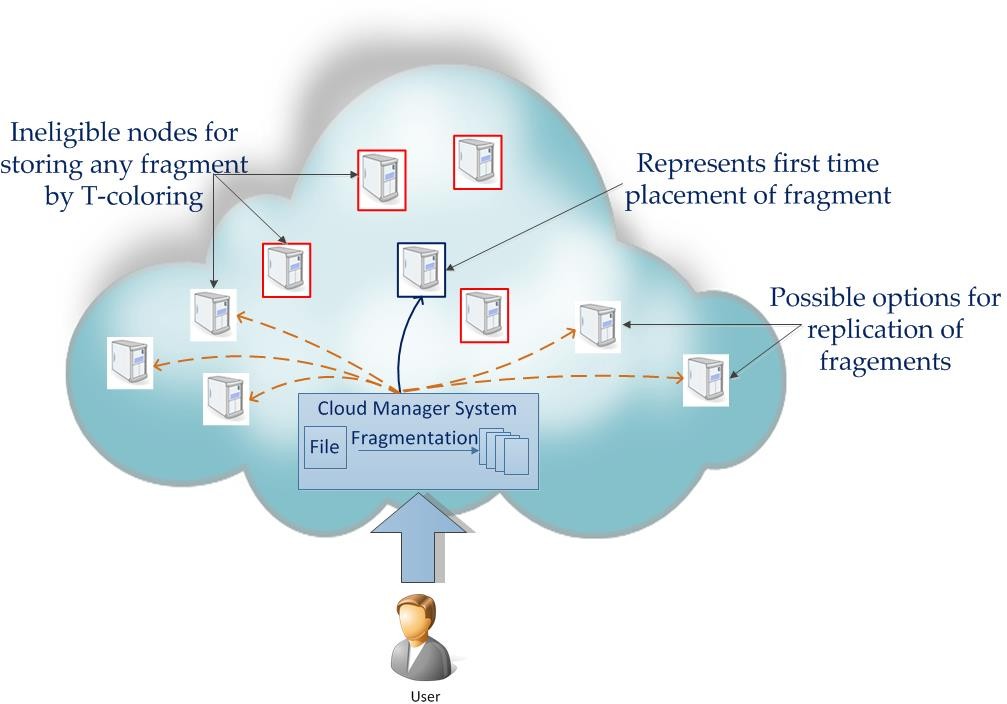
**Develop Cloud Manager System:** The communicational backbone of cloud computing is the Data Centre Network (DCN). We use the Microsoft Azure Cloud Architecture to evaluate the performance of our scheme on legacy as well as state of the art architectures. We developing an Azure cloud-based web application along with corresponding to create multiple nodes in different regions. The managers have all rights about system scalability and update size of the nodes. And also, can manage user activities and restrictions. Users need to register account with valid email address. User need to verifying identities for avoiding Sybil or anonymous attackers. Users can upload there any kind of files and can also Downloadable. User can use cloud like a File System basic.

**T-Coloring and Fragmentation:** In this methodology, we propose not to store the entire file at a single node. This methodology fragments the file and makes use of the cloud for replication. The fragments are distributed such that no node in a cloud holds more than a single fragment, so that even a successful attack on the node leaks no significant information. This methodology uses controlled replication where each of the fragments is replicated only once in the cloud to improve the security. Although, the controlled replication does not improve the retrieval time to the level of full-scale replication, it significantly improves the security.

**Request, Replication and Downloading Files:** In the DROPS methodology, user sends the data file to cloud. The cloud manager system (a user facing server in the cloud that entertains user’s requests) upon receiving the file performs: fragmentation, first cycle of nodes selection and stores one fragment over each of the selected node, and second cycle of nodes selection for fragments replication. The cloud manager keeps record of the fragment placement and is assumed to be a secure entity.

To handle the download request from user, the cloud manager collects all the fragments from the nodes and re-assembles them into a single file. Afterwards, the file is sent to the user. User can download a file on user’s dashboard show option that file can downloadable. And every downloaded file requests and sent requests are stored in cloud manager server. Request will be subject to change during the process of DROPS methodology

**Architecture Diagram:**

Figure 1 represents the Data Fragmentation in Cloud for Optimal Performance and Security. User login to Cloud Manager, gets an account verification for the login. File is upload in Drive where the Cloud Manager fragments the file using T – coloring Approach and the file is replicated. User sends Request for Download, Cloud Manager Downloads the data and sends them to the User.

