

## **CRITERIA III: RESEARCH, INNOVATION AND EXTENSION**

### **3.2.2: NUMBER OF BOOKS AND CHAPTERS IN EDITED VOLUMES/BOOKS PUBLISHED AND PAPERS PUBLISHED IN NATIONAL/ INTERNATIONAL CONFERENCE PROCEEDINGS**

**DATA COLLECTION YEAR FOR ASSESSMENT**

**2017-18**

Navman's

Introduction to  
**Cost**  
**Accounting**



Dr. R. K. Gupta | Dr. Himani Gupta

# Contents

1. Introduction (Definitions, Objects, Importance & Methods) ....	1.1 – 1.24
2. Elements of Cost & Their Classification ....	2.1 – 2.20
3. Accounting for Material I (Material Control - Concepts & Techniques) ....	3.1 – 3.40
4. Accounting for Material II (Inventory System, Pricing of Material Issues, Treatment of Material Losses) ....	4.1 – 4.32
5. Accounting for Labour ....	5.1 – 5.52
6. Overheads : Allocation, Apportionment & Absorption	6.1 – 6.52
7. Single Unit and Output Costing ....	7.1 – 7.72
8. Job and Batch Costing ....	JBC.1 – JBC.20
9. Contract Costing ....	CC.1 – CC.96
10. Operating Cost ....	OC.1 – OC.48
11. Process Cost Accounts. (Including Inter Process Profits) ....	PC.1 – PC.108
12. Examination Papers of GGS IPU ....	i – xvi



# 1

## INTRODUCTION

### (Definitions, Objects, Importance & Methods of Cost Accounting)

*"Cost accounts are the key to economy in manufacture, and are indispensable to the intelligent and economic management of a factory."*

*W. Strachan*

1	Meaning and Definitions of Cost & Accounting	1.02
2	Definitions of Cost Accounting and Cost Accountancy	1.03
3	Nature of Cost Accounting	1.04
4	Need, Reasons for Study & Evolution of Cost Accounting	1.04
5	Comparison between Cost Accounts & Financial Accounts	1.06
6	Differences between Financial Accounting & Cost Accounting	1.08
7	Similarities between Financial Accounting & Cost Accounting	1.09
8	Aims and Objects of Cost Accounting	1.09
9	Scope & Functions of Cost Accounting	1.11
10	Advantages & Importance of Cost Accounting	1.11
11	Criticisms of Cost Accounting System	1.13
12	Characteristics of an Ideal System of Cost Accounting	1.14
13	Different Methods/Systems or Types of Cost Accounting	1.15
14	Techniques of Costing	1.17
15	Installation of a Costing System	1.18
16	Steps for Installing a Costing System	1.18
17	Practical difficulties in Installing a Costing System	1.19
18	Steps to Overcome from Practical Difficulties	1.20
19	Cost Center	1.20
20	Unit of Cost	1.21
21	Profit Center	1.22
22	Examination Questions	1.22

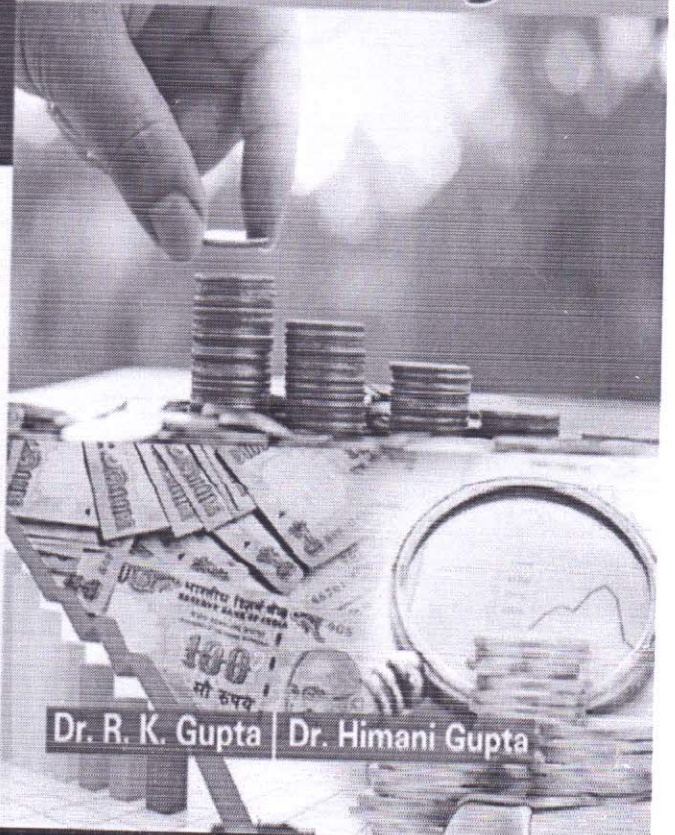
It is necessary to keep proper accounts of every business or industry for its successful operations. Every businessman and the owner of every industry tries to know that how much profit or loss has been occurred to him through his business or industry. Moreover he also tries to know the reason behind any loss or profit occurred to his business or industry so that he may control the unfavourable causes and support the favourable reasons for maximization of profit. For this ultimate purpose of maximization of profit he adopts the system of accounting for every transaction. Now the question arises what the system of accounting is. According to the Committee on terminology of American Institute of Certified Public Accountants (AICPA), "Accounting is the art of recording, classifying and summarizing in a significant manner and in terms of money transactions and events which are in part at least, of a financial character and interpreting the result thereof." Therefore the system of accounting is the method of accounting of the economical transactions of a business and representing the results thereof.



Dr. R. K. Gupta  
Dr. Himani Gupta

Navman's

# Cost Accounting



Cost Accounting

Dr. R. K. Gupta | Dr. Himani Gupta



Shri Navman Publication  
Aligarh - 202001 (U.P.) IN

**Book of Abstracts**  
**2017**  
**IIM Indore-NASMEI**  
**Summer Marketing Conference**

**July 27-29, 2017**  
**Indian Institute of Management Indore**



**Emerald Group Publishing (India) Private Limited**  
**New Delhi**

---

Emerald Offices  
Bingley, Cambridge, Sao Paulo, Johannesburg, Dubai, New Delhi, Beijing, Kuala Lumpur, Melbourne

**Emerald Group Publishing (India) Private Limited**

1001-1004, 10th Floor, Hemkunt Towers, 6, Rajendra Place, New Delhi - 110008

**Title: Book of Abstracts: 2017 IIM Indore-NASMEI Summer Marketing Conference**

Copyright © 2017

Contact: Conference Secretariat (marconference@iimdr.ac.in)

No part of the publication may be reproduced, stored in a retrieval system, transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the publisher. Any opinions expressed in the articles/chapters are those of the authors. Whilst Emerald India makes every effort to ensure the quality and accuracy of the content, Emerald India makes no representation implied or otherwise, as to the articles/chapters suitability and application and disclaims any warranties, express or implied, to their use.

This edition can be exported from India by the publisher, Emerald Group Publishing (India) Private Limited.

ISBN: 978-1-78635-416-7



## Contents

Case Studies on Transformation of Traditional Marketing to Digital and Social Media Marketing: Indian Context <i>Pratibha Barik, B. B. Pandey</i>	1
Atithi Devo Bhava: Social Media and Digital Marketing Strategy of Indian Tourism Departments <i>Arpan Yagnik, Sujo Thomas, Karishma Dalal</i>	2
Customer Satisfaction, Loyalty and Switching – Evidence from India <i>Aakash Ashok Kamble, Shubhangi Walvekar</i>	3
Rethinking Marketing Management Pedagogy: An Alumni's Opinion-Based Study <i>Subhjit Bhattacharya, Rohit Vishal Kumar, Anindya Dutta</i>	4
Exploring The Role of Value in Social Security Marketing <i>Saunak Bhattacharyya, Mrinalini Pandey</i>	5
Materialism and Consumer Decision-Making Styles of Indian Teenagers: A Second-Order Structural Equation Modelling Approach <i>Sartaj Chaudhary, A. K. Dey</i>	6
Do Friends Influence Perceived Value from a Consumption Experience? An Experimental Investigation <i>Diptiman Banerji, Ramendra Singh, Prashant Mishra</i>	7
Open Defecation and Value Added Social Campaign to Eradicate the Problem <i>M. Yaseen Khan, Aporva Tatke</i>	8
Beauty is only Skin Deep: Impact of Celebrity Attractiveness on Purchase Intention <i>Tijo Thomas, Johney Johnson</i>	9
Quality of Healthcare Services in Government and Private Hospitals in Varanasi: Patient's Perspective <i>Preeti Singh</i>	10
Factors Underlying Consumer Behaviour in Healthcare Virtual Communities (HVCs) <i>Vaishali Sharma, Mahima Gupta</i>	11
Perceptual Differences towards Service Quality in Indian Public and Private Banking Sector: A Study of Rohilkhand Region <i>Ankit Agarwal, Raj Kamal</i>	12
Understanding the Link between Employee Satisfaction and Customer Value Creation among Start-ups in the Indian Context <i>Varshini Rajesh, Renuka Kumar, Aditya G. Kovvali</i>	13

# Materialism and Consumer Decision-Making Styles of Indian Teenagers: A Second-Order Structural Equation Modelling Approach

Sartaj Chaudhary<sup>1\*</sup>, A.K. Dey<sup>2</sup>

<sup>1</sup>Jagannath International Management School, New Delhi, India.

<sup>2</sup>Birla Institute of Management Technology, Greater Noida, India.

## Abstract

The purpose of this paper is to study the influence of materialism on consumer decision-making styles of teenagers. The conceptual model is developed through a review of literature and is then validated in the context of high school children in NCR, India. A total of 1,216 responses were considered. The model is validated using second-order structural equations. The model is found to be a good fit to the empirical data, and six out of the seven hypothesised relationships were found to be significant. This study examines the influence of materialism on the consumer decision-making styles and its characteristics in the case of the teenage segment. This study is restricted to CBSE schools in NCR and hence cannot be generalised to the whole teenage population in India. The paper identifies the constructs of materialism and gives empirical support to materialism having a direct impact on consumer decision-making styles and its constructs. Marketers can use the findings to segment the teenager market and devise effective strategies. This is the first study that examines the impact of materialistic values on the consumer decision-making styles of teenagers in India. This is for the first time that both materialism and consumer decision-making styles have been studied as second-order constructs.

## Keywords:

Materialism, Consumer Decision-Making Styles, Teenagers, India, Second Order, Structural Equation Modelling



Book of Abstracts  
of the 2017  
IIM Indore-NASMEI  
Summer Marketing  
Conference

\*Corresponding Author: Sartaj Chaudhary (sartaj.khera@jagannath.org)

# **3rd International Conference on Computers and Management (ICCM 2017)**

Kota, India  
28-29 December 2017

## **Editors:**

**C. P. Gupta  
Sh. Dinesh Soni**

**R. K. Banyal  
Seema Sharma**

ISBN: 978-1-5108-5316-4

**Printed from e-media with permission by:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2017) by International Association of Academicians Connecting Scholars, Scientists and Engineers (IAASSE) All rights reserved.

Printed by Curran Associates, Inc. (2017)

For permission requests, please contact International Association of Academicians Connecting Scholars, Scientists and Engineers (IAASSE) at the address below.

International Association of Academicians Connecting Scholars, Scientists and Engineers (IAASSE)

[www.iaasse.org](http://www.iaasse.org)  
[info@iaasse.org](mailto:info@iaasse.org)

**Additional copies of this publication are available from:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: 845-758-0400  
Fax: 845-758-2633  
Email: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

## TABLE OF CONTENTS

<b>Design and Implementation of Energy-Aware Hierarchical Clustering Technique of WSN for Improving Network Life .....</b>	<b>1</b>
<i>Meenakshi Yadav, Anoop Bhola, Chandra Kumar Jha</i>	
<b>Fusion of K-means Algorithm with Dunn's Index for Improved Clustering .....</b>	<b>N/A</b>
<i>Amit Bhadana, Manoj Singh</i>	
<b>Modeling for VM Allocation Using Particle Swarm Optimization .....</b>	<b>12</b>
<i>Taskeen Zaidi, Ram Pratap</i>	
<b>Impact of Method Noise on SAR Image Despeckling .....</b>	<b>19</b>
<i>Prabhishek Singh, Raj Shree</i>	
<b>Transition in Step Network Through Simulation Tool .....</b>	<b>23</b>
<i>Taskeen Zaidi, Nitya Nand Dwivedi</i>	
<b>Pair-Wise Selection Approach for Test Case Prioritization in Regression Testing .....</b>	<b>29</b>
<i>Shilpi Singh, Raj Shree</i>	
<b>Privacy Policies: Preserving Confidentiality of Big Data .....</b>	<b>36</b>
<i>Kanika, Alka Agrawal, R.A. Khan</i>	
<b>A Review: Study and Analysis of Images in Different Color Models .....</b>	<b>45</b>
<i>Neetish Kumar, Deepa Raj</i>	
<b>Software Defects Prediction Using AI Technique: A Review .....</b>	<b>52</b>
<i>Sunil Kumar Singh, Raj Shree</i>	
<b>Avert Traffic Violations by Automatic License Plate Detection Using Deep Learning Technique .....</b>	<b>58</b>
<i>S. Preethi, Kumar P Madhan, S Pradeep, Rosaline R Anto Arockia</i>	
<b>The Survey of Machine Learning Algorithm for Component Based Software Data Exchange .....</b>	<b>65</b>
<i>Amit Verma, Gurpreet Singh Kamboj, Iqbaldeep Kaur</i>	
<b>IOT Based Interactive Smart Refrigerator .....</b>	<b>72</b>
<i>N. G. Murali, S. Aarthi, M. Ethiraj, S. Baghavathi Priya</i>	
<b>Prevention of Bike Accidents Using an Intelligent Helmet .....</b>	<b>79</b>
<i>P. N. Vignesh, Rosaline R. Anto Arockia, M. Barath, K. A. Athar Zafeer</i>	
<b>Code Smell Detection Text Mining Tool Analysis for Source Code Improvization .....</b>	<b>86</b>
<i>Amit Verma, Ashish Kumar, Iqbaldeep Kaur</i>	
<b>ARIS: A Machine Learning Algorithm to Test Games .....</b>	<b>93</b>
<i>S. C. Shivani, S. Santhakalakshmi, S. Baghavathi Priya</i>	
<b>A Road Map to Big Data and Machine Learning .....</b>	<b>103</b>
<i>S. Sbha, S. Bafhavathipriya</i>	
<b>Smart-EVM Using Multi-modal Biometrics with Embedded Security .....</b>	<b>110</b>
<i>R. Pavithra, Kumar N. Sharath, P. Siddhartha, G. Anitha</i>	
<b>Smart Applications in Smart City and Improved Traffic Management System Using Collaborative Approach Among Nano Robots .....</b>	<b>116</b>
<i>Mamata Rath, Bibudhendu Pati, Binod Kumar Pattanayak</i>	
<b>A Robust Fall Detection System Using Deep Learning Algorithms .....</b>	<b>124</b>
<i>K. Durga Devi, G. Anitha, S. Baghavathi Priya</i>	
<b>Visitor Counter in Indian Railways .....</b>	<b>129</b>
<i>S. Vasanthakumar, N. Sangamithra, K. Vijay, K. Sai Yashwanth, M. Mehfooza</i>	
<b>Performance Evaluation of Nonlinear Filters for Impulse Noise Removal .....</b>	<b>133</b>
<i>Kaushal Sishor, Prabhishek Singh</i>	
<b>Manifold Surveillance Issues in Wireless Network and the Secured Protocol .....</b>	<b>139</b>
<i>Mamata Rath, Bibudhendu Pati, Binod Kumar Pattanayak</i>	
<b>Improving DV-Hop Based Localization Algorithms in Wireless Sensor Networks by Considering Only Closest Anchors .....</b>	<b>148</b>
<i>AManpreet Kaur, Padam Kumar, Govind P. Gupta</i>	
<b>3D Facial Model for Analysing the Facial Paralysis .....</b>	<b>160</b>
<i>Banita, Poonam Tanwar</i>	
<b>An Intuitionistic Fuzzy AHP Based Multi Criteria Recommender System for Life Insurance Products .....</b>	<b>170</b>
<i>Akshay Hinduja, Manju Pandey</i>	
<b>Agile Sink Based Data Gathering Protocol Employing Genetic Algorithm Utilizing Binary String (MSDGP-GAB) for Prolonged Network Lifetime in Wireless Sensor Networks .....</b>	<b>180</b>
<i>Amiya Bhusan Bagjadab, Sushree Bibhuprada B. Priyadarshini, Dinesh Dash</i>	

<b>Bug Model based Intelligent Recommender System with Exclusive Curriculum Sequencing for Learner-Centric Tutoring</b> .....	187
<i>Ninni Singh, Neelu Jyothi Ahuja, Amit Kumar</i>	
<b>Collaborative Model for Security in Cloud</b> .....	195
<i>Brijesh Pandey, Abhineet Anand</i>	
<b>Data Characterization of ISBSG R12 Using Data Analytics: An Exploratory Study</b> .....	199
<i>Ghazi Alkhatib, Khalid Al-Sarayrah</i>	
<b>Data Security Issues and their Solutions in Cloud Computing</b> .....	207
<i>Anubhav Raj Singh, Abhineet Anand</i>	
<b>Cloud Computing in Banking Sector</b> .....	211
<i>Shashwat Singh, Abhineet Anand</i>	
<b>Security and Compliance Management in Cloud Computing</b> .....	214
<i>Ahtisham Hashmi, Aarushi Ranjan, Abhineet Anand</i>	
<b>Brand Positioning Strategy in Marketing Management</b> .....	221
<i>D. Prabha</i>	
<b>A Comparative Study of Job Stress Level of Software Professionals: A Case Study of Private Sector in India</b> .....	233
<i>Geeta Kumari, Ashfaue Alam, Gaurav Joshi</i>	
<b>An Efficient Technique to Sort Large Datasets Using Merge of Multiple Streaming Files</b> .....	240
<i>Tanu Chaturvedi, Manoj Singh</i>	
<b>A Study of the Impact of Data Warehousing and Data Mining Implementation on Marketing Effort</b> .....	244
<i>Kanika Chaudhry, Sanjay Dhingra</i>	
<b>3D Facial Model for Analysing the Facial Paralysis</b> .....	251
<i>Banita, Poonam Tamwar</i>	
<b>An Institutionistic Fuzzy AHP Based Multi Criteria Recommender System for Life Insurance Products</b> .....	261
<i>Akshay Hinduja, Manju Pandey</i>	
<b>Ontology Development Utilizing Social Network Data Attributed to Drugs</b> .....	270
<i>Puja Munjal, Priyank Kumar, Akshay S. Nair</i>	
<b>Author Index</b>	

**RAJASTHAN TECHNICAL UNIVERSITY, KOTA**  
**CERTIFICATE OF PRESENTATION**



*This certificate is awarded to:*

**Puja Munjal**

*Jagannath University, Jaipur*

*for paper titled*

***Ontology development utilizing social network data attributed to drugs***

*in technical presentation, recognition and appreciation of research contributions to*

***3<sup>rd</sup> International Conference on Computers & Management  
(ICCM- 2017)***

*held at*

***Apex Institute of Engineering & Technology, Jaipur***

*on 28-29 December 2017*



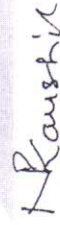
**Dr. C.P. Gupta**

**General Chair**



**R.K. Banyal**

**General Chair**



**Prof. N.P. Kaushik**

**Vice Chancellor**

# Ontology development utilizing social network data attributed to drugs

Puja Munjal, Sandeep Kumar  
Jagannath University, India

Hema Banati  
University of Delhi, India

## ABSTRACT

*The Social networking sites have provided a colossal change in the way people seek information regarding general healthcare. These destinations offer open doors for individuals to impart insights and encounters unreservedly in online social groups which can play a vital role in the awareness of clinical and healthcare sector. Nowadays, there exists diversity in illness, medicines, source, symptoms and prevention methods. To cater this diversity, the information must be structured in such a way that doctors and patients can easily find disease and their cures according to its category. However there are various retrieval systems which lack the use of semantics to retrieve relevant information. In this paper, a social media enabled methodology is proposed which can detect the opinions of user generated content on various social media web forums and further update the ontology which will facilitate easy retrieval of relevant information regarding healthcare. Further a modular ontology is created using protégé software for different diseases from both infectious and non-infectious categories. This ontology also includes cures for different diseases with causes of that disease.*

*Keywords—Ontology; Knowledge Management; Healthcare ; Social Media; Social Network; Protégé; Semantic Web;*

## INTRODUCTION

Nowadays in the field of medicine, analysis of healthcare data is playing a crucial role, both by facilitating physicians to collect patient's vital healthcare information and shortening the process of the medical assessment [1][2]. There is abundance of diverse healthcare data, collected from various sources in different formats and terminologies. In any case, the availability and utility of the medicinal services information is extremely compelled by absence of normal vocabulary [3]. To counter this, World Wide Web can prove to be crucial channel, because of its reach to a vast population of drug users [4]. A number web enabled social forums, provide a stage to pill clients will impart their experiences, questions, Also conclusions something like different medications. The web based data has huge potential to even monitor the illicit use of pharmaceutical drugs [5][6]. The earlier attempts of web-based studies to gather information on pharmaceutical drugs are largely based on surveys and manual searches. Till date very few efforts have been made to utilize computerized methods to analyze user generated content from web forums or other social network sites which can



inspect health related issues. Also the earlier studies for content analysis of web-based data were limited by manual coding and lacked serious methodological strategy [7][8].

