Editor's Note

IJRACSE : International Journal of Research in Advanced Computer Science Engineering is an international peer reviewed, open access, online journal published by Yuva Engineers for professionals and researchers in various disciplines of Engineering and Technology.IJRACSE is an is a science and Technology enrichment initiative designed for professionals & Researchers across the world. IJRACSE's goal is to inspire young engineers and professionals to develop an interest in research and development, in doing so, recognise the importance and excitement of engineering, technology & management for the upliftment of entire Mankind.

IJRACSE solicits innovative research papers on the Engineering and Technological issues of the modern day world. The initiative brings together academic, industry, and students to a single-path, highly selective forum on the design, implementation, and applications of engineering.IJRACSE takes a broad view of Engineering to include any ideas that collectively addresses a challenge. We invite submissions covering a broad range of Engineering streams including conventional Computer Science Engineering, Programming, Algorithms, Circuits, Networking, Control Systems, Information Technology, Artificial Intelligence, Microprocessor, Microcontrollers, Computer Graphics & Multimedia.

You can be an Electronics engineering Professional/Researcher but you have an idea in computer science engineering, you are most welcomed to submit your idea. We are not restricting authors on the stream they belong to. Any one can submit paper on any topic he/she wish to. Authors can submit more than one paper, but has to submit separately. Multiple Authors can submit one paper as well.Policy Of the Journal: Submitted papers should be original and must have not been published nor submitted for review/publication to any other editorial. Please do not copy from Internet and submit them. We don't encourage any kind of plagiarism. Try to put articles in your own words. Give credits and references to original authors and researchers where ever necessary.

Aim of the Journal:

The Journal Aims is to promote research and development of Engineering, Science, Technology and Management. The journal is working with the aim to provide a platform and publish original research work, review work, ideas and Designs.

Scope of the Journal:

We seek technical papers describing ideas, groundbreaking results and/or quantified system experiences. We especially encourage submissions that highlight real-world problems and solutions for it. Topics of interest include, but are not limited to, the following: Computer Science Engineering,

Parallel Processing and Distributed Computing, Foundations of High-performance Computing, Graph Theory and Analysis of Algorithms, Artificial Intelligences and Pattern/Image Recognitions, Neural Networks and Biomedical Simulations, Virtual Visions and Virtual Simulations, Data Mining, Web Image Mining and Applications, Data Base Management & Information Retrievals Adaptive Systems, Bifurcation, Biocybernetics & Bioinformatics, Blind Systems, Neural Networks &Control Systems, Cryptosystems &Data Compression, Evolutional Computation &Fuzzy Systems, Image Processing and Image Recognition, Modeling & Optimization, Speech Processing, Speech Synthesis & Speech Recognition, Video Signal Processing, Watermarking & Wavelet Transform, Computer networks & security, GIS, remote sensing & surveying and All topics related Computer Science.

The Features and Benefits of IJRACSE:

1. Fast and Easy procedure for publication of papers.
2. We follow Proper Peer review process and Editorial and Professional Ethics.
3. Each article/Paper will be published In the PDF version of Online Journal of IJRACSE. This paper may also be published in other associated Journals.
4. Permanent and Direct Link of your paper IJRACSE, So that you can share the link on your Linked, Facebook, Twitter etc pages to showoff to the world.
5. IJRACSE Provides Individual "Hardcopy of Certificate of Publication" to each author of the published paper.
6. IJRACSE is indexed in all major Indexing sites and databases.
7. Open access and free for anyone to view and download without registering.
8. The Most popular and widely read "Yuva Engineers" Monthly Print Magazine is our parent Publication. The Yuva Engineers Print Version is having a dedicated reader base of over 1 Lakh Readers. Selected Papers of the IJRACSE will be published in the print version aswell.

K.V.A.Sridhar
Editor & Publisher

INTERNATIONAL JOURNAL OF RESEARCH IN ADVANCED COMPUTER SCIENCE ENGINEERING

Address : 11-4-650,204 Sovereign Shelters,
Redhills,Lakdikapul,
Hyderabad-500004.