# PROPERTIES OF GOOD PSEUDO RANDOM NUMBER GENERATORS (PRNGS)

Great PRNGs pass various hypothetical and factual tests. Specifically, a great generator ought to have a significant stretch, implying that there are numerous numbers in the succession before it rehashes. Different factual tests have been proposed for PRNGs, a large number of these depend on goodness-of-fit of the points to the expected distribution in the event that you were examining from a uniform distribution. For instance, the equidistributional test watches that there is a similar number of points in interims of a similar length. This can be tried on the run-test as well as for tuples of numbers produced by means of PRNG [5]. One more test is the run-test which checks groupings of created numbers which are decreasing or increasing or stay over a specific value. The sequences length and number of must display certain conduct.

# METHODOLOGY OF THE ALGORITHM

This algorithm is very much useful in the file fragmentation process, based on the random number generated the file can be divided into fragments equal to the random number.

A basic pseudo random number is generated using linear congruential generator (LCG) but here initial values for the algorithm are changed since the number of fragments for any file are more hence the initial values used in this algorithm are in the range of 100-500 and this value will be used to perform the mod operation in LCG.

# a.Increased Pseudo Random Number Generation Algorithm.

The algorithm of the random number generator is as follows

**Step 1:** Choose the initial value of M for LCG within the range min to max.

**Step2:** Generate random number using LCG

**Step3:** Add the LCG number and random number (selected between min to max) provides new random number.

**Step4:** Perform a XOR operation between new\_num and a 4-digit secret number store it as a new random number.

**Step5:** Ad above formed number to Increased Random number List go to step 2.

**Step6:** Select any number from the Increased Random number List.

# b.Algorithm for Increased Pseudo Random Number

define initial values to A, C, M define PIN

For (0 to max) begin for

X[i+1] ← (A\*Xi +C) mod M Var ← X[i] + Rand\_min\_max () Random[i] ←var XOR PIN

R← Rand\_min\_max (Random[i])

end for

In the fragment Generation Algorithm, the text file will be fragmented. Each fragment’s referred as block in the algorithm. Block size will be calculated based on the random number generated. Input to the algorithm is Lower range and higher range which needs to be calculated since the new random number always within the range of lower and higher range, it is not within the specified range the random number will be discarded.

Once the random number is accepted then the total number of characters in the input file will be calculated on the basis of total file size and random number block size will be determined.

Input: Lr- Lower Range, Hr- Higher Range, F-File.

N ← Compute\_Random();

If Lr<= N>= Hr

begin

Size←sizeofFile(F);

Count←char\_count(F);

Endif;

While (count not equal 0) Begin while

Block=count/n;

For (i is lessthan or equal to block) Begin for

B[j] ← readCharAt(i);

J++;

Create\_Fragment(b[j]);