Manual extracting of data from various sources in qualitative research of web communications requires the researchers perform rigorous steps of "reading" a text document, then to "break" it into smaller meaningful segments and finally analyzing them to fetch meaningful information. Hence manual coding is a cumbersome task, seriously limiting the wider application of web-based data pertaining to healthcare sector[9]. Recently many social network platforms like facebook, twitter and web forums etc. are generating important healthcare related information which can be critical for healthcare sector[10]. However, this suffers with a shortcoming of data being in unstructured format, as a result the search for correct terms becomes difficult [11][12]. Need of the hour is the formulation of a well-organized structure, resulting from an automated and dynamical collection of information from all possible resources. This structured information helps a user to fetch correct and coherent information. In this paper a general medical healthcare methodology has been proposed that can provide updated information regarding various diseases and drugs semantically searched from social network web forums. The organization of the paper is as follows: Section II on one hand discusses the essential background work, with brief description of important concepts like semantic web, ontology etc. and on the other hand explains advantages of content of the social network in the development of ontology. Section III describes the methodology for utilizing user generated content for Healthcare. Section IV contains future work and conclusion.

## BACKGROUND

**Semantic Web:** The Semantic Web [13] is a platform generated by the W3C, resulted from collaborative effort by a number of scientists worldwide. The key target of the semantic web is to provide machine-readable web intelligence resulting from hyperlinked dictionaries, which will facilitate the web authors to explicitly define their words and concepts. This facilitates to develop smart and efficient web which can replace existing traditional linguistic analysis.

**Semantic Web Layered Structure:** Generally a layered structure is represented by SW, as shown in Figure 1; where by different degree of expressiveness is associated with each layer. The attributes of each layer are as follows:

- Users are allowed by the XML layer, to make available storing a transferring data in controlled form
- The very next layer from bottom is the RDF layer which critically represents data in the World Wide Web.
- The next upper layer is the ontology vocabulary, which enables the implementation of semantics to RDF by explicitly specifying the concepts and the attached constraints.
- The logic layer establishes the rules attributed to the explicit inference.
- Trust is the top most layer which give components to build up confidence in a given verification [14].

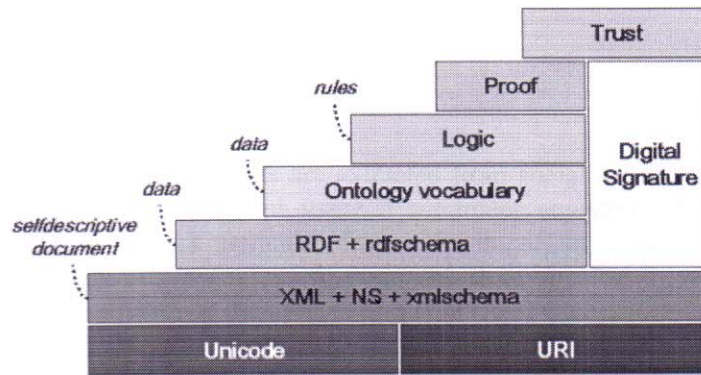


Figure 1: Semantic Web structure having Ontology Layer

### Ontology

Ontology layer is pivotal layer of semantic web, which chiefly lays down the knowledge base associated to a certain domain by means of providing relevant concepts [15] and attached relations [16]. It also specifies other critical parameters required for modeling a domain. A well-organized structure is the basis of core ontology. Following is the mathematical representation of ontology [17]:

$$\mathcal{O} = (C, \leq_C, R, \sigma, \leq_R)$$

This representation consists of two disjoint sets  $C$  and  $R$  whose elements are called concept identifiers and relation identifiers.

The initial step to learn ontology is to establish the subtasks, on which lays the foundation of the complex task of further development of ontology. Developing ontology practically includes:

- Defining and hierarchical arrangement of classes.
- Defining slots and describing permitted values for these slots.
- Assigning instantaneous values for slots.

### Social Network Data

Social media content can be utilized to semantically construct a dynamic ontology with properties of mutual sharing, reusability and improved trust value for gaining information regarding healthcare.

The field of medical information has witnessed a vast use of semantic web since the year 2000, based on various architectures and frameworks proposed by researchers all around the world [18][19]. The analysis of sentiments and contents, posted on social network sites (SNS) has proved critical to the field of physical and mental health [20]. There are several reports of studies based on measurement or prediction of depressed mental state of a person analysis of posts on SNS [21]. More recently natural language processing (NLP) has been used to analyze social media postings by military personals involved in combat, critical for national defense of a country [22].

### III. METHODOLOGY

This paper proposes a methodology to develop and augment a general healthcare ontology, as shown in Figure 2. This methodology initializes the search process by considering the drug

108

specific query and the crawler contents are extracted from social media health forums. This information gathered is then analyzed using a sentiment analyzer, which facilitates the detection of the opinion about a particular drug. The important keywords extracted in the process will be ontologically organized to form the drug specific knowledge base. This ontology can be further utilized by the users

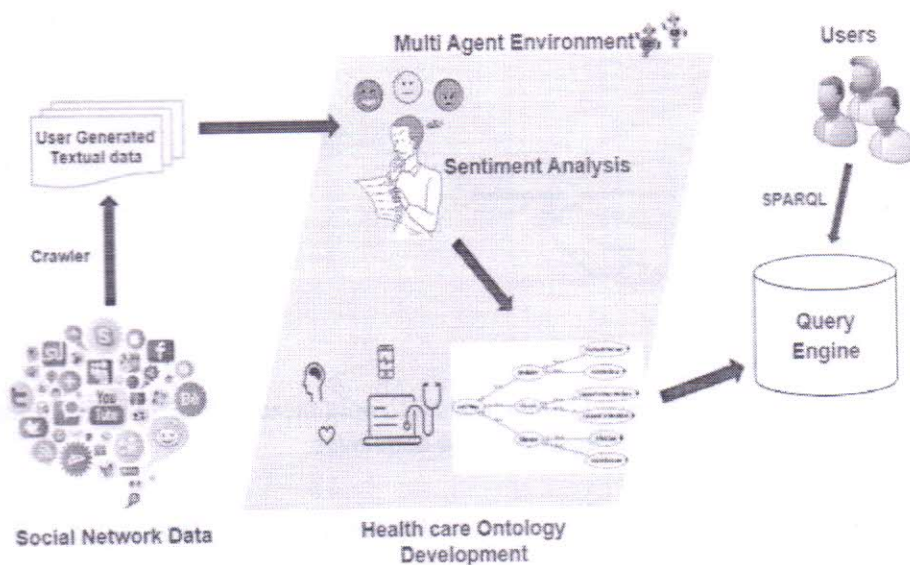


FIGURE 2: Methodology- Social media content enabled healthcare ontology

There are multiple phases involved in the creation of an ontology. The initial phase is the requirements analysis phase where main components required for ontology are identified which are concepts, relationships and hierarchies. In the design phase, classes of the ontology are defined. In the final development phase, structure of the ontology is developed using the OWL language.

In this work we have successfully developed the structure of ontology using Protégé<sup>1</sup> which is a free open source software to create intelligent systems. Protégé<sup>1</sup> can create complete knowledge based system fully supporting latest OWL 2 Web Ontology Language and RDF specifications from the World Wide Web Consortium in which the default class is named as OWL: Thing Like in Java Language we have object class which is referred as a superclass of all the classes present in the language. Similarly, "Thing" is defined as the default parent class in ontology hierarchy. In this ontology, three main attributes have been taken into account which are:

- i. Causes
- ii. Diseases
- iii. Drugs

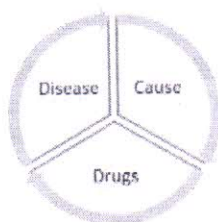


Figure 2: Three main attributes in developing a healthcare ontology

107

Each subclass is having "is a" relationship with owl: Thing and their associated parent class.

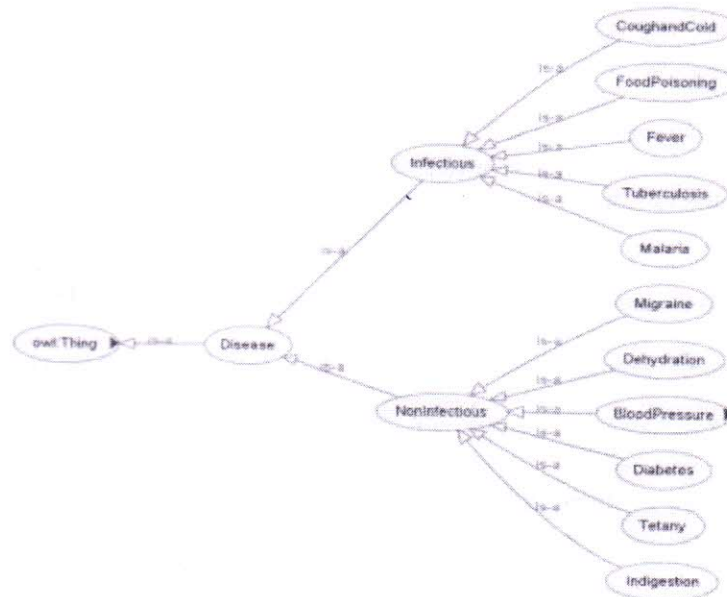


Figure 3: Graphical Representation of a class named Disease in Healthcare ontology developed using Protégé<sup>1</sup>

#### IV CONCLUSION AND FUTURE WORK

Ontologies play a significant role in biomedical research over different applications. There is great requirement of semantic **reconcilability** in the domain of different healthcare systems that share information and knowledge. This social media driven information accumulation can accelerate the updating of particular ontologies that can be utilized to develop heterogeneous systems. This work is having a high potential of developing an automated system whereby the opinions for specific diseases and drugs will be collected from online social media. This will save the critical time spent by a person searching about the medical advice by visiting individual social network sites.

#### V REFERENCES

- [1] V. Kumar and others, "Ontology Based Public Healthcare System in Internet of Things (IoT)," *Procedia Comput. Sci.*, vol. 50, pp. 99–102, 2015.
- [2] Gai, Keke, et al. "Electronic health record error prevention approach using ontology in big data." High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICCESS), 2015 IEEE 17th International Conference on. IEEE, 2015..
- [3] A. Sunitha and G. S. Babu, "Ontology-Driven Knowledge-Based Health-Care System, An Emerging Area-Challenges And Opportunities-Indian Scenario," *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, vol. 40, no. 8, p. 239, 2014.
- [4] R. Kavuluru *et al.*, "An up-to-date knowledge-based literature search and exploration framework for focused bioscience domains," in *Proceedings of the 2nd ACM SIGHT International Health Informatics Symposium*, 2012, pp. 275–284.

106

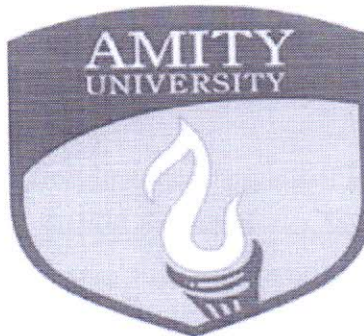
- [5] M. B. Miles and A. M. Huberman, *Qualitative data analysis: An expanded sourcebook*. sage, 1994.
- [6] R. S. Falck, R. G. Carlson, J. Wang, and H. A. Siegal, "Sources of information about MDMA (3, 4-methylenedioxymethamphetamine): perceived accuracy, importance, and implications for prevention among young adult users," *Drug Alcohol Depend.*, vol. 74, no. 1, pp. 45–54, 2004.
- [7] E. J. Cone, "Ephemeral profiles of prescription drug and formulation tampering: evolving pseudoscience on the Internet," *Drug Alcohol Depend.*, vol. 83, pp. S31–S39, 2006.
- [8] E. W. Boyer and J. D. Wines, "Impact of Internet Pharmacy Regulation on Opioid Analgesic Availability," *J. Stud. Alcohol Drugs*, vol. 69, no. 5, pp. 703–708, 2008.
- [9] A. M. Pandya, R. E. Rosales, R. B. Rao, and H. Steck, *Medical ontologies for computer assisted clinical decision support*. December.
- [10] S. Konovalov, M. Scotch, L. Post, and C. Brandt, "Biomedical informatics techniques for processing and analyzing web blogs of military service members," *J. Med. Internet Res.*, vol. 12, no. 4, 2010.
- [11] T. J. Bright, E. Y. Furuya, G. J. Kuperman, J. J. Cimino, and S. Bakken, "Development and evaluation of an ontology for guiding appropriate antibiotic prescribing," *J. Biomed. Inform.*, vol. 45, no. 1, pp. 120–128, 2012.
- [12] V. Bertaud-Gounot, R. Duvauferrier, and A. Burgun, "Ontology and medical diagnosis," *Inform. Health Soc. Care*, vol. 37, no. 2, pp. 51–61, 2012.
- [13] T. B. Lee, J. Hendler, O. Lassila, and others, "The semantic web," *Sci. Am.*, vol. 284, no. 5, pp. 34–43, 2001.
- [14] I. Bittencourt, E. Costa, E. Soares, and A. Pedro, "Towards a new generation of web-based educational systems: The convergence between artificial and human agents," *IEEE Multidiscip. Eng. Educ. Mag.*, vol. 3, no. 1, pp. 17–24, 2008.
- [15] T. Gruber, "A Translation Approach to Portable Ontology Specifications, Knowledge Systems Lab," Stanford University, Tech. Report KSL92-71, 1993.
- [16] A. Kogilavani and B. D. P. Balasubramanie, "Ontology enhanced clustering based summarization of medical documents," *Int. J. Recent Trends Eng.*, vol. 1, no. 1, 2009.
- [17] E. Bozsak *et al.*, "KAON—towards a large scale Semantic Web," *E-Commer. Web Technol.*, pp. 231–248, 2002.
- [18] H. Hu and L. Kerschberg, "Standardizing the Crowdsourcing of Healthcare Data Using Modular Ontologies," in *Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual*, 2017, vol. 2, pp. 107–112.
- [19] O. Mohammed, R. Benlamri, and S. Fong, "Building a diseases symptoms ontology for medical diagnosis: an integrative approach," in *Future Generation Communication Technology (FGCT), 2012 International Conference on*, 2012, pp. 104–108.
- [20] M. Park, C. Cha, and M. Cha, "Depressive moods of users portrayed in Twitter," in *Proceedings of the ACM SIGKDD Workshop on healthcare informatics (HI-KDD)*, 2012, vol. 2012, pp. 1–8.
- [21] M. De Choudhury, M. Gamon, S. Counts, and E. Horvitz, "Predicting Depression via Social Media.," *ICWSM*, vol. 13, pp. 1–10, 2013.
- [22] H. Jung, H.-A. Park, and T.-M. Song, "Development and Evaluation of an Adolescents' Depression Ontology for Analyzing Social Data.," *Stud. Health Technol. Inform.*, vol. 225, pp. 442–446, 2016.

2017  
Recent Developments in  
Control, Automation and Power Engineering  
(RDCAPE)

26-27 October 2017

Amity School of Engineering and Technology, Noida, India

Organized by:



Technically Co-Sponsored by : IEEE UP Section



## TABLE OF CONTENT

1. Smart Solar Hybrid Led Streetlight <b>Aman Jha, Manoj Kumar, Jitendra Jain, Indar Prakash Singhal</b>	1
2. Dynamic Stability Algorithm for A Hexapod Robot <b>B.Veekshan Sree Sessa Sai, B. Akshay Kumar, Nippun Kumar A. A.</b>	7
3. Design of Signed Distance Method Based Fuzzy Logic Controller for Tito Process <b>Aprajita Singh, P. S. Londhe</b>	13
4. Non-Intrusive Load Monitoring Based on Graph Signal Processing <b>Amit Kumar, Hemant Kumar Meena</b>	18
5. Hdl And Timing Analysis of Amba Ahb On Fpga Platform <b>Anshu Gaur, Piyush Sharma, Shiv Pratap Pandey</b>	22
6. Efficient Clear Air Turbulence Avoidance Algorithms Using Iot For Commercial Aviation <b>Amlan Chatterjee, Hugo Flores, Bin Tang, Ashish Mani, Khondker S. Hasan</b>	28
7. Investigation of The Effect of Transverse Crack on The Modal Properties of Cantilever Beams with Different Geometries Using Finite Element Analysis <b>Sameera Mufazzal, S M Muzakkir</b>	34
8. A Data Driven Approach for Scheduling the Charging of Electric Vehicles <b>Anjali Jain, Ashish Mani, Anwar S. Siddiqui, Sharad Sharma, Hemender Pal Singh</b>	39
9. Novel Architecture for Area and Delay Efficient Vedic Multiplier <b>Aayush Goel, Ankit Gupta, Maninder Kumar, Neeta Pandey</b>	45
10. A Generalized Bus Dependency Matrix Based Centrality Measures for Reactive Power Compensation <b>Dibya Bharti, Mala De</b>	49
11. Modelling of Dc Linked Pv/Hydro Hybrid System for Rural Electrification <b>Anuradha, Akhilendra Yadav, S.K.Sinha</b>	55
12. Fuzzy Logic Based Pitch Angle Controller for Scig Based Wind Energy System <b>K. A. Naik, C. P. Gupta</b>	60
13. A New General Topology for Asymmetrical Multilevel Inverter with Reduced Number of Switching Components <b>Kamaldeep Boora, Dr. Jagdish Kumar, Himanshu</b>	66

76. Whether Colour, Shape and Texture of Leaves Are the Key Features for Image Processing Based Plant Recognition? An Analysis!	Jibi G Thanikkal, Ashwani Kumar Dubey, Thomas. M.T	404
77. Analysis of Different Filters for Noise Reduction in Images	<b>Bhawna Dhruv, Neetu Mittal, Megha Modi</b>	410
78. Performance Optimization Of Self Excited Induction Generator: A State of Art	Swati Paliwal, Sanjay Kumar Sinha, Yogesh Kumar Chauhan	416
79. Optimal Tuning of Pss And Statcom-Based Controllers Using Differential Evolution Algorithm	Jitendra Bikanaria, Dr. Sanjeev Kumar Sharma, Kapil Parkh, Nishant Dhakre	421
80. Voltage and Frequency Controller for Seig Based Battery Storage System	Vasundhara Tripathi, Monika Jain	427
81. Overview of Architecture for Gps-Ins Integration	P Srinivas, Wg Cdr (Retd) Dr. Anil Kumar	433
82. Development of Web Based Gas Monitoring System Using Labview	Neeraj Khara, Priya Sharma, Divya Shukla, Ishfaq Gaffar Dar	439
83. Deep Learning Lstm Based Ransomware Detection	Sumith Maniath, Aravind Ashok, Prabakaran Poornachandran, Sujadevi Vg, Prem Sankar a U, Srinath Jan	442
84. Predictive Analysis Using Hybrid Clustering in Diabetes Diagnosis	Kanika Bhatia, Rupali Syal	447
85. Comparative Study of Dual Active Bridge Isolated Dc to Dc Converter with Single Phase Shift and Dual Phase Shift Control Techniques	Bhimisetty Manoj Kumar, Anupam Kumar, Dr. A.H.Bhat, Dr.Pramod Agarwal	453
86. Automized Gamma Correction for Shadow Removal in Color Aerial Images	Vertika Jain, Ajay Khunteta	459
87. Analysis of Pwm Techniques on Multilevel Cascaded H-Bridge Three Phase Inverter	B. Hemanth Kumar, Makarand. M Lokhande	465
88. A Methodology For 11-Level Ac Output Voltage Generation for Stand-Alone/ Grid Tied Solar Pv Applications	Vani Bhargava, Sanjay Kumar Sinha, M P Dave	471
89. Investigation of Pedestrian Collision Avoidance with Auto Brake	Avinash. R, Niresh. J, Harish Kumar. V, Neelakrishnan. S	477
90. Regenerative Braking Energy Storing Phenomena in Fuel Cell Based Electric Vehicle		





# AMITY UNIVERSITY

A RESEARCH & INNOVATION DRIVEN UNIVERSITY



## AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY (ASET)

Department of Electrical & Electronics Engineering

presents

### RDCAPE 2017

International Conference

on

### Recent Developments in Control, Automation & Power Engineering RDCAPE-2017

### CERTIFICATE OF APPRECIATION

This is to certify that Mr./Ms./Dr. BHAWNA DHRUV  
of AIT, Amity University Uttar Pradesh, Noida has presented research paper / delivered keynote talk on  
Analysis of Different Filters for Noise Reduction in Images  
in "International Conference on Recent Developments in Control, Automation & Power Engineering" (RDCAPE - 2017) held on  
26th - 27th October 2017 at Amity University Uttar Pradesh, Noida.

Prof. Sanjay Kumar Sinha

General Co-Chair

Prof. (Dr.) M.K. Dixit

Co-Patron

Prof. (Dr.) Abhay Bansal

Co-Patron

# Analysis of Different Filters for Noise Reduction in Images

Bhawna Dhruv<sup>1</sup>, Neetu Mittal<sup>2</sup>, Megha Modi<sup>3</sup>

<sup>1</sup>Research Scholar, <sup>2</sup>Assistant Professor, <sup>3</sup>MD

<sup>1,2</sup>Amity University Uttar Pradesh, Noida

<sup>3</sup>Yashoda Super Specialty Hospital, Uttar Pradesh

<sup>1</sup>bdhruv08@gmail.com, <sup>2</sup>savini09@gmail.com

**Abstract**-Reducing noise from images still prevails as a challenge in the field of image processing. Image processing proves to be very successful in allowing an extensive range of algorithms to be applied to the input data set in the form of image and retrieve crucial results. These algorithms tend to avoid problems such as noise and signal distortion. An image obtained after noise removal has higher clarity in terms of both interpretation and analysis for study in different fields such as medical, satellite imaging and radar. This paper attempts to analyze the efficacy of different filtering techniques on the image containing 04 types of noises Gaussian, Poisson, Salt & Pepper and Speckle. The performance of filtering techniques Median, Average and Wiener is evaluated by performance measuring parameters execution time and entropy.

**Keywords**-Noise Removal, Filtering techniques, Execution Time, Entropy, Median Filter, Average Filter, Wiener Filter

## I. INTRODUCTION

Most images remain affected by the presence of noise i.e. unwanted signals leading to challenging analysis of images. Image de-noising is a process of removal of unwanted disturbances from the image making image interpretation and analysis easier. The process of image de-noising is achieved by filtering the unwanted noise and accentuating the features and quality of an image [1]. Filters help in providing advancement to visual enhancement and interpretation further laying down the foundation for image segmentation. This further accomplishes different processes such as interpolation and re-sampling. The type of filter to be used during analysis depends upon the behavior of data in the form of image. Two major categories of filter are linear and non-linear filter [2]. Linear filter works on the principle of superposition property and shift invariance utilizing the concept of convolution masks. The usage of this filter depends upon whether preserving the edge is a priority or smoothing the image is. Unlike the linear filters, non linear filters focus upon either the

median or rank order filtering. In case the original image contains large amount of noise but is low in magnitude, a linear filter must be adopted. Whereas if the image possesses less amount of noise but is high in magnitude, then a non linear filter would suffice the analysis [3]. The noise may be random variations in the image making the visual and pictorial interpretation laborious. In this paper, different types of filtering techniques such as Median, Average and Adaptive filters are applied to an image having Gaussian, Poisson, Salt & Pepper and Speckle noise. To evaluate the results measuring parameter entropy has been used. Further execution time is also critically evaluated for comparison of each filter with the help of graphical analysis.

## II. TYPES OF NOISE IN IMAGE

Unwanted signals in an image are noise. It is defined as random variations of information in an image. Noise can occur due to variations of brightness, contrast or color information in an image. There are several ways that can add noise to any image such as electronic transmission, film grain, sensor heat and radio astronomy [4].



Fig 1. Original Image of Cameraman

There are different varieties of noise:

A. Gaussian Noise

The Gaussian noise in an image is introduced during acquisition of digital images. It is an analytical noise whose probability density function is equal to Gaussian distribution [5]. This noise can be modeled by adding random values to an image. Gaussian noise shown in Fig. 2.

$$P_z = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(z-\mu)^2}{2\sigma^2}} \quad - (1)$$

Probability Distribution Function



Fig. 2 Cameraman Image with Gaussian noise

B. Poisson Noise

The other name of Poisson noise is also photon noise. This is a signal dependent noise as shown in fig.3. This occurs when finite number of particles carrying energy fall less to give boost to the statistical fluctuations. The value of Poisson distribution is always higher than the Gaussian distribution [6].



Fig 3 Cameraman Image with Poisson noise

C. Salt & Pepper Noise

It is also known as spike noise. This noise occurs when there exist dark pixels in bright region and vice versa. This further indicates that sudden disturbance in image signals give rise to salt and pepper noise shown in fig. 4



Fig.4 Cameraman Image with Salt & Pepper noise

D. Speckle Noise

Speckle Noise is a crude noise which corrupts the element of medical images in general. This noise occurs due to modeling of reflectivity function. Presence of speckle noise in an image hinders the image interpretation as shown in fig. 5. It can be modeled as:

$$g(n,m) = f(n,m) * u(n,m) + \epsilon(n,m) \quad - (2)$$



Fig.5 Cameraman Image with Speckle noise

### III. FILTERING TECHNIQUES

De noising is a process of removal of noise from an image. This helps in upgrading the image quality and making the image interpretation easier for analysis [7]. Several filtering techniques that exist are:

#### A. Median Filter

Median filter also known as edge preserving filter is a nonlinear method used in the process of de noising. It proceeds in a way that every pixel is reacquired by the median value of neighboring pixels [8, 9]. Median filter proves to preserve the edges and lines of an image in best possible way thereby removing the outliers. It can be stated as:

$$y[m, n] = \text{median}\{x[i, j], (i, j) \in w\} \quad (3)$$

Where,  $w$  is neighborhood focused on the location  $[m, n]$  in an image.

#### B. Average Filter

Mean filtering is a process of smoothing images by compressing the extent of intensity variations among the neighboring pixels. This filter proceeds in a way that every pixel is replaced by the mean of neighboring pixel including itself [10]. There exist certain issues while implementing the mean filter. They are:

- i) A single pixel with peculiar value can influence the average value of all pixels in the neighborhood.
- ii) Edges might get blurred while interpolating the new values [11].

#### C. Adaptive Wiener Filter

Removal of blur due to linear motion in an image can be efficiently achieved by Wiener filter. This proceeds in a way that optimum solution is acquired between converse filtering and polished noise [12]. It is a continuous assessment of the actual image which can be stated in Fourier domain as:

$$W(f_1, f_2) = \frac{H^*(f_1, f_2)S_{xx}(f_1, f_2)}{(H(f_1, f_2))^2 S_{xx}(f_1, f_2) + S_{nn}(f_1, f_2)} \quad (4)$$

The major drawback of this technique is that it is singular in nature, hence focusing on the use of generalized inverse filtering [13].

### IV. RESULTS & DISCUSSION

The cameraman image with 04 different noises i.e. Gaussian, Poisson, Salt & Pepper and Speckle noises is considered. To effectively remove these noises from these images, three different filtering techniques i.e. median, average and wiener are applied. All the three filters behave differently for each type of noise. The comparative efficacy of these filtering techniques is done by determining the parameters, time of execution and Entropy .summarized in Table I by determining the parameters i.e. Time of execution and Entropy.



Fig. 6(a) Cameraman Image With Gaussian Noise



Fig. 6(b) Noise removal With Median Filter



Fig. 6(c) Noise removal With Average Filter



Fig. 6(d) Noise removal With Wiener Filter

Fig. 6 Removal of Gaussian Noise From Cameraman image with different Filters



Fig. 7 (a) Cameraman Image With Poisson Noise



Fig. 7(b) Noise removal With Median Filter



Fig. 7(c) Noise removal With Average Filter



Fig. 7(d) Noise removal With Wiener Filter

Fig. 7 Removal of Poisson Noise From Cameraman image with different Filters



Fig. 8 (a) Cameraman Image With Salt & Pepper Noise



Fig. 8 (b) Noise removal With Median Filter



Fig. 8 (c) Noise removal With Average Filter



Fig. 8 (d) Noise removal With Salt & Wiener Filter

Fig. 8 Removal of Salt & Pepper Noise from Cameraman image with different Filters



Fig. 9 (a) Cameraman Image With Speckle Noise



Fig. 9 (b) Noise removal With Median Filter



Fig. 9 (c) Noise removal With Average Filter



Fig. 9 (d) Noise removal With Wiener Filter

Fig. 9 Removal of Speckle Noise from Cameraman image with different Filters

A handwritten signature or mark in the bottom right corner of the page.

TABLE I: EXECUTION TIME OF DIFFERENT FILTERS OF CAMERAMAN IMAGE WITH DIFFERENT NOISES

Type of Noises	Type of Filters		
	Median	Average	Wiener
Gaussian	0.1388	0.13631	0.92193
Poisson	0.14914	0.16771	0.14113
Salt & Pepper	0.11961	<b>0.12426</b>	0.91137
Speckle	<b>0.09535</b>	0.14118	<b>0.08193</b>

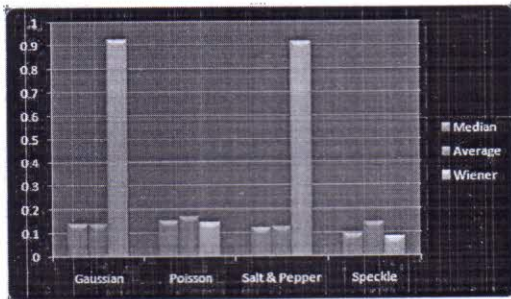


Fig. 10: Graphical Analysis of Execution Time

From Table I, it has been observed that the median, average and wiener filter behave differently for Gaussian, Poisson, Salt & Pepper and Speckle noise. This fact has been evaluated by performance measuring parameter i.e. execution time. For Gaussian noise, Median, Average and Wiener filter, the execution time is 0.13886 sec, 0.13631sec and 0.92193 sec respectively.

For Poisson noise, Median, Average and Wiener filter gives the execution time 0.14914 sec, 0.16771 sec and 0.14113 sec respectively. For Salt & Pepper noise, Median, Average and Wiener filter execution time 0.11961 sec, 0.12426 sec and 0.91137 sec respectively. Similarly for Speckle noise, Median, average and Wiener filter gives the execution time 0.09535 sec, 0.14118 sec and 0.08193 sec respectively.

TABLE II :ENTROPY OF DIFFERENT FILTERED CAMERAMAN IMAGES WITH DIFFERENT NOISES

Type of Noises	Type of Filters		
	Median	Average	Wiener
Gaussian	0.14397	7.01561	6.88412
Poisson	0.21365	7.02671	4.23211
Salt & Pepper	0.1689	6.5946	7.1983
Speckle	<b>0.32168</b>	<b>7.8623</b>	<b>7.2341</b>

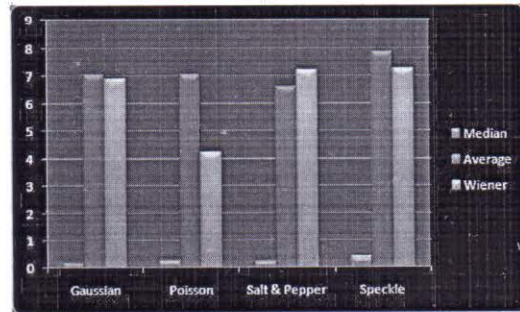


Fig 11: Graphical Analysis of Entropy

From Table II, it has been observed that the median, average and wiener filter behave differently for Gaussian, Poisson, Salt & Pepper and Speckle noise. This fact has been evaluated by performance measuring parameter i.e. entropy. For Gaussian noise, Median, Average and Wiener filter, the entropy is 0.14397, 7.01561 and 6.88412 respectively.

For Poisson noise, Median, Average and Wiener filter gives the entropy 0.21365, 7.02671 and 4.23211 respectively. For Salt & Pepper noise, Median, Average and Wiener filter has entropy 0.1689, 6.5946 and 7.1983 respectively. Similarly for Speckle noise, Median, Average and Wiener filter gives the entropy 0.32168, 7.8623 and 7.2341 respectively.

## VI.CONCLUSION

Noise removal serves as one of the crucial step for improving the quality of an image for visual interpretation. Effective de-noising can be achieved by filtering out the unwanted signals. From the analysis, it clearly depicted that among all the noises (Gaussian, Poisson, Salt & pepper and Speckle) speckle noise give the best entropy for median, average and wiener filter. For median and wiener filter least execution time is taken in comparison of other filters. Salt and pepper noise gives the best results on average filter.

## REFERENCES

- [1] Murat Alparson, Gungor and Irfan Karagoz, "The Effects of the Median Filter with Different Window Sizes for Ultrasound Images", Proc IEEE International Conference on Computer and Communications, pp 549-552,2016.
- [2] Chikako Abe and Tetsuya Shimamura, "Iterative Edge Preserving Adaptive Wiener Filter for Image De noising", International Journal of Computer and Electrical Engineering, Vol 4, No.4,pp 503-506, 2012.
- [3] Prajoy Podder and Md Mehedi Hasan," A Meta Study of Reduction of Speckle Noise Adopting Different Filtering Techniques, Proc IEEE International Conference of

114

- Electrical Engineering and Information Communication Technology, pp1-6, 2016.
- [4] G A Eninicke, "iterative Filtering and Smoothing of Measurements Possessing Poisson Noise", IEEE Transactions on Aerospace and Electronic Systems, Vol 51, No. 3, pp 2205-2211, 2015.
  - [5] Priyanka Punhani and Dr Naresh Kumar Garg, "Noise removal in MR Images using Non Linear Filters", Proc IEEE International Conference on Computing, Communication and Networking Technologies, pp1-6, 2015.
  - [6] Jingdong Chen, Jacob Benesty, Yiteng Huang and Simon Doclo, "New insights into the Noise Reduction Wiener Filter", IEEE Transactions on Audio, Speech and Language Processing, Vol 14, No 4, pp 1218-1234, 2006.
  - [7] Teng Li, Bingbing Ni, Mengdi Xu, Meng Wang, Qingwei Gao and Shuicheg Yang, "Data Driven Affective Filtering for Images and Videos", IEEE Transactions on Cybernetics, Vol 45, Issue 10, pp 2336-2349, 2015.
  - [8] Yi Wang, Jiangyun Wang, Xiao Song and Liang Han, "An Efficient Adaptive Fuzzy Switching Weighted Mean Filter for Salt and Pepper Noise Removal", IEEE Signal Processing Letters, pp 1582-1586, 2016.
  - [9] Sashikala Gurusamy and K Sidappa Naidu, "An Efficient De noising Method for Salt and Pepper Noise with Removal of Blur in an Original Image", Proc IEEE International Conference of Inventive Computation Technologies, Vol 3, pp 1-5, 2016.
  - [10] Qiao Jihong, Chen Lei and Chen Yan, "A Method for Wide Density Salt and Pepper Noise Removal", Proc IEEE Control and Decision Conference, pp 2940-2943, 2014.
  - [11] Isabel Rodrigues, Joa Sanches and Jose Bioucas Dias, "De noising of Medical Images Corrupted by Poisson Noise", Proc IEEE International Conference on Image Processing, pp 1756-1759, 2008.
  - [12] Suhailo Sari, Hazlu Roslan and Tetsuya Shimamura, "Noise Estimation by Utilizing Mean Deviation of Smooth Region in Noisy Image", Proc IEEE International Conference on Computational Intelligence, Modeling and Simulation, pp 232-236, 2012.
  - [13] Fitri Utamingrum, KeiichiaUchimura and Gou Koutaki, "High Density Impulse Noise Removal Based on Linear Median Filters", Proc IEEE Korean Japan Joint Workshop on Frontiers of Computer Vision, pp 11-17, 2013.

183

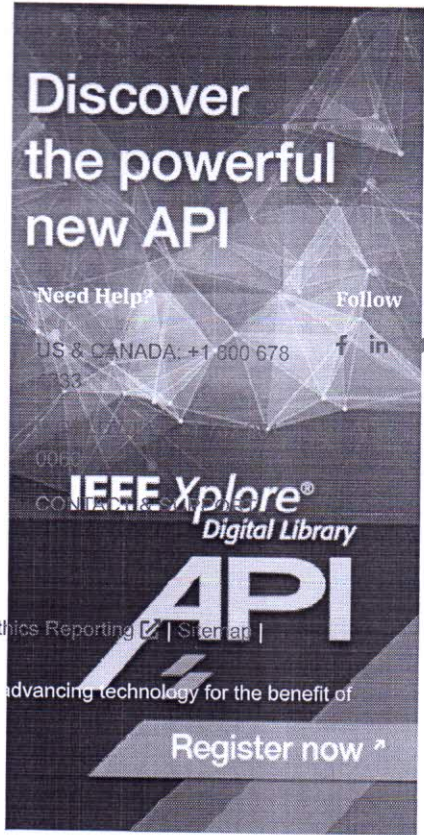
Authors	▼
Keywords	▼
Metrics	▼

[CHANGE USERNAME/PASSWORD](#)

[PAYMENT OPTIONS](#)  
[VIEW PURCHASED DOCUMENTS](#)

[COMMUNICATIONS PREFERENCES](#)  
[PROFESSION AND EDUCATION](#)  
[TECHNICAL INTERESTS](#)

[About IEEE Xplore](#) [Contact Us](#) [Help](#) [Accessibility](#) [Terms of Use](#) [Nondiscrimination Policy](#) [IEEE Ethics Reporting](#) [Sitemap](#) [Privacy & Opting Out of Cookies](#)



Discover the powerful new API

Need Help? Follow

US & CANADA: +1 800 678 4333

Worldwide: +1 732 981 0060

IEEE Xplore<sup>®</sup> Digital Library

**API**

advancing technology for the benefit of

Register now

**IEEE Account**

- » [Change Username/Password](#)
- » [Update Address](#)

**Purchase Details**

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

**Profile Information**

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)


**Need Help?**

- » [US & Canada: +1 800 678 4333](#)
- » [Worldwide: +1 732 981 0060](#)
- » [Contact & Support](#)

[About IEEE Xplore](#) [Contact Us](#) [Help](#) [Accessibility](#) [Terms of Use](#) [Nondiscrimination Policy](#) [Sitemap](#) [Privacy & Opting Out of Cookies](#)

IEEE Xplore is a registered trademark of IEEE. © Copyright 2012 IEEE. All rights reserved. IEEE is a registered trademark of IEEE. All rights reserved. IEEE is a registered trademark of IEEE. All rights reserved.