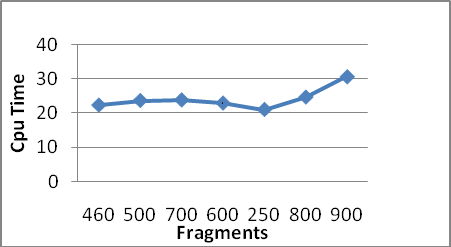
endfor

Count ← count - block; endwhile

output: fragments of the file

# RESULTS AND DISCUSSION

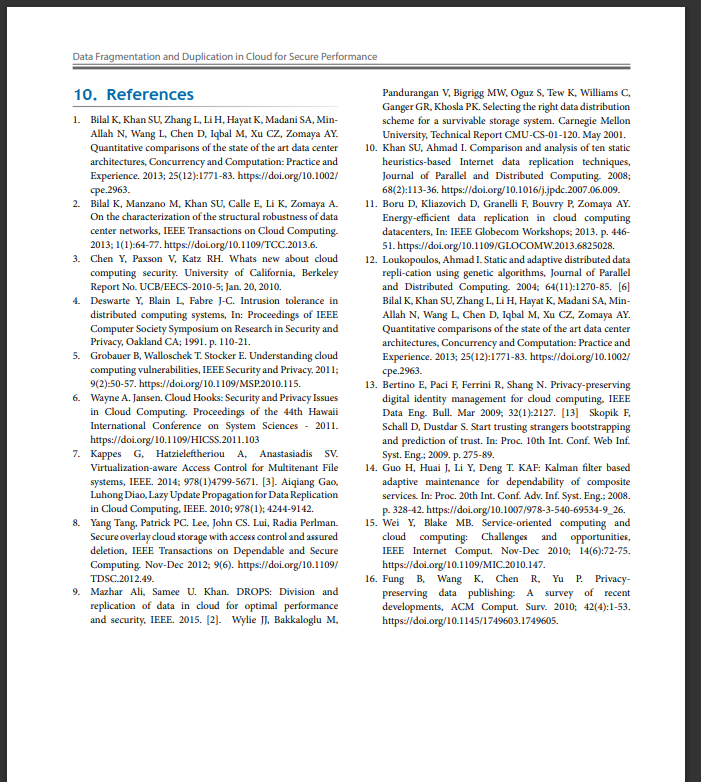
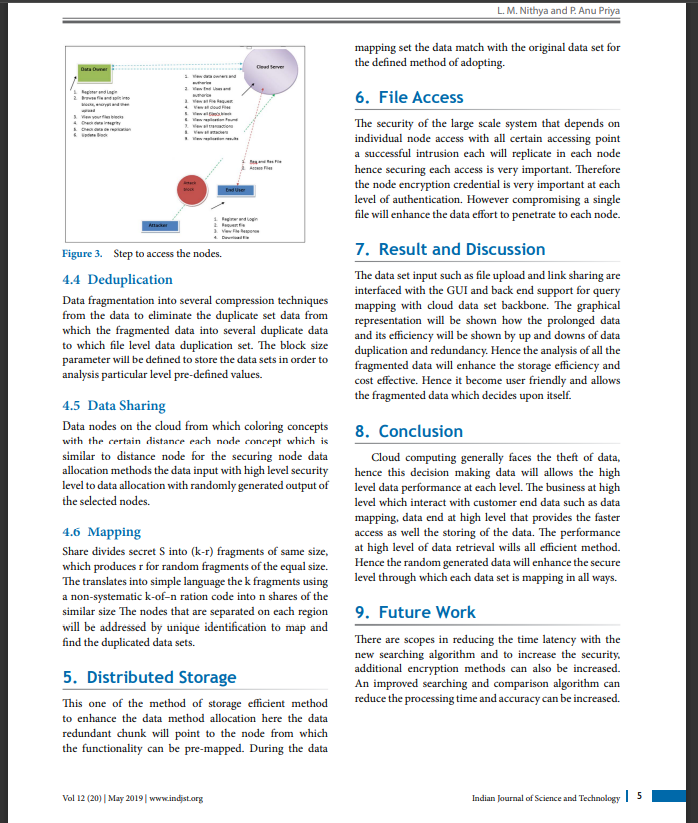
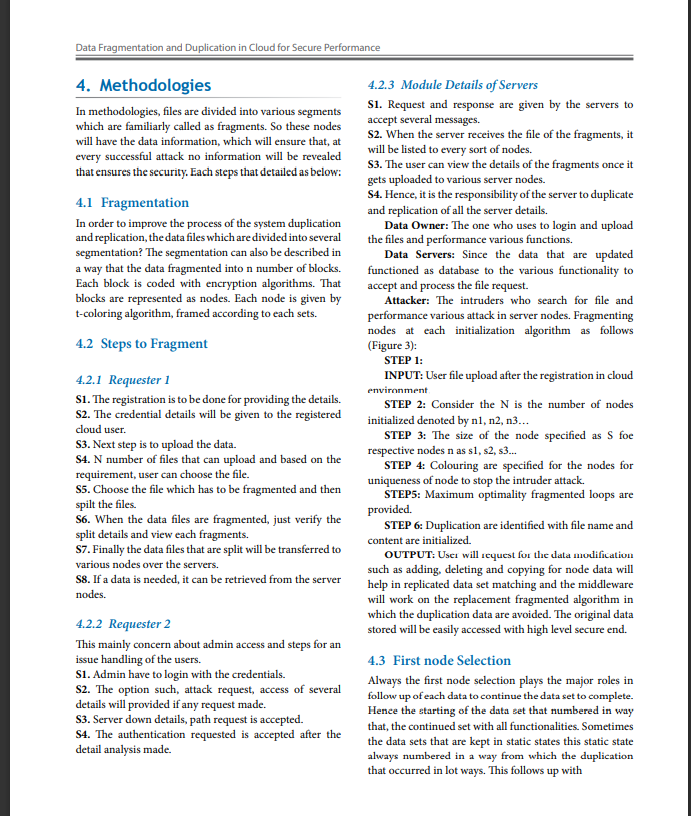
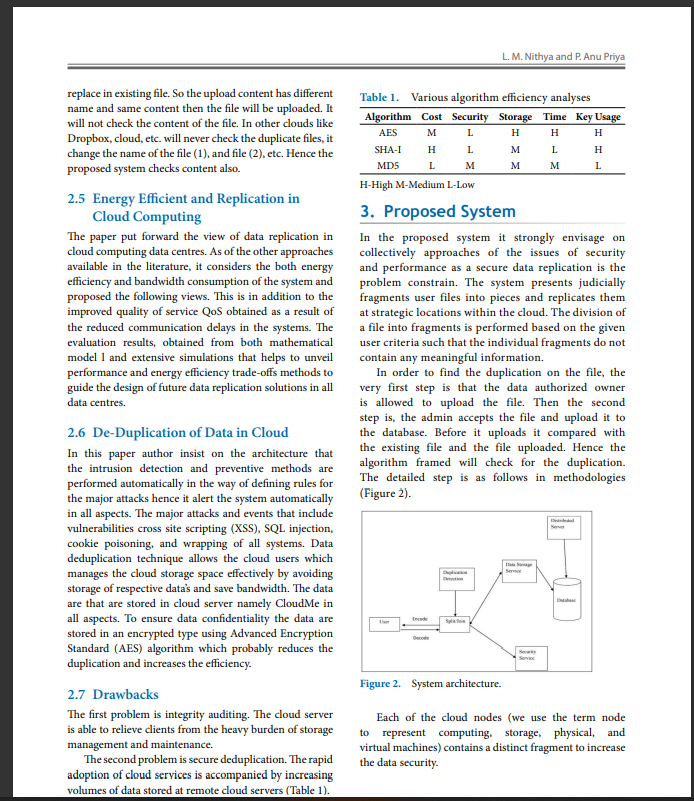
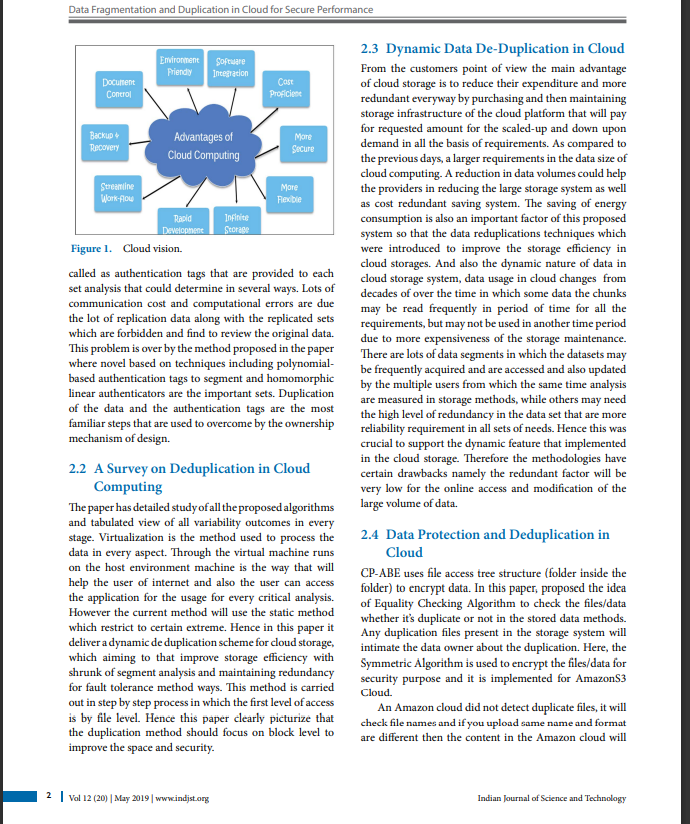