- Matrix Method for Non-Dominated Sorting and Population Selection for Next Generation in Multi-Objective Problem Solution** 

Prince Rajpoot; Pragya Dwivedi  
Publication Year: 2018 , Page(s): 670 - 676  
Cited by: Papers (6)

▶ Abstract [HTML](#)  

- Matrix Method for Non-Dominated Sorting and Population Selection for Next Generation in Multi-Objective Problem Solution** 

Prince Rajpoot; Pragya Dwivedi  
2018 8th International Conference on Cloud Computing, Data  
Science & Engineering (Confluence)  
Year: 2018

- Load Balancing for Virtual Resources Management in Data Center** 

Md. Owais Qurani; Ravinder Singh  
Publication Year: 2018 , Page(s): 677 - 682

▶ Abstract [HTML](#)  


- Load Balancing for Virtual Resources Management in Data Center** 

Md. Owais Qurani; Ravinder Singh  
2018 8th International Conference on Cloud Computing, Data  
Science & Engineering (Confluence)  
Year: 2018


- A Comparative Study of Security Features Provided by Different Cloud Services to Enterprises** 

Vansh Sirohi; Tanya Jain; Rachita Arora; Puja Munjal  
Publication Year: 2018 , Page(s): 683 - 687  
Cited by: Papers (1)

▶ Abstract [HTML](#)  

- A Comparative Study of Security Features Provided by Different Cloud Services to Enterprises** 

Vansh Sirohi; Tanya Jain; Rachita Arora; Puja Munjal  
2018 8th International Conference on Cloud Computing, Data  
Science & Engineering (Confluence)  
Year: 2018

- Reverse Engineering Technique (RET) to Predict Resource Allocation in a Google Cloud System** 

Biplob R. Ray; Sujan Chowdhury  
Publication Year: 2018 , Page(s): 688 - 693  
Cited by: Papers (3)

▶ Abstract [HTML](#)  

- Reverse Engineering Technique (RET) to Predict Resource Allocation in a Google Cloud System**



Date of Conference: 11-12 Jan, 2018 **INSPEC Accession Number:** 18044655  
 Date Added to IEEE Xplore: 23 August 2018 **DOI:** 10.1109/CONFERENCE.2018.8442448  
**ISBN Information:** **Publisher:** IEEE  
**Conference Location:** Noida, India

Citations Keywords Metrics More Like This  
 SUBSCRIBE Cart Create Account Sign In  
 IEEE.org IEEE Press IEEE-SA IEEE Spectrum Mini Sites  
 Browse My Settings Help Institutional Sign In

**Contents**

**I. Introduction**  
 Cloud Figuring out calculating has come out as an order of the day for service ruled figuring out/calculating where figuring out/calculating (basic equipment needed for a business or society to operate) and solutions are delivered as a service [1]. Nowadays a number of enterprises are encouraging the use of cloud computing as a feasible option as not only it reduces costs but also improves IT. **Significance of Cloud Computing** facilitates in providing the utilities to the information technology industry hence reducing the upfront cost of computing from deploying many cutting-edge IT service, furthermore it allows new functionality that not even within reach as of now. However, there are few major hindrances in the way of broader cloud adoption viz. security, interoperability, and portability [2] [3].

- Authors >
- Figures >
- References >
- Citations >
- Keywords >
- Metrics >

US & CANADA: +1 800 878 4333  
 WORLDWIDE: +1 732 981 0060  
 CONTACT & SUPPORT

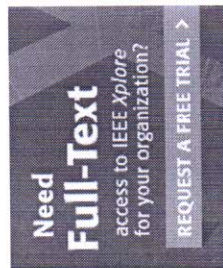
COMMUNICATIONS PREFERENCES  
 PROFESSION AND EDUCATION  
 TECHNICAL INTERESTS

PAYMENT OPTIONS  
 VIEW PURCHASED DOCUMENTS

CHANGE USERNAME/PASSWORD

About IEEE Xplore Contact Us Help Accessibility Terms of Use Nondiscrimination Policy IEEE Ethics Reporting Sitemap  
 Privacy & Opting Out of Cookies

q  
 ADVANCED SEARCH



**More Like This**

Efficient Secure Outsourcing Computation of Matrix Multiplication in Cloud Computing  
 2016 IEEE Global Communications Conference (GLOBECOM)  
 Published: 2016

Secure Collaborative Outsourced Data Mining with Multi-owner in Cloud Computing  
 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications  
 Published: 2012

[Show More](#)

All

Conferences > 2018 8th International Conf...

**A Comparative Study of Security Features Provided by Different Cloud Services to Enterprises**

**Publisher:** IEEE [Cite This](#) PDF

Vanah Sirshi ; Tanya Jan ; Rachita Arora ; Puja Munjal **All Authors**

111  
 Base Edition  
 Text Views

**Alerts**

Manage Content: Alerts  
 Add to Calendar: Alerts

**Abstract**

Document Sections  
 I. Introduction  
 II. Related Work  
 III. Principles of Security  
 IV. Services Provided by Cloud  
 V. Comparative Study of 3 CSP  
 Show Full Outline

**Abstract:** Cloud computing is a rapidly growing technology which offers enterprises to outsource their data and software to the cloud server while enabling them to respond to the ch... [View more](#)

**Metadata**

**Abstract:** Cloud computing is a rapidly growing technology which offers enterprises to outsource their data and software to the cloud server while enabling them to respond to the changes occurring in technology and operational environment. Organizations are expected to pay as per their use while utilizing the service offered by cloud service providers (CSP). But the main concern while outsourcing their data to the CSP is security which needs to be addressed since their data will be processed by the third party cloud. This paper presents a comparison of the services provided by three renowned CSP. Also this research study facilitates an enterprise to choose the best CSP based on the most important security parameter.

**Published in:** 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)

# A comparative study of security features provided by different cloud services to Enterprises

Vansh Sirohi, Tanya Jain, Rachita Arora, Puja Munjal  
Department of Information Technology  
Jagannath International Management School, Vasant Kunj  
New Delhi-110070, India

**Abstract**— Cloud computing is a rapidly growing technology which offers enterprises to outsource their data and software to the cloud server while enabling them to respond to the changes occurring in technology and operational environment. Organizations are expected to pay as per their use while utilizing the service offered by cloud service providers (CSP). But the main concern while outsourcing their data to the CSP is security which needs to be addressed since their data will be processed by the third party cloud. This paper presents comparison of the services provided by three renowned CSP. Also this research study facilitates an enterprise to choose the best CSP based on the most important security parameter.

**Keywords**— *cloud computing; security; enterprise; cloud service providers (CSP);*

## I. INTRODUCTION

Cloud Figuring out/calculating has come out as an order of the day for service ruled figuring out/calculating where figuring out/calculating (basic equipment needed for a business or society to operate) and solutions are delivered as a service [1]. Nowadays a number of enterprises are encouraging the use of cloud computing as a feasible option as not only it reduces costs but also improves IT and business buoyancy. Cloud computing facilitates in providing the utilities to the information technology industry hence reducing the upfront cost of computing from deploying many cutting-edge IT service, furthermore it allows new functionality that is not even within reach as of now. However, there are few major hindrances in the way of broader cloud adoption viz. security, interoperability, and portability [2][3].

In addition, the degree to which cloud computing can be subsumed into the business activities at all organizational level is what alignment between business and cloud computing is all about [4]. Strategic IT alignment is a pivotal element for the efficacious application of IT in a company [5]. As per the theories about organization fit, the success of calibration mainly depends upon the fit between the technology and the company.

Besides the overwhelming business and benefits of the cloud, the security and privacy concern has been one of the dominant impediments in its universal adoption. Especially for the outsourced data services, the owner's absolute control over their data is at last renounced to the cloud service providers (CSP's) [6]. In this paper Security parameters in cloud computing are explored and on the basis of same comparison

between different architecture based CSP which are AWS, Rackspace, Salesforce is done.

## II. RELATED WORK

Many new technologies are emerging in the booming IT sector including cloud computing which is set to reform the way we work in an enterprise. Almost all the vendors and enterprises are running to be a part of cloud friendly environment while neglecting their own economical processes and the values bought by cloud services which can be defined through two characteristics: utility and guarantee [7]. Whereas cloud computing has a major influence on an organization to make it's working easier it might as well cause a number of changes in the enterprise which provides it with numerous advantages as well as disadvantages to employees, employers and the enterprise. The major concern while using cloud computing is security. Therefore, a general model with seven key factors for cloud adoption is developed to support decision makers to investigate cloud adoption decisions [8]. A comparison between history of electrical power to the cloud computing and all the risks involved while choosing a discreet cloud service provider (CSP) [9]. In order to dodge the cloud computing failures an enterprise should first verify cloud security and analyze the security issues which are involved in the process of adoption and plan ways to resolve all of them before implementing it in the organization. Before moving to enterprise cloud computing planning should be done and this movement should be gradual over a period of time [10].

Data confidentiality, non-repudiation and integrity should be an enterprise's first priority while choosing a cloud service provider and to overcome all the security and privacy issues of cloud computing an enterprise should not only expect assurance from cloud side but verification and authentication from both CSP and the enterprise itself [11]. The technique to secure user data while using cloud computing is to sign the data using digital signature in association with certificates and establishing a secure authentication channel between TTPA and cloud server by sending and receiving challenges and responses [12]. To support the decision makers while adopting cloud computing services a general model for cloud computing adoption specifying seven key factors is developed [13]. The theory of the alignment of cloud computing is extended in order to improve the after-sale services of a cloud service provider in return which would enhance the alignment of cloud computing in enterprises and other industries with the help of Task

technology fit (TTF) and Technology organization compatibility (TOC) [14].

The lack of de facto standard is the biggest challenge in cloud computing. Therefore, a number of architectural features are classified which would play a major role in the decision making for an enterprise while adopting the cloud computing services and it is beneficial for the cloud service providers too since it gives the basic idea for creating future architectures [15]. To allow the continuity of a business by dodging the security issues an enterprise should do regular security updates and apply new patches [16]. Enterprises can move slowly towards cloud by initially keeping the highly confidential information to themselves and storing less secure data in cloud [17]. Number of studies has been conducted to state the risks offered by cloud computing revolving around privacy and security aspects forgetting the diverse legal, operational, organizational and technical areas which are causing major risk to the failure of cloud computing [18].

### III. PRINCIPLES OF SECURITY

There are mainly 4 factors which can facilitate the security in cloud services for the enterprise.



Fig. 1. Principles of Security

1. **Confidentiality:** Since the enterprises using cloud computing store their data in third party cloud therefore cloud service providers must ensure that the permission to access that data should only be granted to the authorized people and not to the others and these authorized people are expected to be trained against all the below listed risk factors which might cause their data to be passed into unauthorized hands.

- a. Confidentiality is directly affected by the leakage of data caused by an error occurred by human or hardware.
- b. The threats from inside user which could be customers, administrators, developers and environment managers are called inside user threats.
- c. Hardware attack, social engineering, chain attacks rooted on cloud service provider containing sensitive data like personal information, sensitive government or card details are called external user threat.

2. **Accountability:** At the time of server crash to guarantee minimum loss of data and to maintain the accountability and integrity of that data it is protected physically and cryptographically. Therefore, with the help of file permissions, user access controls and version controls the

accountability of data at the time of server crash or electromagnetic pulse ensures the accuracy, consistency and trustworthiness of data. Data integrity plays a vital role in the working of enterprise cloud computing and if any user introduces a faulty component in the system it will affect the integrity of other user's data. Ex-employees of cloud service providers could damage their data sources due to the lack of access. Due to lack of segregation of data, integrity can be risked.

3. **Accessibility:** Availability of the data on a software or hardware to any authorized organization is the property of accessibility of data which is maintained by communication with bandwidth. Due to natural calamities or hardware issues causing system crashes, bottlenecks and system redundancy backup data is provided. Due to insecure office environment external or internal physical disruption can happen.

4. **Trust:** It is the factor which defines relationship between an enterprise(customer) and a CSP. CSP should always be capable of gaining the trust of an enterprise(customer) by providing services or features in such a way that the enterprise(customer) believes in the working process of the CSP. CSP are given a task which requires at-most level of trust between CSP and enterprise(customer) that is a CSP handles highly confidential data of an enterprise(customer) so which makes trust a pivotal principle to work on.

### IV. SERVICES PROVIDED BY CLOUD

#### 1. SaaS (Software as a Service)

The cloud provider installs and manages the software which is rented to the enterprise as a form of SaaS (Software as a Service), also the better part is that it is not needed to be installed on every system before use. While using SaaS user can access their data anywhere and everywhere through internet and when the device on which the data is being accessed is misplaced still no data is lost. Enterprises can rent various apps according to their usage such as email, calendaring or business applications.

#### 2. IaaS (Infrastructure as a Service)

IaaS is used for accessing, monitoring and managing the infrastructure equipment. With this digital concept a user can access their computers, storage and infrastructure. It provides a centralized platform for the operating systems, networking, security and servers, in such a way that it reduces costs.

#### 3. PaaS (Platform as a Service)

PaaS is a model which facilitates development of applications and services by providing a specific platform. User can access their data which is hosted in the cloud via any internet connection. PaaS uses point-and-click tools to establish web applications like Database development and testing.

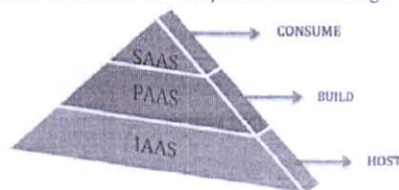


Fig. 2. Services provided by Cloud

## V. COMPARATIVE STUDY OF 3 CSP

There are various cloud Service providers to the enterprises few names are Microsoft Azure service platform, cloud sigma, E24 cloud, Google cloud platform etc.

In this research study mainly three diversified cloud service providers are taken which are AWS, Rackspace and Salesforce on the basis of cloud service model they provide

- a) *Amazon Web Service: (AWS)* is among one of the most opted providers [19]. It mainly facilitates IaaS.
- b) *Rackspace:* is providing PaaS and thousands of organizations, including global enterprises are using Rack space [20].

- c) *Salesforce:* is the consumer based service provider (SaaS) and is ranked World's No. 1 CRM (Customer Relationship Management) platform [21].

Table 1 Illustrates the comparison study based on 4 Principles of Security i.e. Confidentiality, Accountability, Accessibility and Trust. Further in Table 2 Security being the major concern while an enterprise selects to migrate on cloud, it should not be fuddle about the responsibilities of the user and the CSP. These responsibilities are differentiated on the basis of services (IaaS, PaaS, SaaS) opted by enterprises(customers) and provided by CSP. This table put forward the cloud security responsibilities of CSP and enterprises (customers).

Table 1. Comparisons between Principles of Security for Cloud Service Providers

POS	AWS(IAAS)	RACKSPACE(PAAS)	SALESFORCE(SAAS)
Confidentiality	<p><b>1. Identity and Access Control:</b></p> <ul style="list-style-type: none"> <li>• AWS provides IAM (Identity Access management) which is permission based access control system.</li> <li>• AWS multi factor authentication.</li> </ul> <p><b>1. DDoS Mitigation (Distributed Denial of Service attack):</b> It is a way to make an internet service unavailable via devastating it with traffic more than one source.</p>	<p><b>1. Access Control:</b> It provides permission based access control.</p> <p><b>2. Managed Security Service:</b> Branch detection-active Search for threats 24*7 and Minimizing breach Windows.</p>	<p><b>1. Password Policies:</b></p> <ul style="list-style-type: none"> <li>• Password expiration</li> <li>• Password length</li> <li>• Password complexity</li> </ul> <p><b>2. Two-Factor Authentication:</b> It offers two-part-related (verifying someone's identity) which calls for that all login attempts have each usernames and passwords and a 2nd (verifying someone's identity) aspect. this could be (accomplished or gained with effort) by using the Salesforce.</p>
Accountability	<p><b>1. Data Encryption:</b> Amazon S3 (turns into secret code) your records on the item level as it writes it to disks in its data centers and (changes secret codes into readable messages) it for you when you access it through server side (turning messages into secret code).</p> <p><b>2. Cryptography:</b> Cryptographic keys. AWS provides Amazon cloud HSM (Hardware Module) which provides Secure cryptographic key storage.</p>	<p><b>1. Host and network protection:</b> They provide (raised, flat supporting surface) which is targeted at non-harmful programs or apps attacks and even traditional (back-and-forth conversation to agree on something) (success plans/ways of reaching goals). Through this Rackspace provide advance host and network protection.</p> <p><b>2. Vulnerability management:</b> Uses scanning and agent technologies to understand your (surrounding conditions) and custom-design their Customer Security Operations Center response to threats and attacks.</p>	<p><b>1. My Domain:</b> Custom domain can draw special attention to your brand and secure your organization this can be done by My domain.</p> <p><b>2. Login IP Ranges:</b> User can login to salesforce from their IP addresses typically your corporate network or VPN. This will restrict the unauthorized access.</p> <p><b>3. Decrease Session Timeout Thresholds:</b> Sometimes user don't log off their computers, by using the automatically closing sessions you can protect your computer programs from approved access</p>

POS	AWS(IAAS)	RACKSPACE(PAAS)	SALESFORCE(SAAS)
<b>Accessibility</b>	<ol style="list-style-type: none"> <li>1. Data transfer at just the right speed.</li> <li>2. User can control their place of data.</li> <li>3. Effortless data replication.</li> </ol>	<ol style="list-style-type: none"> <li>1. Global Infrastructure.</li> <li>2. 24 x 7 x 365 Cyber Security Operations Center (CSOC).</li> <li>3. Multiple layer redundancy</li> </ol>	<ol style="list-style-type: none"> <li>1. 24 x 7 data availability across the globe.</li> </ol>
<b>Trust</b>	<ol style="list-style-type: none"> <li>1. <b>AWS Macie:</b> It works on the principle of Artificial Intelligence in which security is provided through machine learning techniques thus providing new discoveries and exploring of sensitive data.</li> <li>2. <b>Amazon Inspector:</b> It automatically applications for vulnerabilities or deviations.</li> </ol>	<ol style="list-style-type: none"> <li>1. <b>Log management:</b> Rackspace will collect Standard operating system logs and work with you to identify additional data that may be collected. All log data is retained for one year with additional retention facility available.</li> <li>2. <b>Threat remediation:</b> Self-capable of acting on Anomalous events on enterprise behalf on Pre-approved actions.</li> </ol>	<ol style="list-style-type: none"> <li>1. <b>Educate Users About Phishing:</b> Salesforce highly advocates phishing education for all Salesforce users. Most computer-attacks use harmful programs or apps (evil and cruel software) to infect a computer with evil and cruel code designed to steal passwords, data, or disrupt a whole computer/network.</li> </ol>

Table 2. Responsibility Matrix of CSP and Enterprises

Responsibility	SaaS		PaaS		IaaS		On-Premises	
	CSP	E	CSP	E	CSP	E	CSP	E
Data Governance		✓		✓		✓		✓
End Points		✓		✓		✓		✓
User access management		✓		✓		✓		✓
Identity Infrastructure	✓	✓	✓	✓		✓		✓
Application	✓		✓	✓		✓		✓
Network Control	✓		✓	✓		✓		✓
OS security	✓		✓			✓		✓
Hosts	✓		✓		✓			✓
Network	✓		✓		✓			✓
Data center	✓		✓		✓			✓

CSP	Cloud Service Providers
E	Enterprise

## VI. CONCLUSION

Cloud Computing is creating worldview of conveying IT administrations to shoppers as a utility benefit over the Internet.

The colossal advantage of cloud figuring is that the cloud offers assets to numerous clients whenever progressively and as indicated by client needs.

Likewise, clients just pay for the administrations that they require. Nonetheless, paying little heed to the way that the cloud offers a few advantages for endeavors from adaptability to diminishing cost, moving a current framework to the cloud isn't a simple assignment for the reason that there are various variation challenges in various spaces and the most important challenge is Security.

Security being the major concern for an enterprise to migrate on cloud, this preliminary research work enriches the knowledge of an enterprise about what Security features will be provided if they choose (IAAS or PAAS or SAAS) cloud service for the enterprise. This comparative study was done on 3 renowned companies providing different services and illustrated the services based on 4 principles of security i.e. Confidentiality, Accountability, Accessibility and Trust.

This research paper facilitates enterprises in figuring out what kind of security their Enterprise data need in order to successfully migrate to a cloud and will support in decision making process of an enterprise.

## VII. REFERENCES

- [1] Foster, Ian, et al. "Cloud computing and grid computing 360-degree compared." Grid Computing Environments Workshop, 2008. GCE'08. Ieee, 2008.
- [2] Dubey, Abhijit, and Dilip Wagle. "Delivering software as a service." *The McKinsey Quarterly* 6.2007 (2007): 2007.
- [3] Patrascu, Alecsandra, and Victor-Valeriu Patriciu. "Logging for cloud computing forensic systems." *International Journal of Computers Communications & Control* 10.2 (2015): 222-229.
- [4] Mingxing, Shao, Peng Long, and Fan Yanan. "Empirical Study on Alignment of Cloud Computing in Enterprises." *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2015 International Conference on. IEEE, 2015.
- [5] Tallon, Paul P., and Alain Pinsonneault. "Competing perspectives on the link between strategic information technology alignment and organizational agility: insights from a mediation model." *Mis Quarterly* (2011): 463-486.
- [6] Li, Ming, et al. "Toward privacy-assured and searchable cloud data storage services." *IEEE Network* 27.4 (2013): 56-62.
- [7] Avram, Maricela-Georgiana. "Advantages and challenges of adopting cloud computing from an enterprise perspective." *Procedia Technology* 12 (2014): 529-534.
- [8] Pantelić, Ognjen, Ana Pajić, and Ana Nikolic. "Analysis of available cloud computing models to support cloud adoption decision process in an enterprise." *Computers Communications and Control (ICCCC)*, 2016 6th International Conference on. IEEE, 2016.
- [9] Onwudebelu, Ugochukwu, and Benedict Chukuka. "Will adoption of cloud computing put the enterprise at risk?" *Adaptive Science & Technology (ICAST)*, 2012 IEEE 4th International Conference on. IEEE, 2012.
- [10] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." *Computer Science and Electronics Engineering (ICCSEE)*, 2012 International Conference on. Vol. 1. IEEE, 2012.
- [11] Tsai, Chang-Lung, et al. "Information security issue of enterprises adopting the application of cloud computing." *Networked Computing and Advanced Information Management (NCM)*, 2010 Sixth International Conference on. IEEE, 2010.
- [12] Subha, T., and S. Jayashri. "Efficient privacy preserving integrity checking model for cloud data storage security." *Advanced Computing (ICoAC)*, 2016 Eighth International Conference on. IEEE, 2017.
- [13] Goyal, Pankaj. "Enterprise usability of cloud computing environments: issues and challenges." *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)*, 2010 19th IEEE International Workshop on. IEEE, 2010.
- [14] Mingxing, Shao, Peng Long, and Fan Yanan. "Empirical Study on Alignment of Cloud Computing in Enterprises." *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2015 International Conference on. IEEE, 2015.
- [15] Rimal, Bhaskar Prasad, et al. "Architectural requirements for cloud computing systems: an enterprise cloud approach." *Journal of Grid Computing* 9.1 (2011): 3-26.
- [16] Bisong, Anthony, and M. Rahman. "An overview of the security concerns in enterprise cloud computing." *arXiv preprint arXiv:1101.5613* (2011).
- [17] Sabahi, Farzad. "Cloud computing security threats and responses." *Communication Software and Networks (ICCSN)*, 2011 IEEE 3rd International Conference on. IEEE, 2011.
- [18] Dutta, Amab, Guo Chao Alex Peng, and Alok Choudhary. "Risks in enterprise cloud computing: the perspective of IT experts." *Journal of Computer Information Systems* 53.4 (2013): 39-48.
- [19] Jefferies "Amazon's AWS Still the Only Cloud People Want" By Tiernan Ray Says Barron's. <http://www.barrons.com/articles/amazons-aws-still-the-only-cloud-people-want-says-jefferies-1506441053>, September 26, 2017.
- [20] "#1 hosting provider for the Internet Retailer Top 1,000 ecommerce websites (for the third consecutive year)", Says Magic Quadrant for Public Cloud Infrastructure Managed Service Providers Worldwide <https://www.gartner.com/doc/3627018/magic-quadrant-public-cloud-infrastructure,2017>.
- [21] "The innovative company behind the world's #1 CRM platform", Says IDC Worldwide Semiannual Software Tracker, [https://www.idc.com/tracker/showproductinfo.jsp?prod\\_id=521](https://www.idc.com/tracker/showproductinfo.jsp?prod_id=521), May 2017.

Click on a row for full paper view. Multiple papers can be accessed at a time in a new tab. The list can be sorted by clicking on column heading. Type in the search bar to search according to paper ID, title or author name.

| Track # 1 |

**Sustainable Computing**

| Track # 2 |

**High Performance Computing**

| Track # 3 |

**High Speed Networking and Information Security**

| Track # 4 |

**Software Engineering and Emerging Technologies**

| Track # 5 |

**4th International Workshop on Information Engineering and Management (IWIEM 2018)**

| Track # 6 |

**ICT Based Innovations**

| Track # 7 |

**Next Generation Computing**

| Track # 8 |

**Next Generation Networking**

| Track # 9 |

**Software, Systems & Architecture**

**-: All Papers Listed Below :-**



SID	TID	PID	Title	Authors
1	3	642	A Graphics-Hardware based Approach for Reliability Analysis of Wireless Communication Systems	Shabbir Ahmad and R. L. Shrama
1	3	803	Malware Behavior Analysis based on System Calls	Yogesh Chandra and Sneha Chatterjee
1	3	840	Analysis of Wireless Networking Attacks on Robots	Gaurav Nale, Sharayu Sathe and Umesh Kulkarni
1	3	846	Security Threats in Cloud Computing and their Counter Measures	Nitish Pathak, Garima Malik and Aarush Verma
1	3	921	Proposed Security Solutions at Different levels of Network Required in UIDAI System	Arpana Chaturvedi and Vinay Kumar
1	3	940	Cyber Terrorism: Literature Survey on Attack Taxonomies and their Classification	Harshit Tripathi, Suresh Kumar Rewar, Mukund Kumar, Indu Kashyap and Prasenjit Banerjee
1	3	955	Game Theory based Attack Graph Analysis for Cyber War Strategy	Pallaw Kumar Mishra and Garima Tyagi
1	3	968	Denial of Service Attack: Modus Operandi and Current Status	S.M.K. Quadri and Suhail Qadir Mir
1	3	1133	S.M.K. Quadri and Suhail Qadir Mir	Ashish Sharma and Nausheen Khilji
1	3	3130	Survey on Factorization of RSA using Quantum Computer	Kunal Gagneja and K. John Singh
2	3	1158	Dissection of Ransomware: A Detailed Analysis	Prachi and Suchita Jangir
2	3	1180	SMX Algorithm: A Novel Approach to Avalanche Effect on Advanced Encryption Standard AES	Sohail Shahul Hameed and Bhargavi Goswami
3	3	1227	IoT: A Structured System with Research Challenges and Future Directions	Rohit Goyal, Manmohan Singh Rauthan, Rakesh Ranjan and Rakesh Arya

Showing 176 to 200 of 761 entries

Previous 1 ... 7 8 9 ... 31 Next

[Papers \(papers.html\)](#) [Organizer \(organizer.html\)](#) [Sponsors \(sponsors.html\)](#) [Committee \(committee.html\)](#) [Contact \(contact.html\)](#)

© Copyright INDIACom-2018 ISSN: 0973-7529 ISBN: 978-93-80544-29-8

Application Designed & Developed by : **BVICAM**

Application Maintained by: **Ankit Jain**

MCA Batch 2016-2019, BVICAM



# Proposed Security Solutions at Different Levels of Network Required in UIDAI System

**Ms. Arpana Chaturvedi**

Dept. Of Information Technology  
Jagannath International Management School  
JIMS, OCF, Pocket 9, Sector-B, Vasant Kunj  
New Delhi, INDIA  
Email ID: pcord.bca@jagannath.org

**Dr. Vinay Kumar Authors**

Vivekanand School Of IT  
Vivekanand Institute Of Professional Studies  
VIPS, GGSIPU  
New Delhi, INDIA  
Email ID: vinay5861@gmail.com

**Abstract**— Aadhaar System provides many positive solutions to citizen of India and has various positive impacts for India. It manages benefits in more efficient and easier way for India but making it mandatory to avail benefits might be a major security issue and might not be a right decision. It makes the Aadhaar database main target for exploitation and increases the security risk behind it. Another major security issue against privacy rights is forcing Aadhaar mandatory to file taxes. Identification and Authentication are basic independent and necessary information required for any communication. It is required at the time of request by any requestor to access services. As per the security principle and standard notion of digital authentication, one must provide both identification and authentication. Requestor can provide user id, login id, email id etc but authentication should always be a conscious process. Process execution must execute with active participation of a user. In the current scenario, the way government is forcing to link Aadhaar Card with different services, while using the Aadhaar details they rarely involve active participation of the owner. Apart from Authorization and Authentication, there are so many other security issues lying at different levels and which are to be taken care of. In this paper the solution to various security issues are proposed and suggested to implement in UIDAI system.

**Keywords** — Cryptography, UIDAI, Authentication, Identification.

## I. INTRODUCTION

Aadhaar project is for the citizen of Indian to provide first biometric identity to all [1]. At the same time population is growing exponentially hence it is became important to review minutely the availability and implemented features of the UIDAI project. It is must that the project should be extendible, secure, reliable, scalable and interoperable. The whole Enterprise, Application, Data and Security architecture should be reviewed. Application architecture should properly understood and reviewed at Central as well as State/UT level in terms all features and specifically security. The System level interaction based architecture has also to be reviewed in terms of features like its interaction with UID and partner system. While deployment of architecture, what applications are required at each level, working of central unit, working of state and union territory unit and application release strategy. After

understanding the entire UIDAI System, it is must to understand the revised security requirement and protection of information to have a much reliable, scalable and secure system. In this paper the discussion is composed of Existing Aadhaar Application, Existing Security Features, Drawbacks of existing UIDAI System, Issues related to security breach to privacy, Key Security considerations to meet the entire enterprise data security of UIDAI System, Privacy protection from different level of security threats. We proposed security architecture with the suggestions of different security algorithm which if might get implemented can provide better security controls at different levels and better privacy controls to the personal data. The paper is organized in five sections. Section 2 includes the concept of Aadhaar application, Existing Security Features, Drawbacks of Existing Security features. Section 3 includes the Key Security consideration required to be reviewed by Enterprise architecture, Issues related to Security breach an Authentication process in UIDAI. Section 4 includes the proposed security architecture and security algorithm to be implemented at different levels. Section 5 includes conclusion with the future benefits of UIDAI system and Section 6 includes acknowledgement.

## II. AADHAAR APPLICATION, EXISTING SECURITY FEATURES AND ITS DRAWBACKS

### A. Aadhaar Application

Aadhaar Application runs on commodity multi-core blade Linux servers with 8086 64-bit architecture on a 10 Gbps (Giga Bit per Second) network. It is written in Java language using open source components and frameworks. The partner ecosystem is explained in Fig.1. The System has the large scale OS with large-scale storage i.e. SATA (Serial Advanced Technology Attachment) with the smaller storage having SSDs (Solid State Device). The application has heterogeneous compute and storage infrastructure and it works uniformly as a compute/storage cluster.

The Existing system has approximately 30,000 enrolment stations deployed by registrars, around 10,000+ trained and certified operators and supervisors to operate the Enrolment Station[1][2][4]. Enrolment station enrolls approximately 50 people in a day and approximately 1 million enrolments per

day on the field. The growth of population is natural and the existing architectures is required to be revised to enhance scalability and extensibility.

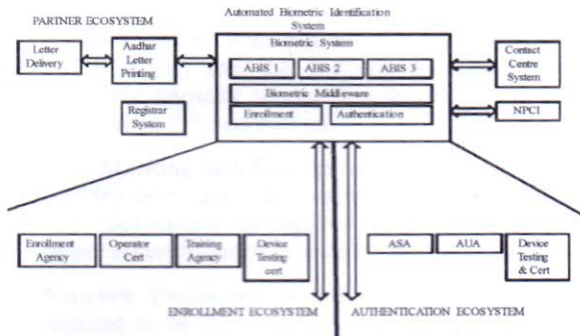


Fig. 1. Working of Partner Ecosystem

**B. Existing Security Features in UIDAI**

- Implementation of 2048 bi Public Key Infrastructure (PKI) encryption of biometric data during transit. Availability of End to end encryption from enrolment to Central Identities Data Repository (CIDR). [2][3][14]
- Trusted network carriers i.e. Authentication Service Agencies (ASAs) between Central Identities Data Repository (CIDR) and Authentication User Agencies (AUAs). Effective precautions against denial of service (DoS) attacks.
- HMAC (Hash Message Authentication Code) based tamper detection of PID (Personal Identity Data) blocks, which encapsulate biometric and other data at the field devices[12].
- Registration processes and authentication processes of AUAs.
- Hash of Aadhaar number generated using (Secure Hash algorithm) SHA-n is stored in CIDR.
- Storing of Audit trails in SHA-n encrypted form, with HMAC based tamper detection.
- Biometric data is stored in original form whereas password and PINs are stored in HASH form.
- Protection against replay attacks is implemented by unique session keys and HMAC for Authentication requests.
- Vertical partitioning or 100 way shard is used to store Resident data in which first two digits of Aadhaar numbers are used as shard keys.
- RefIDs i.e. coded indices are used for an enrolment and update requests link to partitioned databases.
- All system and its administration accesses through a hardware security module (HSM) which maintains an audit trails.

- All analytics carried out only on anonymised data.
- C. Drawbacks of existing security measure*

- Unauthorized and surreptitious examination, log and audit trails and transaction records leads to profiling and surveillance against targeted people or against individuals.
- There are no security measures which have been taken against insider attacks. It might results as the biggest security and privacy threat.
- There are no security measures taken to protect keys used to decode encrypted data as most of the cryptographic encryption techniques are used which uses keys to decode them.
- All the Hardware Security Modules are under administrative control. We cannot rely on insiders as they might get compromised by insider attacks.
- Non existence of strong tamper detection and frequent audit of field devices. Enrolment agencies are required to ensure whether the field devices are working as per the norms and specifications or not. The system does not provide any assurance that whether any possibilities of data leakages exists or not.
- In the CIDR in spite of crucial user credentials like Biometric information only non-invertible intermediate representations for matching of data should be stored.

**III. KEY SECURITY FEATURES REQUIRED TO BE REVIEWED IN EXISTING ENTERPRISE ARCHITECTURE OF UIDAI**

A holistic approach is required to meet the entire enterprise data security of UIDAI System based on Hadoop and the key considerations (Fig. 2) to secure the entire UIDAI Ecosystem are[1][2][3][8][20]:

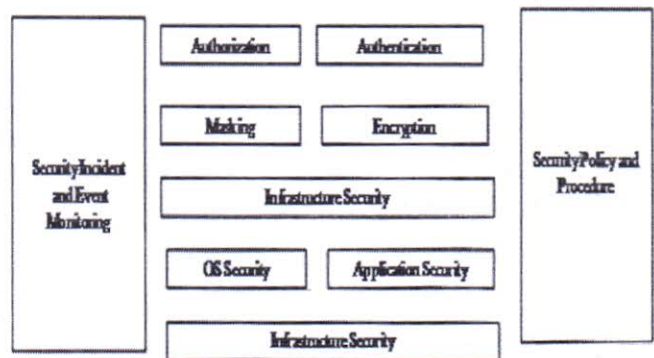


Fig. 2. Key Considerations to Secure UIDAI System

- **Authentication:** A single point of authentication should be available in the system. This point is of authentication should be aligned and integrated with the existing UIDAI identity and access Management.

103

- **Authorization:** A role based authorization is required to be enforced in the system. To provide access to the sensitive data the system should also have a fine grained access control.
- **Access Control:** Who can do what on UIDAI Dataset and who can use the Dataset, how much of the processing capacity should be available in the clusters are required to be controlled.
- **Data Masking and Encryption:** Proper encryption and masking techniques on biometric and demographic data of an individual's are required to be deployed to ensure secure access to sensitive data for authorized personnel.
- **Network Perimeter Security:** Perimeter security is required to be deployed for the overall Hadoop based UIDAI system. It is necessary to control how the data can move in and move out of the ecosystem to the other infrastructures.  
Design and implementation of the network topology is required to provide proper isolation between the UIDAI system and rest of the enterprise.  
To prevent unauthorized traffic, proper network level security is required by configuring the appropriate firewall rules
- **System Security:** It is required to harden the Operating System and the applications installed in the UIDAI system to provide system level security. All vulnerabilities of Operating System and applications are required to be addressed.
- **Infrastructure Security:** Strict infrastructure and physical access security is required to be enforced in the Data Centres.
- **Audit and Event Monitoring:** To provide Audit Reports for various activities like accessing and processing of data, retrieving of data a proper audit trail is required. It is also required for any changes that occur within the UIDAI Ecosystem.

A. Issues related to the security breach of privacy:

- a) **Identification without consent[12]:**
  - Global Aadhaar ids should be used to track individual activities across multiple domains of services (AUAs) as arises due to existence of correlation of identities across domains by available possibilities. Possibility of use of *Identification without consent* is more likely to arise as Aadhaar ids are valid across all domains.
  - There is always the possibility of illegal use or unauthorized use of demographic data or biometrics in the System. It may be because of not an appropriate match of fingerprints, iris scans, or photographs of an individual. The inappropriate matching process with the Aadhaar or AUAs database can lead to *identification without consent*.
- b) **Surveillance without legal or authorized sanction:** Illegal use of stored authentication and identification

related information, trails of an individual with respect to location, time can be used track and put individual under *surveillance without legal or authorized sanction*.