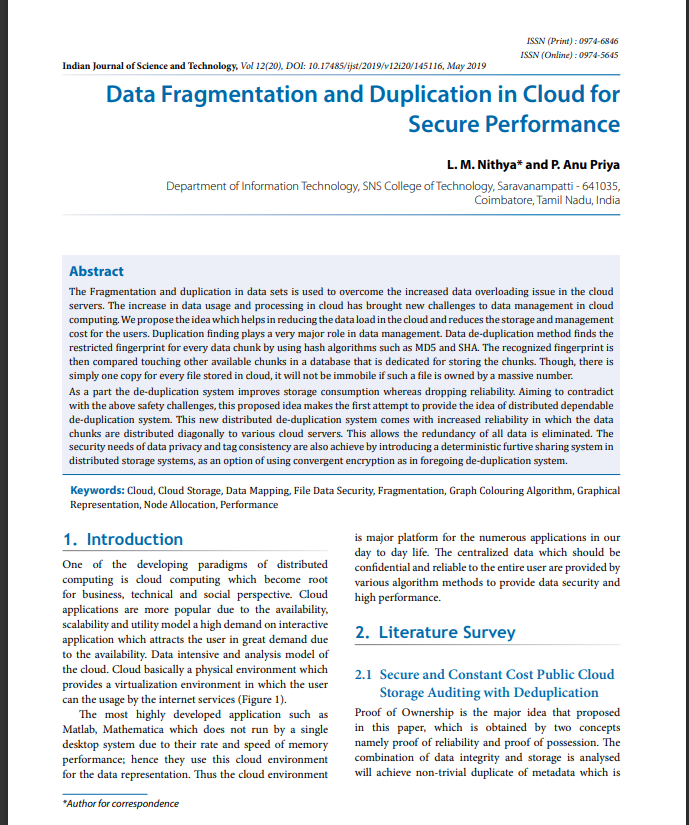
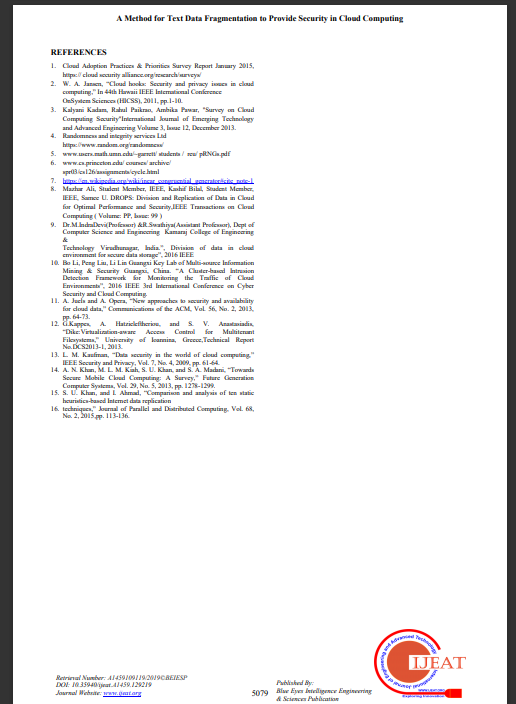
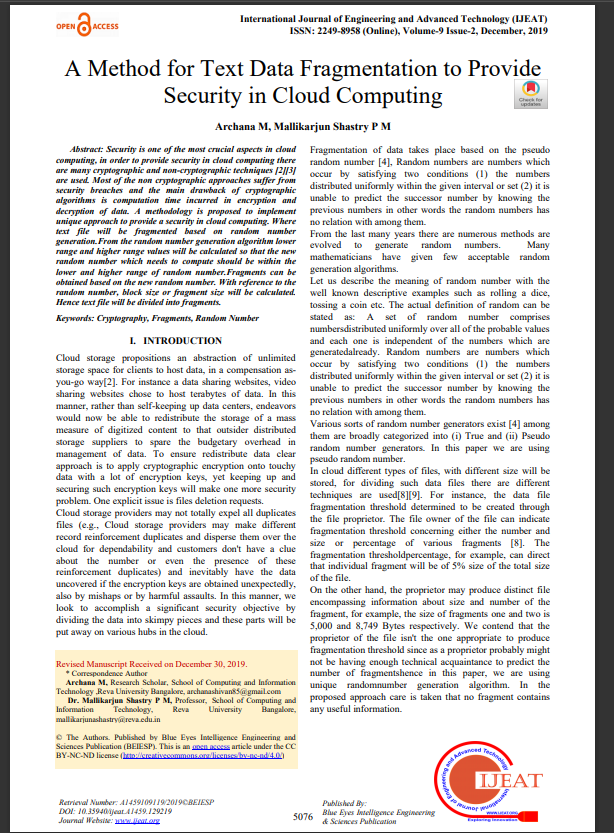
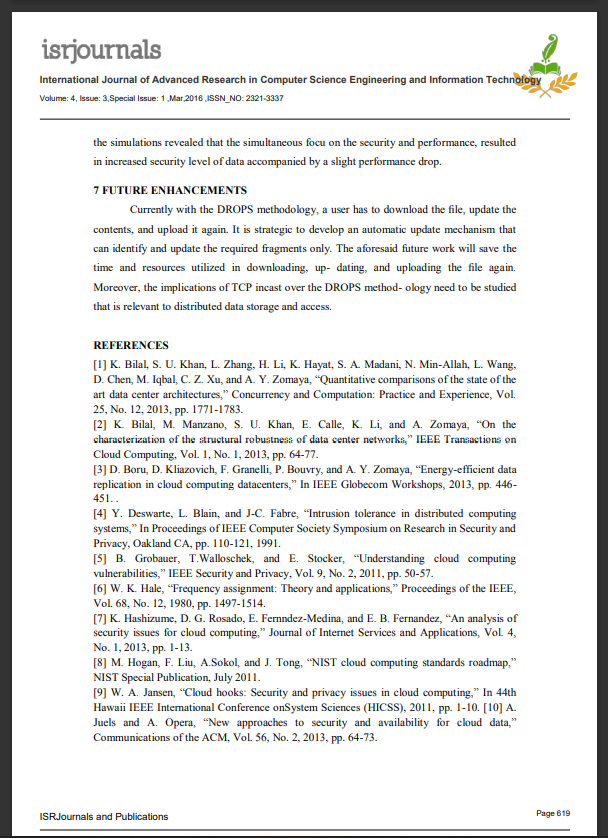
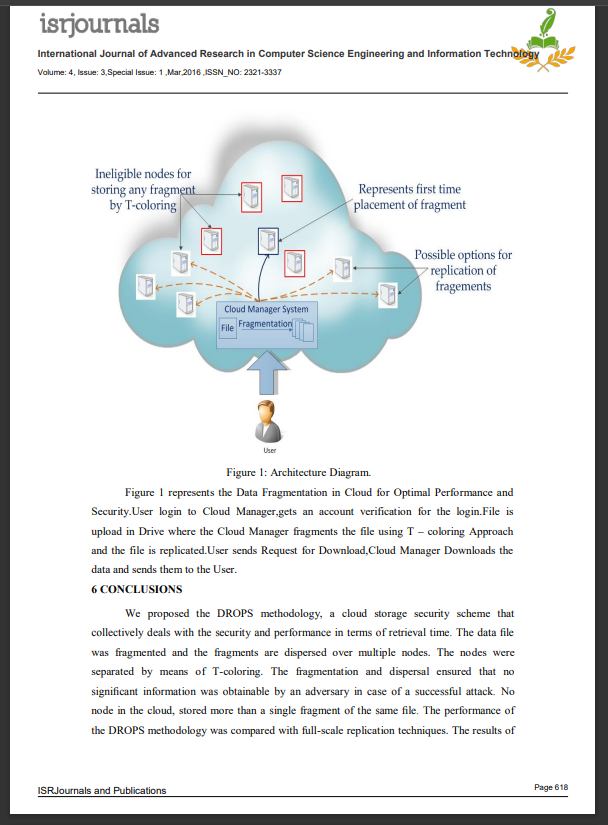
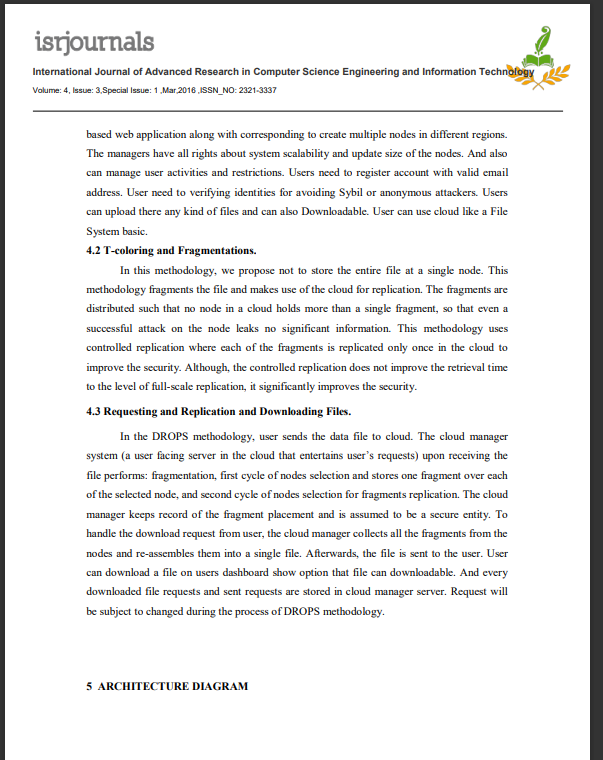
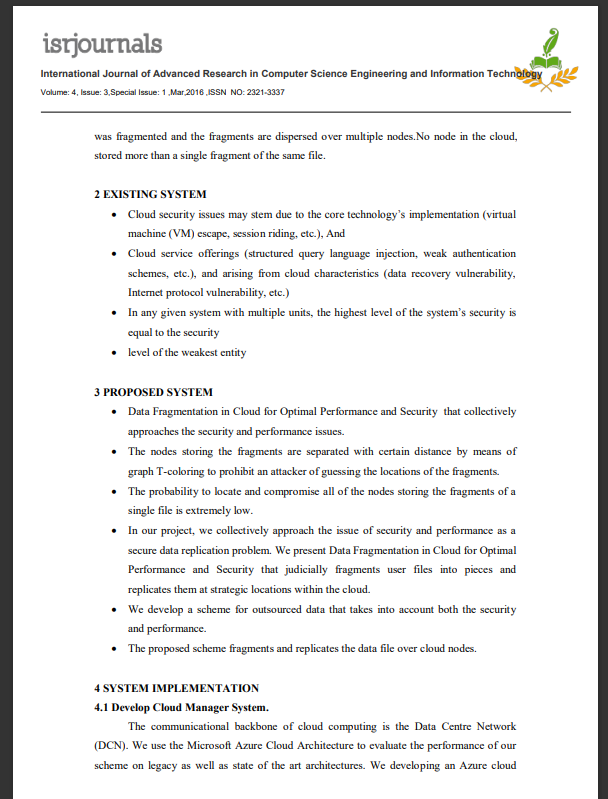
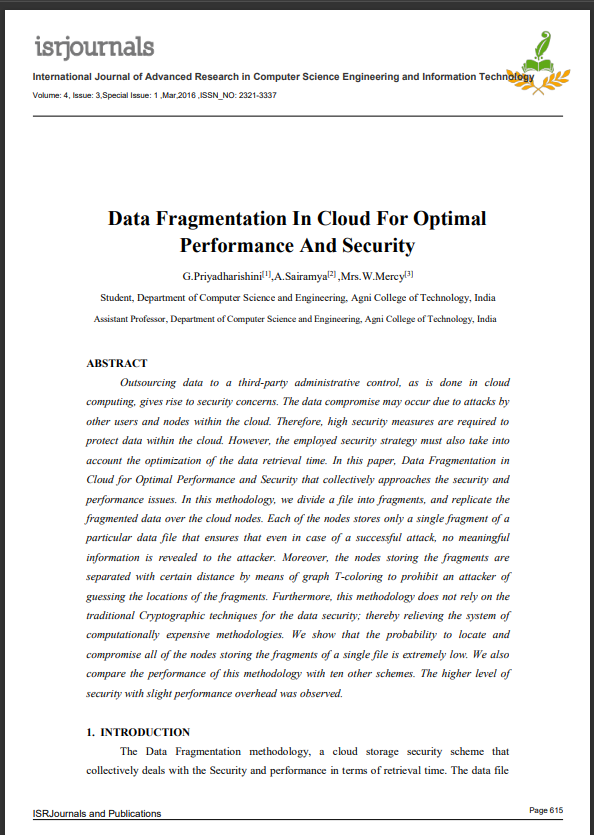
Using java, we have simulated the proposed approach in localhost, where the owner feeds the source file and then in the execution range of random number is calculated. After the calculation of random number range new pseudo random number is generated using above specified algorithm, intern based on the source file block/fragment size will be calculated with reference to the random number, number of fragments will be generated. We have computed the total time taken for generation of random numbers and fragments. In the proposed algorithm 4-digit secret pin is XORed with obtained random which greatly enhances the randomness of a number. We compared the randomness of a number generated from our algorithm with the traditional pseudo random number. With reference to the graphs plotted below shows that randomness of a number is greatly enhanced and also our proposed algorithm consumes very less number off CPU resources for both random number generation and data fragmentation.