- c) **Possibilities of Insider Attacks:** The most dangerous threat is the involvement or *possibility of insiders attacks*. The other party's attacks are only possible or more likely due to involvement of insiders. Insiders are the elements who have access to all components of the Aadhaar System.

B. Privacy Protection:

Privacy protections are required to strongly protect stored data, logs and transaction trials data. [12] Privacy Protection is not only required for Aadhaar or AUA's database but also for internal and external attacks. Insider Leaks, System Hacks, Tampering with authenticated records and audit trails are certain factors due to which it is difficult to trust the existing UIDAI system.

Pre-approved, audited and tamper proof digitally signed computer program are required to perform proper authorized. It is difficult to trust the Enrolment Agencies, Enrolment Devices, Point of Sale devices and various government or private AUAs from the view of data privacy, protection and security point.

All government and private Authentication User Agencies (AUAs) are also can't be trusted with biometric, demographic data, sensitive and private user data related to its medical and immunization records. To ensure the trust and reliability of the system, strong legal frameworks and policy frameworks are required.

Pre-approved, audited and tamper-proof programs should only be allowed to perform *correlation of identities*. It is essential for carrying declared data analysis otherwise it should not be possible at any cost in other situations.

C. Existing Authentication Process in Aadhaar:

Aadhaar authentication is the process of verification wherein Aadhaar number along with demographic, biometric and OTP details are submitted to the UIDAI's CIDR.[12] CIDR verifies whether the data submitted is matches with the data available in CIDR or not. If it matches, the system responds back in Yes otherwise in No. This authentication is used in various ways by service delivery agencies. Few are:

- a) Authentication process used to match Aadhaar number and the demographic details like Name, DOB, address etc. of the resident stored in CIDR.
- b) Authentication of residents through OTP delivered to resident's registered mobile number or email id stored in the CIDR.
- c) Authenticate by using any one of the biometric modalities stored in the CIDR.
- d) Authenticate using OTP and any one of the biometric modalities stored in the CIDR.

102

- e) Authenticate using OTP and two of the biometric modalities stored in the CIDR.

*D. Drawbacks and Proposed Solution for Authentication process in Aadhaar:*

In the existing authentication process private Biometric details may get compromised and get problematic. [6] These are chances of intentional fraudulent which may take place by lifting fingerprints of the resident from different objects that the resident may touch or by picking iris details of the resident using high resolution and directional cameras without his/her consent.

It is suggested to use always at least one private biometric detail in conjunction with other public authentication details including the consent of individual. [9][10] It may vary as per the situations and circumstances but should ensure that right authentication procedure be implemented. Government has made Aadhaar mandatory to file Income Tax Return (ITR), to obtain Permanent Account Number (PAN), to get benefits of MNREGA, subsidies etc. The inter-linkage of Aadhaar data to facilitate benefits to individuals required proper authentication and identification. Hence there should be clear distinction between authentication and identity verification required in any process. It is also required to be incorporated the same in the Authentication architecture and in the legal and policy framework [15].

**Identification without consent:**

Aadhaar number is publicly available to avail various services and lies across multiple service domains. It increases the risk of misuse of information of the resident without his or her consent and leads to multiple breaches in privacy. It also increases the theft of identity of a resident in various harmful ways.

Lack of mapping between them mitigates the risk of breaches in privacy and increases the possibility of leakage of Aadhaar numbers from AUAs database during processing. Aadhaar id is a lifetime identity and once it gets compromised or identity gets stolen, it will become very difficult to revoke it.

**IV PROPOSED SECURITY SOLUTION TO OVERCOME THE ISSUES AND SECURITY ARCHITECTURE FOR IMPLEMENTATION**

*A. Proposed Solution to overcome the issues:*

Each and every resident should be mandatory allotted with domain-specific identifier. To overcome various issues both domain-specific identifier and global identifiers should be mapped and used. The suggested ways to solve authentication and identification issues are:

- 1) AUAs should use domain-specific identifiers and should do the proper mapping between global Aadhaar ids and various domain-specific identifiers like the bank account, PAN numbers, passport numbers, driving license numbers,

ration card numbers etc. It is very much required while dealings verifications of authentication and identifications to provide various services to right beneficiaries.

- 2) UIDAI should issue unique local identifier for different domains and to associate them cryptographically with the unique global identifier. It is suggested that to avoid correlation across multiple domains, a strong cryptographic measure required to be embedded with the master unique global identifier. It provides a way to make impossible the chances of identity theft as it will be difficult to know the global unique identity of an individual.
- 3) Allow linking of identifiers lying with different domains and UIDAI or AUAs in a bidirectional way. Hence a strong policy framework should be revised having incorporated data analysis software which should be cryptographically secure, should prevent external correlation attackers, ensure bidirectional linking between local identifiers embedded with cryptic master identifiers[16].

*B. Proposed Architecture for Security Implementation:*

A typical UIDAI system and its interaction with various stakeholders are shown in the Fig. 3. To implement security in each of these interactions requires elaborate planning and careful execution. The reference architecture mentioned in Fig.3 is dedicated in the following diagram summarizes the key security pillars that need to be considered for securing the UIDAI System.

In Distributed System, the first step is to establish trust between parties. [18] This is done with the authentication process where the Client sends its password to the server and the server verifies the password. The sent password may get compromised if the client sends password over an unsecured network. It is proposed to use Kerberos, a secured network authentication protocol. It doesn't transfer the password over the secured network and provides much stronger authentication for all client/server applications.

Working of Kerberos depends upon time sensitive tickets generated using symmetric cryptography. Kerberos is derived from Greek mythology where it means three headed dog. They guard the gates of Hades and in the security the three heads are:

- The user who is trying to authenticate
- The service to which client is trying to authenticate
- Kerberos security server is known as key distribution centre and is trusted by both the user and the service. The KDC stores the secret keys (passwords) for the users and services that would like to communicate with each other.

KDC provides two main functionalities known as Authentication Service and Ticket Granting Services. Authentication Service is responsible for authenticating the users and services, while the TGS provides a ticket that is time limited cryptographic message. [20] This ticket is used by client to authenticate with the server

101

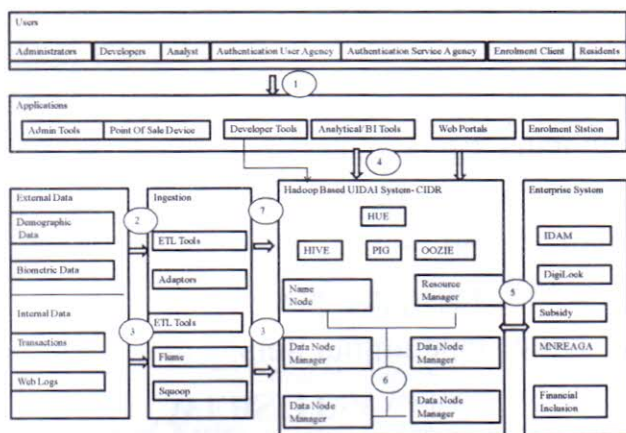


Fig.3: Reference Security Architecture

**Working of Kerberos:** [7] [18] The authentication and authorization flow in a Kerberos cluster is shown in the Fig. 4. It primarily aims at Client-Server Model and provides mutual authentication to both user and the server verify each others. The protocol follows process in four steps.

- User Client Based Logon
- Client Authentication
- Client Service Authorization
- Client Service Request

The client authenticates itself to the Authentication Server (AS) which forwards the username to a Key distribution centre (KDC). The KDC issues a Ticket Granting Ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in.

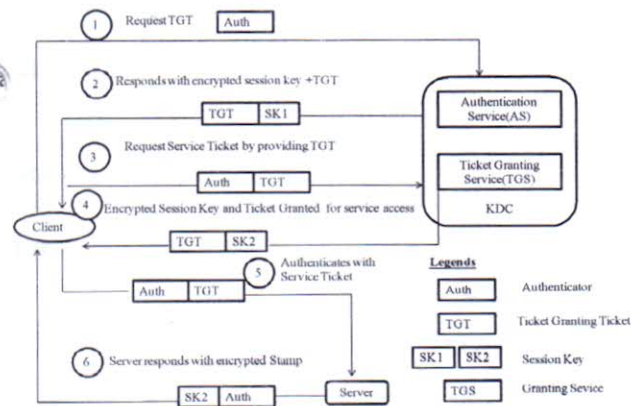


Fig. 4: Working of Kerberos

When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to

the Ticket Granting Service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a Ticket and session keys, which are returned to the client. The client then sends the Ticket to the service server (SS) along with its service request.

- Kerberos protocol is executed generally 3 phases and they are:

**Phase I in Kerberos**

In the first phase the user logs on to the Authenticating agency and it provides the user with a ticket of logging in to the session.

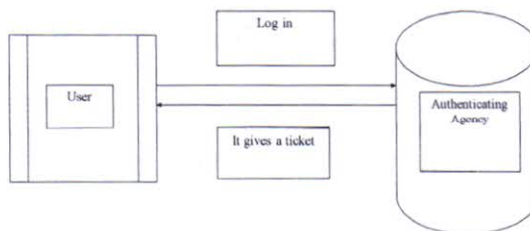


Fig. 5: Phase I in Kerberos

**Phase II in Kerberos**

In the second phase the user tries to connect to the data server agency and asks permission to access data. The data server requires the user to provide it with a token, so that it can know that it is the authenticate user which can be permitted to use data.

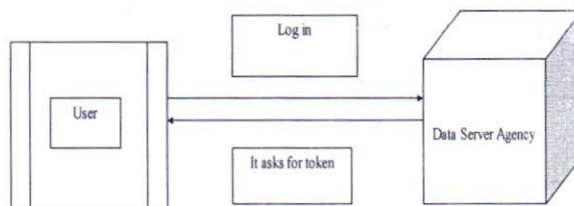


Fig. 6: Phase II in Kerberos

**Phase III in Kerberos**

In the third phase the user again connects to the given by the data server agency. Thus the authenticating agency and sends them the same message as authenticating agency creates a token (which contains a secret key shared between authenticating agency and the data server). This token is forwarded by the user to the data serve, which verifies and then gives permission to the user to access the data.

Since the protocol is time-sensitive, it is required that all the machines which communicate with each other should have the time synchronized with a maximum lag of five minutes. If any server time offset is more than five minutes, it will not be able to authenticate.

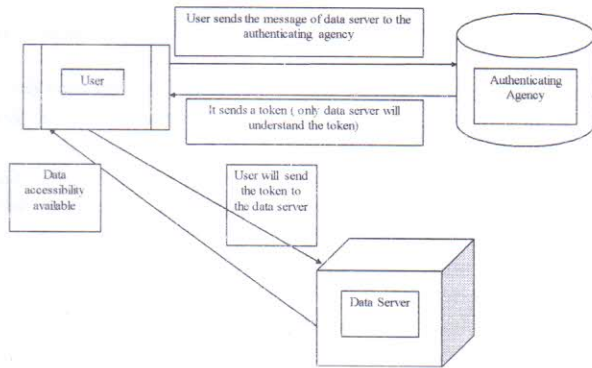


Fig. 7: Phase III in Kerberos

**Advantage of Kerberos:** [7] [18] The advantage of using Kerberos:

- A password never travels over the network. Only time sensitive tickets will travel over the network.
- Passwords or secret keys are only known to the KDC and the principal. This makes the system scalable for authenticating a large number of entities, as the entities only need to know their own secret keys and set that secret key in KDC.
- Kerberos supports passwords or secret keys to be stored in a centralized credential store that is LDAP compliant. This makes it easy for the administrators to manage the system and the users.
- Servers don't have to store any tickets or any client-specific details to authenticate a client. The authentication request will have all required data to authenticate the client. The server only needs to know its own secret key to authenticate any client.
- The client authenticates with KDC and gets the TGT that is used for all subsequent authentications. This makes the overall authentication system faster, as there is no need for any lookup against the credential store after the first authentication is done.

### Hadoop Security Implementation in UIDAI

It is very complex and difficult to enforce security in UIDAI according to the current requirement. [20] The present and alarming security requirement proposed for the UIDAI System are:

#### User-Level access control:

- Users should only be allowed to access authorized data.
- Submission of jobs to the Hadoop cluster should be allowed to authenticated users only.
- User should have permissions to modify their jobs only.
- Only authenticated services should get register with Data Nodes or Task Tracker.

- Data block access within Data Node needs to be secured, and only authenticated users should be able to access the data stored in the Hadoop cluster.

#### Service Level Access Controls:

- Scalable Authentication: Hadoop clusters and the authentication models should be scalable to support such large network authentication.
- Impersonation: Hadoop services should be able to impersonate the user executing or accessing the jobs so that the correct user isolation can be maintained.
- Self-Served: Hadoop jobs run for long durations, so they should be able to ensure that the jobs are able to self-renew the delegated user authentication to complete the job.
- Secure IPC: Hadoop services should be able to authenticate each other and ensure secured communication between them. To achieve the preceding, Hadoop leverages the Kerberos authentication protocol and some internal-generated tokens to secure the Hadoop clusters.

#### User and Service authentication

Hadoop's remote procedure call using Simple authentication and Security Layer should be used for User authentication to Name Node and Job Tracker. Kerberos should be used as authentication protocol to authenticate the users within SASL.

All Hadoop services support Kerberos authentication. A client submits the Map Reduce job to the Job Tracker. Map Reduce jobs are usually long running jobs and they need to access the Hadoop resources on behalf of the user. This is achieved using Delegation Token, Job Token and the Block Access Token.

#### Delegation Token

It is a two party authentication protocol which is based on JAVA SASL and Digest – MD5. A delegation Token is used between the user and the Name Node to authenticate the user. Once the user authenticates them with Name Node using Kerberos, the user is provided with the delegation Token by Name Node. The user doesn't have to perform Kerberos Authentication once he/she obtains the delegation Token. The user also designates the Job Tracker or Resource Manager process as the user that will renew the Delegation Token as part of the Delegation Token Request.

The Delegation Token is secured and shared with Job Tracker or Resource Manager after authentication and Job Tracker will use the Delegation Token for accessing HDFS resource on behalf of the user. Job Tracker will automatically renew this Delegation Token for long running jobs.



### Job Token

A job runs on the Task Nodes and the user has to be secured in Task Nodes. When the user submits Map Reduce Jobs to Job Tracker, it will create a secret key that will be shared with the Task Tracker that will run the Map Reduce job. This secret key is the Job Token. The Job Token will be stored in the local disk of Task Tracker with permission only for the user who submitted the job. Task Tracker starts the child JVM task i.e. Mapper or Reducer using the user id that submitted the job. Thus, the child JVM will run securely with Task Tracker using this Job Token. The Job Token is used to ensure that an authenticated user submitting the job in Hadoop has access to only the folders and jobs for which he is authorized in the local file system of Task Nodes. Once the Reduce jobs are started in Task Tracker, this Task Tracker contacts Task Tracker that runs the Map Task and fetches the mapper output files. The Job Token is also used by Task Trackers to securely communicate with each other.

### Block Access Token

Block Access Token is the token provided by Name Node to a Hadoop Client.[19] BAT is used to ensure that only authorized user have access permission to access the data blocks stored in the Data Nodes. Hadoop Client when requests for data from HDFS, the client need to fetch the data blocks directly from the Data Node just after the client fetches the block id from Name Node. There should be a secured mechanism where the user privileges are securely passed to Data Node. When a client wants to access the data stored in the HDFS, it requests Name Node to provide the Block Ids for the files. Name Node verifies the requested users permission for the file and provides the list of block IDS and data Node Locations. The Client then contacts Data Node to fetch the required Data Block. To ensure that the authentication performed by Name Node is also enforced at Data Node, Hadoop implements the BAT.

The Block Access Token implements a symmetric key encryption where both name Node and Data Node shares a common secret key. Data Node receives this secret key once it registers with Name Node and is generated periodically. Each of these secret keys is identified by KeyID.

BAT is a lightweight and contains expiration Date, KeyID, ownerID, blockID and access modes. The access modes define permission available to the user for the requested block ID. The BAT generated by Name Node is not renewable and needs to be fetched again once the token expires. BAT has a lifetime of 10 hrs. This BAT ensures that the data blocks in Data Node are secured and only authorized users can access the data blocks.

The Proposed key steps in overall Hadoop Kerberos operations are:

- All Hadoop services authenticate themselves with KDC. Data Node registers with Name Node. Similarly, Task

Tracker registers itself with Job Tracker. Node Managers register themselves with Resource Manager.

- A Client authenticates with KDC. A Client requests service tickets for Name Node and Job Tracker/Resource Manager.
- For any HDFS file access, a client contacts the Name Node server and requests the file. Name Node authenticates the client and provides the authorization details to the client along with the Block Access Token (BAT). The BAT is a user required by Data
- Node to validate the authorization of the client and provides access to the corresponding blocks.

For a Map Reduce Job submission in the Hadoop cluster, the client request for a Delegation Token from Job Tracker. This Delegation Token is used for submitting a Map Reduce Job to the cluster. The Delegation Token is renewed by Job Tracker for long running jobs.

### V.CONCLUSION

In this paper looking at the various existing security features in UIDAI System and Authentication Process, drawbacks have been drawn out. On the basis of existing drawbacks, various security alternatives, privacy protection required in the system, Reviewed architecture is proposed with suggested implementation of Kerberos, a secured network authentication protocol that provides strong authentication for client/server applications without transferring the password over the network. In future I would like to work on different security algorithms required to be implemented on Network layer, Data layer and application layer.

### VI. ACKNOWLEDGMENT

This research was supported by various research work done by researchers. I thank all of them as their research work has provided the insight and expertise to me and their work has greatly assisted my research. I would like to thank and show my gratitude to Dr. Vinay Kumar, Prof. VIPS, New Delhi and Dr Meenu Dave, Professor, JaganNath University, Jaipur for sharing their pearls of wisdom with me during the course writing this research paper. I am immensely grateful to the reviewers for their comments on an earlier version of the manuscript, although any errors are my own and should not tarnish the reputations of these esteemed persons.

### REFERENCES

- [1] UIDAI. 2014. "AADHAAR TECHNOLOGY & ARCHITECTURE: Principles, Design, Best Practices, & Key Lessons", [https://uidai.gov.in/images/Aadhaar Technology Architecture March2014.pdf](https://uidai.gov.in/images/Aadhaar%20Technology%20Architecture%20March2014.pdf).
- [2] UIDAI. 2011. Aadhaar Security Policy & Framework for UIDAI Authentication (Version 1.0).[http://uidai.gov.in/images/authDoc/d3\\_4\\_security\\_policy\\_framework v1.pdf](http://uidai.gov.in/images/authDoc/d3_4_security_policy_framework_v1.pdf).
- [3] UIDAI. 2016a. "Authentication Overview", <https://uidai.gov.in/auth.html>.
- [4] UIDAI. 2016b. "Operating Model Overview", <https://uidai.gov.in/authentication2/operationmodel.html>.
- [5] Wikipedia. 2016a. "Aadhaar", <https://en.wikipedia.org/wiki/Aadhaar>.





- [6] Justice A P Shah, The Planning Commission: Government of India. 2011 (December), "Report of the Group of Experts on Privacy", <http://planningcommission.nic.in/reports/genrep/reprivacy.pdf>.
- [7] Wikipedia. 2016g. Kerberos (protocol). <https://en.wikipedia.org/wiki/Kerberos> (protocol).
- [8] Security and Privacy Challenges in the Unique Identification Number Project A Government of India initiative under UIDAI Position Paper - Prepared by DSCI 21-01-2010, [https://www.dsci.in/sites/default/files/security\\_and\\_privacy\\_challenges\\_in\\_the\\_uidai\\_project.pdf](https://www.dsci.in/sites/default/files/security_and_privacy_challenges_in_the_uidai_project.pdf)
- [9] PTI, 2015 "Right to privacy not a fundamental right, cannot be invoked to scrap Aadhaar", [http://articles.economicstimes.indiatimes.com/2015-07-23/news/64773078-1\\_fundamental-right-attorney-general-mukul-rohtagi-privacy](http://articles.economicstimes.indiatimes.com/2015-07-23/news/64773078-1_fundamental-right-attorney-general-mukul-rohtagi-privacy)
- [10] Rengamani H., Kumaraguru P., Chakraborty R., Rao H.R. (2010), "The Unique Identification Number Project: Challenges and Recommendations" [http://www4.comp.polyu.edu.hk/~iceb/content/slides/Haricharan\\_Rengamani-H\\_R\\_Rao\\_Unique\\_Identification\\_Number\\_Presentation.pdf](http://www4.comp.polyu.edu.hk/~iceb/content/slides/Haricharan_Rengamani-H_R_Rao_Unique_Identification_Number_Presentation.pdf)
- [11] Japreet Grewal, Vanya Rakesh, Sumandro Chattapadhyay, and Elonnai Hickok, 31st August, 2016, "Report on Understanding Aadhaar and its New Challenges", <https://cis-india.org/internet-governance/blog/report-on-understanding-aadhaar-and-its-new-challenges>
- [12] Shweta Agrawal Subhashis Banerjee Subodh Sharma, "Privacy and Security of Aadhaar: A Computer Science Perspective", <http://www.cse.iitdernet.in/~suban/reports/aadhaar.pdf>
- [13] Wikipedia. 2016d. Hardware security module. [https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module).
- [14] Wikipedia. 2016e. Hash-based message authentication code, [https://en.wikipedia.org/wiki/Hashbased\\_message\\_authentication\\_code](https://en.wikipedia.org/wiki/Hashbased_message_authentication_code).
- [15] Mehta, Pratap Bhanu. 2016. "Privacy after Aadhaar" <http://indianexpress.com/article/opinion/columns/privacy-after-aadhaar-money-bill-rajya-sabha-upa/>.
- [16] NDTV. 2016a. Truth vs Hype: Aadhaar's One Billion Challenge. <http://www.ndtv.com/video/news/truth-vs-hype/truth-vs-hype-aadhaar-s-one-billion-challenge-411279>.
- [17] Sudheesh Narayan, Dec 2013, Securing Hadoop: Implement robust end-to-end security for your Hadoop ecosystem.
- [18] Raj R. Parmar, Sudipta Roy, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, Tai-Hoon Kim. "Large-Scale Encryption in the Hadoop Environment: Challenges and Solutions", IEEE Access, 2017, <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7922533>
- [19] Derbeko, Philip, Shlomi Dolev, Ehud Gudes, and Shantanu Sharma, 2 May 2016, "Security and privacy aspects in MapReduce on clouds: A survey", computer Science Review, 2016, [https://www.academia.edu/25103224/Security\\_and\\_Privacy\\_Aspects\\_in\\_MapReduce\\_on\\_Clouds\\_A\\_Survey](https://www.academia.edu/25103224/Security_and_Privacy_Aspects_in_MapReduce_on_Clouds_A_Survey)
- [20] "Securing Hadoop" by Sudheesh narayanan, Shroff Publishers and Distributors Pvt.



## Data Science and Analytics

### 4th International Conference on Recent Developments in Science, Engineering and Technology, REDSET 2017, Gurgaon, India, October 13-14, 2017, Revised Selected Papers

- Editors
- ([view affiliations](#))

- Brajendra Panda
- Sudeep Sharma
- Nihar Ranjan Roy

Conference proceedings **REDSET 2017**

- [71 Citations](#)
- 88k Downloads

Part of the [Communications in Computer and Information Science](#) book series (CCIS, volume 799)

- [Papers](#)
- [About](#)

## Table of contents

Page of 4

[Next](#)

1. Front Matter  
Pages I-XIX  
[PDF](#)↓

### 2. Big Data Analytics

1. Front Matter  
Pages 1-1  
[PDF](#)↓
2. [System Behavior Analysis in the Urea Fertilizer Industry](#)  
Arun Kumar, Pardeep Goel, Deepika Garg, Atma Sahu  
Pages 3-16
3. [Performance Analysis of Machine Learning Techniques on Big Data Using Apache Spark](#)  
Garima Mogha, Khyati Ahlawat, Amit Prakash Singh  
Pages 17-26
4. [A Comparative Study of Consumption Behavior of Pharmaceutical Drugs](#)  
Keerti Jain, Priyanka Sharma, Medathati Jayalakshmi

- Pages 27-33
5. Trend Analysis of Machine Learning Research Using Topic Network Analysis  
Deepak Sharma, Bijendra Kumar, Satish Chand  
Pages 34-47
  6. Impact of Ontology on Databases  
Mohini Goyal, Geeta Rani  
Pages 48-60
  7. Design and Implementation of Virtual Hadoop Cluster on Private Cloud  
Garima Singh, Anil Kumar Singh  
Pages 61-71
  8. Healthcare Waste Management and Application Through Big Data Analytics  
Poorti Sahni, Ginni Arora, Ashwani Kumar Dubey  
Pages 72-79
  9. Detecting Internet Addiction Disorder Using Bayesian Networks  
Anju Singh, Sakshi Babbar  
Pages 80-95
  10. A Semantic Web-Based Framework for Information Retrieval in E-Learning Systems  
Olaperi Yeside Sowunmi, Sanjay Misra, Nicholas Omoregbe, Robertas Damasevicius, Rytis Maskeliūnas  
Pages 96-106
  11. A Database for Handwritten Yoruba Characters  
Samuel Ojumah, Sanjay Misra, Adewole Adewumi  
Pages 107-115
  12. Facial Expression Recognition for Motor Impaired Users  
Krishna Sehgal, Sanchit Goel, Rachna Jain  
Pages 116-125
  13. Document Oriented NoSQL Databases: An Empirical Study  
Omji Mishra, Pooja Lodhi, Shikha Mehta  
Pages 126-136

### 3. Data Centric Programming

1. Front Matter  
Pages 137-137  
[PDF↓](#)
2. A Survey of Techniques Used in Processing and Mining of Medical Images  
Sudhriti Sengupta, Neetu Mittal, Megha Modi  
Pages 139-155
3. Weighted Fuzzy KNN Optimized by Simulated Annealing for Classification of Large Data: A New Approach to Skin Detection  
Swati Aggarwal, Lehar Bhandari, Karan Kapoor, Jaswin Kaur  
Pages 156-163
4. Comparative Analysis of Edge Detection Techniques for Medical Images of Different Body Parts  
Bhawna Dhruv, Neetu Mittal, Megha Modi  
Pages 164-176
5. Classifier Dependent Dimensionality Reduction for Resource Restricted Environments  
Divyanshu Kalra, Chaitanya Dwivedi, Swati Aggarwal  
Pages 177-186
6. Improving Road Safety in India Using Data Mining Techniques  
Gaurav, Zunaid Alam  
Pages 187-194

## About these proceedings

### Introduction



# Comparative Analysis of Edge Detection Techniques for Medical Images of Different Body Parts

International Conference on Recent Developments in Science, Engineering and Technology

REDSET 2017: Data Science and Analytics pp 164-176 | Cite as

- Bhawna Dhruv (1) Email author (Bdhruv08@gmail.com)
- Neetu Mittal (1)
- Megha Modi (2)

1. Amity University, , Noida, India
2. Yashoda Super Specialty Hospital, , Ghaziabad, India

Conference paper

First Online: 08 March 2018

- [391 Downloads](#)

Part of the [Communications in Computer and Information Science](#) book series (CCIS, volume 799)

## Abstract

Medical images are arduous to process since they possess distinct modalities. Therefore, the medical practitioners cannot competently detect and diagnosis the diseases in conventional ways. There should be a system which helps physicians to understand medical images very easily. Image segmentation using edge detection is commonly used for image analysis and better visualization of medical images. Various methods have been used for image segmentation such as Threshold detection, Region detection, Edge detection and Clustering technique. Edge detection is one of the prominently used methods for segmentation. This technique focuses on identifying and analyzing the entire image based upon the detected edges. In this paper, MRI images of human body parts such as abdomen, ankle, elbow, hand, knee, leg, liver and brain are considered for edge detection. Further, filtering has been performed on the segmented images to remove the unwanted noise. This makes the image more clearly for further reference. The effectiveness of the proposed technique has been evaluated quantitatively by using the performance measures like Entropy and Standard Deviation. The proposed technique may be highly beneficial for medical practitioners to carry out the diagnosis for effective treatment.

## Keywords

Image segmentation Medical images MRI Edge detection Entropy  
Standard deviation Noise removal  
This is a preview of subscription content, [log in](#) to check access.

## References

1. Singh, H., Agrawal, D.: A meta analysis on content based image retrieval system. In: Proceedings of the IEEE International Conference on Emerging Technological Trends, pp. 1–6 (2016)  
[Google Scholar](#) ([https://scholar.google.com/scholar?q=Singh%2C%20H.%2C%20Agrawal%2C%20D.%3A%20A%20meta%20analysis%20on%20content%20based%20image%20retrieval%20system.%20In%3A%20Proceedings%20of%20the%20IEEE%20International%20Conference%20on%20Emerging%20Technological%20Trends%2C%20pp.%201%E2%80%936%20\(2016%29\)](https://scholar.google.com/scholar?q=Singh%2C%20H.%2C%20Agrawal%2C%20D.%3A%20A%20meta%20analysis%20on%20content%20based%20image%20retrieval%20system.%20In%3A%20Proceedings%20of%20the%20IEEE%20International%20Conference%20on%20Emerging%20Technological%20Trends%2C%20pp.%201%E2%80%936%20(2016%29)))
2. Khader, A., Ali, A., Alfaki, A.: Color and texture fusion-base method for content-based image retrieval. In: Proceedings of the IEEE International Conference on Computing for Sustainable Global Development, pp. 3205–3210 (2016)  
[Google Scholar](#) ([https://scholar.google.com/scholar?q=Khader%2C%20A.%2C%20Ali%2C%20A.%2C%20Alfaki%2C%20A.%3A%20Color%20and%20texture%20fusion-base%20method%20for%20content-based%20image%20retrieval.%20In%3A%20Proceedings%20of%20the%20IEEE%20International%20Conference%20on%20Computing%20for%20Sustainable%20Global%20Development%2C%20pp.%203205%E2%80%933210%20\(2016%29\)](https://scholar.google.com/scholar?q=Khader%2C%20A.%2C%20Ali%2C%20A.%2C%20Alfaki%2C%20A.%3A%20Color%20and%20texture%20fusion-base%20method%20for%20content-based%20image%20retrieval.%20In%3A%20Proceedings%20of%20the%20IEEE%20International%20Conference%20on%20Computing%20for%20Sustainable%20Global%20Development%2C%20pp.%203205%E2%80%933210%20(2016%29)))
3. Patel, J.M., Gamit, N.C.: A review on feature extraction techniques in content based image retrieval. In: IEEE International Conference on Wireless Communications, Signal Processing and Networking, pp. 2259–2263 (2016)  
[Google Scholar](#) ([https://scholar.google.com/scholar?q=Patel%2C%20J.M.%2C%20Gamit%2C%20N.C.%3A%20A%20review%20on%20feature%20extraction%20techniques%20in%20content%20based%20image%20retrieval.%20In%3A%20IEEE%20International%20Conference%20on%20Wireless%20Communications%2C%20Signal%20Processing%20and%20Networking%2C%20pp.%202259%E2%80%932263%20\(2016%29\)](https://scholar.google.com/scholar?q=Patel%2C%20J.M.%2C%20Gamit%2C%20N.C.%3A%20A%20review%20on%20feature%20extraction%20techniques%20in%20content%20based%20image%20retrieval.%20In%3A%20IEEE%20International%20Conference%20on%20Wireless%20Communications%2C%20Signal%20Processing%20and%20Networking%2C%20pp.%202259%E2%80%932263%20(2016%29)))
4. Manno, A.: Content based image retrieval using salient orientation histograms. In: IEEE International Conference on Image Processing, pp. 2480–2484 (2016)  
[Google Scholar](#) ([https://scholar.google.com/scholar?q=Manno%2C%20A.%3A%20Content%20based%20image%20retrieval%20using%20salient%20orientation%20histograms.%20In%3A%20IEEE%20International%20Conference%20on%20Image%20Processing%2C%20pp.%202480%E2%80%932484%20\(2016%29\)](https://scholar.google.com/scholar?q=Manno%2C%20A.%3A%20Content%20based%20image%20retrieval%20using%20salient%20orientation%20histograms.%20In%3A%20IEEE%20International%20Conference%20on%20Image%20Processing%2C%20pp.%202480%E2%80%932484%20(2016%29)))
5. Zaitouna, N.M., Aqelb, M.J.: Survey on image segmentation techniques. *Procedia Comput. Sci.* **65**, 797–806 (2015). International Conference on Communication,



# Comparative Analysis of Edge Detection Techniques for Medical Images of Different Body Parts

Bhawna Dhruv<sup>1</sup>(✉), Neetu Mittal<sup>1</sup>, and Megha Modi<sup>2</sup>

<sup>1</sup> Amity University, Noida, UP, India

Bdhruv08@gmail.com, Savini09@gmail.com

<sup>2</sup> Yashoda Super Specialty Hospital, Ghaziabad, UP, India

Dr.meghamodi@gmail.com

**Abstract.** Medical images are arduous to process since they possess distinct modalities. Therefore, the medical practitioners cannot competently detect and diagnosis the diseases in conventional ways. There should be a system which helps physicians to understand medical images very easily. Image segmentation using edge detection is commonly used for image analysis and better visualization of medical images. Various methods have been used for image segmentation such as Threshold detection, Region detection, Edge detection and Clustering technique. Edge detection is one of the prominently used methods for segmentation. This technique focuses on identifying and analyzing the entire image based upon the detected edges. In this paper, MRI images of human body parts such as abdomen, ankle, elbow, hand, knee, leg, liver and brain are considered for edge detection. Further, filtering has been performed on the segmented images to remove the unwanted noise. This makes the image more clearly for further reference. The effectiveness of the proposed technique has been evaluated quantitatively by using the performance measures like Entropy and Standard Deviation. The proposed technique may be highly beneficial for medical practitioners to carry out the diagnosis for effective treatment.

**Keywords:** Image segmentation · Medical images · MRI · Edge detection  
Entropy · Standard deviation · Noise removal

## 1 Introduction

With the modern approach in the field of information technology, the revision in the analysis of the medical images has devoted noticeably to the early diagnosis of various diseases. Image segmentation especially edge detection technique give much knowledge that help to explain the medical images and improve the sharpness of detection and further diagnosis of different diseases. Image Segmentation is the process of dividing an image into meaningful structures where each pixel has same attributes [1]. The pixel is similar on the basis of criteria such as texture, color or intensity. Image segmentation aims at improving the pictorial information for interpretation. This process can be achieved by converting a low level image into high level image which may deem to be a challenging task as an image is never partitioned accurately for analysis [2]. One of the

91

processes of achieving the same is through Edge detection techniques. The reason behind implementing an edge detector to a set of images is highly suggestive of reduction in amount of data to be processed. This further overlooks insignificant data and captures important properties of an image. Various types of edge detection operators such as Sobel, Roberts, Prewitt, Canny and LoG can be applied to study the results on a particular image [3]. The aim of the paper is to study these edge detection techniques and apply them on the MRI images of different body parts to analyze the results. Image Segmentation plays a vital role in medical image processing, particularly for different body parts abnormalities detection in Magnetic Resonance Imaging (MRI) and computed Tomography (CT). The idea behind using MRI to CT is that the latter doesn't use ionizing radiations, hence giving us a clear picture of the health condition [4]. The results are based upon three parameters i.e. Entropy, Standard Deviation and Execution Time. Entropy, generally defines the amount of information which must be used to compress the image by any compression algorithm [5]. Similarly, the standard deviation explains the variation of the results from the actual value of any parameter in an image.

Moreover, images seized from different sources suffer deterioration which affects the essential features of the image and makes image study difficult. Image restoration attempts to restore the degraded images by removing noise from the image. The process of image restoration completely depends upon the accuracy of image analysis and generally removes unwanted parts [6]. It studies the entire degradation process and evaluates the inverse process to assess the original image. It is an objective process and restores the approximation of the actual image.

In this paper, edge detection techniques are applied with different operators on MRI images.

#### A. Magnetic Resonance Imaging:

Magnetic Resonance Imaging (MRI) is a medical imaging technique used to visualize detailed internal structures of respective body parts with the help of magnetic radiation. It provides three-dimensional real-time views of organs, mostly for the soft-tissue. It furnishes good contrast of soft tissue, gives better visualization of soft-tissue structures like brain, spine, muscles, and joints. The MRI machine used to capture in multiple body planes without changing the physical positions of the patient under scanning as it operates in multiple planes. Image segmentation may be widely used in MRI images of brain to detect tumor and other skin lesions or patches like abnormalities. Also, image segmentation on MRI images is also useful after surgery to keep track of the improvement of treatment and to monitor the growth of tumor before surgery.

## 2 Edge Detection Technique

Edge detection has turned out to be the most competent field in image processing which helps in locating sharp discontinuities in an image. These discontinuities are abrupt changes in the intensity of pixels which define the edges of an image [7]. The edge element is a crucial and significant feature of an image. There are several edge detection techniques depending upon the sensitivity of an image which are designed to work

upon in vertical, horizontal and diagonal directions [8]. It must be noted that the preferred direction of every convolution mask is weighted with highest coefficients. Apart from edge detection, noise removal also plays an important role in image processing. The goal of removing noise is to discard unwanted pixels.

Different edge detection operators:

#### A. SOBEL:

The Sobel operator is used to perform spatial gradient measurement on any image. It is used for edge detection of two basic types i.e. Vertical Direction and Horizontal Direction [9]. This operator consists of  $3 \times 3$  convolution mask which is designed in such a way that every edge whether in vertical or horizontal direction is detected relative to the pixel grid [10]. The convolution mask of the image is generally smaller as compared to the actual image. These masks can be applied in any form i.e. Corresponding to  $G_x$  or  $G_y$  separately or together so as to give an absolute gradient measurement at each point. The intensity of the function at eight distinct points is recognized to sample image point. The  $G_x$  mask highlights the horizontal edges in the image while  $G_y$  highlights the vertical edges, it further calculate the difference between pixel intensities of the particular direction [11]. As it is visible from the mask, the zeros in the middle row helps to compute the difference between the intensities of the edge [12]. This operator is disrupted by noise easily, therefore cannot detect outermost images easily. The basic advantage of using this operator is that weights can be applied to the coefficients which produce better result.

$$|G| = \sqrt{G_x^2 + G_y^2}$$

$$G_x = \sum \sum Sobel_{x,ij} * I_{r+i-2,c+j-2}$$

$$G_y = \sum \sum Sobel_{y,ij} * I_{r+i-2,c+j-2}$$

#### B. ROBERTS:

The Roberts operator is used to highlight the high spatial frequency of the corresponding edges of any image. The kernels used for this operator are rotated by  $90^\circ$  therefore the convolution mask is designed to give the maximum results of the edges running at  $45^\circ$ . Similar to Sobel Operator, the edges can be detected separately or absolute gradient can be computed by combining  $G_x$  and  $G_y$  [13]. The convolution masks are given below:

$$|G| = \sqrt{G_x^2 + G_y^2}$$

Robert also proposed the following equation:

$$y_{ij} = \sqrt{x_{i,j}}$$

$$z_{ij} = \sqrt{(y_{i,j} - y_{i+1,j+1})^2 + (y_{i+1,j} - y_{i,j+1})^2}$$



- x: Initial density of the image.  
 z: Computed derivate.  
 i, j: Location of image.