# CONCLUSION

In cloud computing, security is a most important burden. There are various techniques to fragment the data into chunks but in most of the technique’s threshold value will be used to fragment the data; some techniques divide the file based on the percentage of the file size. In all these algorithms crucial information such as fragment size is vulnerable. In the proposed algorithm we attempted to generate the fragments basedon the increased pseudo random number. In this methodology each fragment will be of different size. In our proposed methodology information pertained to fragment size is encapsulated. We have calculated CPU cycles consumed to generate pseudo random number using our technique on standard three core processor 2.4GHz. Using our technique textdata stored into cloud file can be fragmented using random number and fragments can be encrypted to further enhance the security in cloud.

## CHAPTER 3 RESEARCH PAPER



**CHAPTER 4**

**CONCLUSION**

The field fragmentation analytics for data gives the ability to the data to think analytically, using concepts and methods. Tremendous contribution to the various areas has been made by the fragmentation analytics techniques from the last 2 decades. fragmentation analytics will continue to play an increasingly important role in the various fields. We conclude that further research in this area can be done as there are very promising and profitable results that are obtainable from such techniques. While scientists have not yet realized the full potential and ability of artificial intelligence. This technology and its applications will likely have far- reaching effects on human life in the years to come.

## CHAPTER 5

## REFERENCE

1. Text File Privacy on the Cloud based on Diagonal Fragmentation and Encryption Tawfiq Barhoom and Mahmoud Y. Abu Shawish

JOURNAL OF ENGINEERING RESEARCH AND TECHNOLOGY, VOLUME 8, ISSUE 1, MARCH 2021

2)Data Fragmentation in cloud for optimal performance and security

G.Priyadharishini[1],A.Sairamya[2] ,Mrs.W.Mercy[3]

Student, Department of Computer Science and Engineering, Agni College of Technology, India

Assistant Professor, Department of Computer Science and Engineering, Agni College of Technology, India

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3, Special Issue: 1, Mar,2016, ISSN\_NO: 2321-3337

3)A Method for text data fragmentation to provide security in loud computing Archana M Mallikarjun Shastry P M

4)Data Fragmentation and Duplication in cloud for Secure Performance

**L. M. Nithya\* and P. Anu Priya**

Department of Information Technology, SNS College of Technology, Saravanampatti - 641035,

Coimbatore, Tamil Nadu, India

5) Dataset for file fragment classification of textual file format Mansouri Hanis and Teimouri BMC Res Notes(2019) 12:801

<https://doi.org/10.1186/s13104-019-4837-4>

6) Workload-Driven Fragment Allocation for Partially Replicated Databases Using Linear Programming

2019 IEEE 35th International Conference on Data Engineering (ICDE)

7) Application of data fragmentation and replication methods in the cloud: a review

Felipe Castro-Medina, Lisbeth Rodríguez-Mazahua, María Antonieta Abud-Figueroa, Celia Romero-Torres, Luis Ángel Reyes-Hernández, Giner Alor-Hernández

# Division of Research and Postgraduate Studies, Instituto Tecnológico de Orizaba, Orizaba, Veracruz, México [felipecastromedina123@gmail.com,](mailto:felipecastromedina123@gmail.com) [lrodriguez@itorizaba.edu.mx,](mailto:lrodriguez@itorizaba.edu.mx) {mabud, cromero}@ito-depi.edu.mx, [l.a.reyes.h@gmail.com,](mailto:l.a.reyes.h@gmail.com) [galor@itorizaba.edu.mx](mailto:galor@itorizaba.edu.mx)

# 8) An improvement on fragmentation in Distribution Database Design Based on Knowledge-Oriented Clustering Techniques