### C. PREWITT:

This technique was devised to conquer the problems of Sobel operator i.e. absence of smoothing modules. It detects the edges in both vertical and horizontal direction which is a way of finding the approximations in magnitude and orientation of the edge in an image [14]. It has maximum 8 possibilities of orientation and does not emphasize on central value of the mask. The kernels of this operator are of least values thereby preventing blurring and extra trouble. The convolution mask is given below:

$$|G| = \sqrt{G_x^2 + G_y^2}$$

$$\text{Also, } \theta = \text{atan2}(G_y, G_x)$$

### D. CANNY:

This edge detection technique is also known as optimal edge detector as it focuses on improving the results as compared to the other operators [15]. This initially smoothes the image and removes the noise and then gives the output of spatial gradient measurement on any image. This filter helps to smoothen the noise as well detects the edges meticulously. It works to satisfy the conditions like localization of edge, low error rate and single edge detection. The gradient is calculated using the Gaussian filter [16]. The edge identification image is then exhibited to thresholds followed by the process of hysteresis to suppress the non suppressed pixels.

### E. LoG:

The laplacian of Gaussian is 2D isotropic measure of 2nd special derivative of the image which focuses on highlighting the region where the intensity of the image changes very rapidly [17]. Therefore this is a highly used edge detection technique. The operation of this detector works in a way that it first smoothes the noise using the Gaussian filter and then gives the output as a gray image only [18]. The laplacian of an image is as given below:

$$L(x, y) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2}$$

As it can be seen that all the three filters deal with second derivate measurement of the image, it becomes necessary to first smoothen the image so as to reduce the noise and then the Gaussian filter is applied [19, 20].

### 3 Measuring Parameters of Image Analysis

The quality of any image can be determined on two basis i.e. subjective or objective. The subjective as the name suggests consumes more time as compared to the latter. In our work, we have considered two quantity measures as given:

#### A. Standard Deviation:

The standard deviation is the measure of distribution of the set of data from its mean. It measures the absolute instability of a distribution [21, 22]. Higher instability depicts higher standard deviation. Generally, continuous data is required to calculate standard deviation. It is given by:

$$\sigma = \sqrt{\sum_{i=0}^L (i - \bar{i})^2 h_{lf}(i)}, \dots \bar{i} = \sum_{i=0}^L i h_{lf}$$

#### B. Entropy:

Entropy as defined by the Math works is a statistical measure of randomness that can be used to characterize the texture of input image [23]. Images with low entropy have low contrast whereas high entropy depicts high contrast in an image but are troublesome to compress. It is given by:

$$E = - \sum_{i=0}^{L-1} p_i \log_2 p_i$$

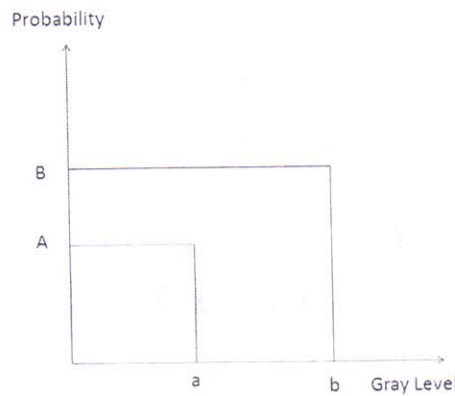
In our work, we have dealt with the MRI images of different body parts. MRI (Magnetic Resonance Imaging) is a medical imaging technique used in radiology to form pictures of the anatomy and the physiological processes of the body in both health and disease. On the images of different body parts, several operators have been applied to study the result.

### 4 Noise Removal

Digital images play fundamental role in the field of research, medical imaging and information systems using satellites. The images collected from distinct sources are noisy hence de-noising techniques are applied so as to achieve better results for analysis. De-noising still prevails as a challenge in the research therefore techniques like image enhancement are used to improve the image quality. The filtering techniques are treated as first step to obtain images rich in quality.

*A. Salt and Pepper:*

The pixels in the image get destroyed due to transformation from analog to digital domain. These corrupted images are known as impulse noise which are of two types i.e. fixed value impulse noise and Random value impulse noise. The fixed impulse noise is also referred to as Salt and Pepper which accepts only 2 values, either 0 for pepper or 255 for salt. The random value impulse noise whereas can accept any value ranging from 0 to 255. This noise generally occurs in an image due to defects in camera's sensor cell or synchronization errors (Fig. 1).



**Fig. 1.** Probability density functions of salt and pepper noise

*B. Wiener:*

When an image is blurred using a low pass filter, the original image can be obtained by using the process of inverse filtering, however this process invites additive noise to the image. The wiener filter optimizes inverse filtering and noise smoothing. It not only discards the noise but also performs inverse filtering. Wiener filtering in Fourier domain can be expressed as:

$$W(f_1, f_2) = \frac{H^*(f_1, f_2) S_{xx}(f_1, f_2)}{(|H(f_1, f_2)|)^2 S_{xx}(f_1, f_2) + S_{nn}(f_1, f_2)}$$

While performing image restoration using wiener filter, a low pass filter as shown below is used to blur the image.

$$H = 1/16 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

The implementation of this filter requires the calculation of power spectra of both original image as well as additive noise. Power spectrum can be calculated using:

$$S_{yy}^{per} = \frac{1}{N^2} [Y(k, l)Y(k, l)^*]$$

Where,  $Y(k, l)$  is DFT of observation.

The technique of wiener filter is not highly used but produces best mathematical results.

### C. Poisson Noise:

It is an ambiguous association with the measurement of light and independence of photon detection. This noise contributes in varying proportion in an image. This generally occurs when the number of photons is not able to provide exact statistical information. It is also known as photon noise and is signal dependent whose magnitude increases with respect to intensity of light.

## 5 Simulation and Results

MRI images of different body parts such as abdomen, ankle, elbow, hand, leg, liver and brain have been taken for analysis. Edge detection operators such as Roberts, Sobel, Prewitt, Canny and LoG have been applied to each image. Further Entropy, Standard Deviation and Execution time is evaluated from the resultant images. Table 1 depicts the results obtained from the same highlighting prominent changes in the values of parameters especially in case of Laplace of Gaussian operator.

From the results shown in Table 1, it is clearly indicated that there are noticeable changes in the values of Entropy, Standard Deviation and Time for LoG operator.

For abdomen, entropy of original image is 4.0522. Different filters have been applied for analysis such as Robert, Sobel, Prewitt, Canny, LoG. Entropy of resultant images after applying filters are different from original image such as 4.0522, 0.1539, 4.0522, 4.0522, 4.0522, and 4.0757 are the entropy of different operators respectively.

For ankle, entropy of original image is 7.0966. Entropy of resultant images after applying filters are different from original image such as, 0.1887, 7.0966, 7.0966, 7.0966, 7.0966 and 6.9408 are the entropy of different operators respectively.































For elbow, entropy of original image is 6.2733. Entropy of resultant images after applying filters are different from original image such as, 0.1741, 6.2733, 6.2733, 6.2733 and 6.0439 are the entropy of different operators respectively.

For hand, entropy of original image is 4.9325. Entropy of resultant images after applying filters are different from original image such as 0.1642, 4.9325, 4.9325, 4.9325 and 4.5715 are the entropy of different operators respectively.

For knee, entropy of original image is 4.1647. Entropy of resultant images after applying filters are different from original image such as, 0.1490, 4.1647, 4.1647, 4.1647 and 4.5715 are the entropy of different operators respectively.



















For leg, entropy of original image is 5.2013. Entropy of resultant images after applying filters are different from original image such as, 0.1446, 5.2013, 5.2013, 5.2013 and 5.3754 are the entropy of different operators respectively.

**Table 1.** Analysis of different operators on MRI of different body parts

Image	Original Image	Roberts	Sobel	Prewitt	Canny	LoG
Abdomen						
Entropy	4.0522	0.1539	4.0522	4.0522	4.0522	4.0757
Standard Deviation	44.0048	0.1475	44.0049	44.0049	44.0049	43.4800
Execution Time (In Sec)	0.116400	1.849964	0.950286	1.977930	2.329548	0.292388
Ankle						
Entropy	7.0966	0.1887	7.0966	7.0966	7.0966	6.9408
Standard Deviation	64.1354	0.1674	64.1356	64.1356	64.1356	62.0044
Execution Time (In Sec)	0.025406	0.364964	0.166824	0.294917	0.320282	0.056844
Elbow						
Entropy	6.2733	0.1741	6.2733	6.2733	6.2733	6.0439
Standard Deviation	52.2844	0.1593	52.2846	52.2846	52.2846	49.7832
Execution Time (In Sec)	0.027801	0.291431	0.195056	0.571107	0.373559	0.067847
Hand						
Entropy	4.9325	0.1642	4.9325	4.9325	4.9325	4.5715
Standard Deviation	56.3903	0.1536	56.3903	56.3903	56.3903	54.3642
Execution Time (In Sec)	0.053466	0.866227	0.426349	0.789168	0.898489	0.145112
Knee						

(continued)

Table 2. (continued)



















Entropy	4.1647	0.1490	4.1647	4.1647	4.1647	4.1790
Standard Deviation	68.6057	0.1446	68.6057	68.6057	68.6057	68.1572
Execution Time (In Sec)	0.148529	2.613820	1.324256	2.792228	2.453288	0.388934
Leg						
Entropy	5.2013	0.1446	5.2013	5.2013	5.2013	5.3754
Standard Deviation	48.0656	0.1419	48.0659	48.0659	48.0659	46.5672
Execution Time (In Sec)	0.055868	1.365116	0.520580	0.919118	1.057049	0.156223
Liver						
Entropy	5.8791	0.1870	5.8791	5.8791	5.8791	5.9122
Standard Deviation	52.0688	0.1665	52.0688	52.0688	52.0688	50.2168
Execution Time (In Sec)	0.055593	1.286821	0.472204	0.866820	1.024173	0.151872
Brain						
Entropy	5.0652	0.2291	5.0652	5.0652	5.0652	5.1647
Standard Deviation	39.4291	0.1891	39.4293	39.4293	39.4293	34.3848
Execution Time (In Sec)	0.019450	0.209662	0.137743	0.207306	0.186673	0.048438

different operators such as Robert, Sobel, Prewitt, Canny, LoG applied on resultant image from Table 1.

From the results shown in Table 2, it is clearly indicated that there are noticeable changes in the values of Entropy, Standard Deviation and Time for LoG operator.

For abdomen, Entropy of the original image is 4.0522 and 4.0757 for LoG operator. For ankle, the entropy of original image is 7.0966 and 6.9408 for LoG operator. For elbow, the entropy of original image is 6.2733 and 6.0439 for LoG operator. For hand, the entropy of original image is 4.9325 and 4.571 for LoG operator. For knee, the entropy of original image is 4.1647 and 4.1790 for LoG operator. For leg, the entropy

Table 1. (continued)































Image	Original Image	Roberts	Sobel	Prewitt	Canny	LoG
Entropy	4.1647	0.1490	4.1647	4.1647	4.1647	4.1790
Standard Deviation	68.6057	0.1446	68.6057	68.6057	68.6057	68.1572
Execution Time (In Sec)	0.148529	2.613820	1.324256	2.792228	2.453288	0.388934
Leg						
Entropy	5.2013	0.1446	5.2013	5.2013	5.2013	5.3754
Standard Deviation	48.0656	0.1419	48.0659	48.0659	48.0659	46.5672
Execution Time (In Sec)	0.055868	1.365116	0.520580	0.919118	1.057049	0.156223
Liver						
Entropy	5.8791	0.1870	5.8791	5.8791	5.8791	5.9122
Standard Deviation	52.0688	0.1665	52.0688	52.0688	52.0688	50.2168
Execution Time (In Sec)	0.055593	1.286821	0.472204	0.866820	1.024173	0.151872
Brain						
Entropy	5.0652	0.2291	5.0652	5.0652	5.0652	5.1647
Standard Deviation	39.4291	0.1891	39.4293	39.4293	39.4293	34.3848
Execution Time (In Sec)	0.019450	0.209662	0.137743	0.207306	0.186673	0.048438

For liver, entropy of original image is 5.8791. Entropy of resultant images after applying filters are different from original image such as, 0.1870, 5.8791, 5.8791, 5.8791 and 5.9122 are the entropy of different operators respectively.

For brain, entropy of original image is 5.0652. Entropy of resultant images after applying filters are different from original image such as, 0.2291, 5.0652, 5.0652, 5.0652 and 5.1647 are the entropy of different operators respectively.

Further noise removal techniques have been applied to perform image restoration on the above resulting images to perceive and conclude the development of best operator and better image quality. Table 2 explains the noise removal techniques with

**Table 2.** Noise removal techniques with different operators on resultant images of Table 1

Image	Original Image	Robert	Sobel	Prewitt	Canny	LoG
Abdomen						
Entropy	4.0522	0.1539	4.0522	4.0522	4.0522	4.0757
Standard Deviation	44.0048	0.1475	44.0049	44.0049	44.0049	43.4800
Execution Time (In Sec)	0.116400	1.849964	0.950286	1.977930	2.329548	0.292388
Ankle						
Entropy	7.0966	0.1887	7.0966	7.0966	7.0966	6.9408
Standard Deviation	64.1354	0.1674	64.1356	64.1356	64.1356	62.0044
Execution Time (In Sec)	0.025406	0.364964	0.166824	0.294917	0.320282	0.056844
Elbow						
Entropy	6.2733	0.1741	6.2733	6.2733	6.2733	6.0439
Standard Deviation	52.2844	0.1593	52.2846	52.2846	52.2846	49.7832
Execution Time (In Sec)	0.027801	0.291431	0.195056	0.571107	0.373559	0.067847
Hand						
Entropy	4.9325	0.1642	4.9325	4.9325	4.9325	4.5715
Standard Deviation	56.3903	0.1536	56.3903	56.3903	56.3903	54.3642
Execution Time (In Sec)	0.053466	0.866227	0.426349	0.789168	0.898489	0.145112
Knee						

(continued)





of original image is 5.2013 and 5.3754 for LoG operator. For liver, the entropy of original image is 5.8791 and 5.9122 for LoG operator. For brain, the entropy of original image is 5.0652 and 5.1647 for LoG operator.

## 6 Conclusion

Although edge detection is an initial step in reviewing an image but it becomes crucial to understand different types of edge detection techniques. On the basis of the analysis of different MRI images, it is clear that LoG proves to provide better results as compared to Roberts, Sobel, Prewitt and Canny. The operators can be localized as per the requirement of a user to conform to an environment. Similarly the noise removal techniques also are essential to produce a relevant analysis and study of the images, in support of this, the results of the same give us a clear picture that wiener filter continues to give better results, although there are minute variations but they play very important role in detection algorithms and noise removal techniques.

## References

1. Singh, H., Agrawal, D.: A meta analysis on content based image retrieval system. In: Proceedings of the IEEE International Conference on Emerging Technological Trends, pp. 1–6 (2016)
2. Khader, A., Ali, A., Alfaki, A.: Color and texture fusion-base method for content-based image retrieval. In: Proceedings of the IEEE International Conference on Computing for Sustainable Global Development, pp. 3205–3210 (2016)
3. Patel, J.M., Gamit, N.C.: A review on feature extraction techniques in content based image retrieval. In: IEEE International Conference on Wireless Communications, Signal Processing and Networking, pp. 2259–2263 (2016)
4. Manno, A.: Content based image retrieval using salient orientation histograms. In: IEEE International Conference on Image Processing, pp. 2480–2484 (2016)
5. Zaitouna, N.M., Aqelb, M.J.: Survey on image segmentation techniques. *Procedia Comput. Sci.* **65**, 797–806 (2015). International Conference on Communication, Management and Information Technology
6. Kabai, L., Abdellaoui, M.: Content based image retrieval using local and global feature extractor. In: IEEE International Conference on Advanced Technologies for Signal and Image Processing, pp. 151–154 (2016)
7. Mageswari, S.U., Sridevi, M., Mala, C.: An experimental study and analysis of different image segmentation techniques. *Procedia Eng.* **64**, 36–45 (2013). International Conference on Design and Manufacturing
8. Abdulrazzaq, M.M., Noah, S.A., Fadhil, M.A.: X-Ray medical image classification based on multi classifiers. In: IEEE International Conference on Advanced Computer Science Applications and Technologies, pp. 218–223 (2015)
9. Zheng, K.: Content based image retrieval for medical image. In: Proceedings of the IEEE International Conference on Computational Intelligence and Security, pp. 219–222 (2015)
10. Lijuan, S., Fengqi, H.: Research on color and texture feature based image retrieval. In: IEEE International Conference on Intelligent, Transportation, Big Data and Smart City, pp. 626–628 (2015)



11. Kumar, T.G.S., Nagarajan, V.: Local smoothness pattern for content based image retrieval. In: IEEE International Conference on Communications and Signal Processing, pp. 1190–1193 (2015)
12. Jyothi, B., Madhavee Latha, Y., Mohan, P.G.K.: An effective multiple visual features of content based medical image retrieval. In: Proceedings of the 9th IEEE International Conference on Intelligent Systems and Control, pp. 1–5 (2015)
13. Rocha, R., Saito, P.T.M., Bugatti, P.H.: Exploiting revolutionary approaches for content based image retrieval. In: International Symposium on Computer Based Medical System, pp. 370–372 (2015)
14. Gupta, N.M.R.: Comparative analysis of medical images fusion using different fusion methods for Daubechies complex wavelet transform. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* 3(6) (2013)
15. Gupta, A., Gangadharppa, M.: Image retrieval based on color, shape and texture. In: 2nd IEEE International Conference on Computing for Sustainable Global Development, pp. 2097–2103 (2015)
16. Bhagyalakshmi, A., Vijayachamundeeswari, V.: A survey on image retrieval using various operators In: IEEE International Conference on Computer Communication and Systems, pp. 18–23 (2014)
17. Wang, Y., Li, Q., Lan, T., Chen, J.: A comparison of image based image retrieval system. In: 17th IEEE International Conference on Computational Science and Engineering, pp. 669–673 (2014)
18. Jenni, K., Mandala, S.: Pre-processing image database for efficient content based image retrieval. In: IEEE International Conference on Advances in Computing, Communications and Informatics, pp. 968–972 (2014)
19. Shriwas, M.K., Raut, V.R.: Content based image retrieval: a past, present and new feature descriptor. In: IEEE International Conference on Circuit, Power and Computing Technologies, pp. 1–7 (2015)
20. Mendoza, O., Melin, P., Licea, G.: A new method for edge detection in image processing using interval type-2 fuzzy logic. In: IEEE International Conference on Granular Computing, pp. 151–155 (2007)
21. Anandakrishnan, N., Santhosh Baboo, S.: An evaluation of popular edge detection techniques in digital image processing. In: IEEE International Conference on Intelligent Computing Applications, pp. 213–217 (2014)
22. Selvakar, P., Hariganesh, S.: The performance analysis of edge detection algorithms for image processing. In: IEEE International Conference on Computing Technologies and Intelligent Data Engineering, pp. 1–5 (2016)
23. Vijaya, A., Sunderesan, M.: Significant image enhancement techniques for removal of noise in LiDar images. In: 3rd International IEEE Conference on Computing for Sustainable Global Development, pp. 3904–3908 (2016)