Telephone : 040-66714050
Mobile +91 9866110776
Email Yuvaengineers@gmail.com
www.ijracse.com

Periodicity : Monthly

Language : English

Publisher,Editor & Owner K.V.A.Sridhar

Printed at Ratnaraj Printers
11-5-431/1, Redhills, Lakdikapul,
Hyderabad - 500004.

EDITORIAL & REVIEW BOARD

Inside

Call For Papers: IJRACSE solicits innovative research papers on Engineering Technological, and Management issues of CSE. The initiative brings together academic, industry, and students to a single-path, highly selective forum on the design, implementation, and applications of engineering & management.

Ten Step Process for Submission:

Step 1..Covering Letter to be Attached as Below:

Dear Sir/Madam,

Please find my submission of Technical paper entitled '_____' with reference to your Call for Papers.

I hereby affirm that the contents of this Technical Paper are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the authors have seen and agreed to the submitted version of the Technical Paper and their inclusion of names as co-authors.

Also, if my/our Technical paper is accepted, I/We agree to comply with the terms and conditions as given on the website of the journal & you are free to publish our contribution in any of your journals/Magazines and website.

Name of the Author: Signature: Designation: College/Organisation: Full address & Pin Code:

Mobile Number (s): Landline Number (s): E-mail Address: Alternate E-mail Address:

Step 2… The Technical Paper should be submitted in Hard copy and aswell as Soft copy. Soft copy should be in CD/DVD. Your soft copy will be published on website giving credits to you.

Step 3…AUTHOR NAME (S) & AFFILIATIONS: The author (s) full name, designation, affiliation (s),College/Institution, Year & Department, Guide Name and Designation(If Any), address, mobile / landline numbers, and email / alternate email address should be in italic & 12-point in Georgia Font. It must centered underneath the title.

Step 4..ACKNOWLEDGMENTS: Acknowledgments can be given to reviewers, funding institutions, etc., if any.

Step 5..ABSTRACT: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

Step 6… FORMAT: Manuscript must be in BRITISH ENGLISH prepared on a standard A4 size PORTRAIT SETTING PAPER. It must be prepared on a single space and single column with 1 margin set for top, bottom, left and right. It should be typed in 12 point Georgia Font with page numbers at the bottom and centre of every page.

All Headings and Sub-Headings must be bold-faced, aligned left and fully capitalized and typed in 12 Point Gerogia Font.

Figures and Table: Please do not copy figures and tables from net. Draw them on your own. Sources of data should be mentioned below the table/figure. It should be ensured that the tables/figures are referred to from the main text.

Step 7...REFERENCES: The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow Harvard Style of Referencing.

Step 8...HOSTING & CERTIFICATION FEE: Send your hard copy+Soft copy along with 1500 rupees DD favoring "Yuva Engineers" Payable at "Hyderabad"

Step 9….ADDRESS TO BE POSTED: Send your entries to "Yuva Engineers, D.NO: 11-4-650, 204 Sovereign Sheleters, Redhills, Lakdikapul, Hyderabad – 500004

Step 10… Details Sheet: Please Attach a separate sheet with your details: Name, Address, email, Telephone number, Branch of Engineering, Semester studying, College name and Address. (If more than one student is submitting the paper, Attach separate sheet with details)

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Unique Method of Mesuring Human Intelligence Based on Possible Metrics and Relative Method

N S R Phanindra Kumar
Assistant professor,
Department of CSE,
AITAM, Tekkali.

Ramesh Bandaru
Assistant professor,
Department of CSE,
AITAM, Tekkali.

ABSTRACT:

The study of human intelligence is possibly the most controversial area in psychology and also identically psychometric assessment of intelligence is a blooming and a dominant aspect of applied psychology. This report consolidates the following issues related to human intelligence:

- The requisites to measure human intelligence.
- Definition for ,,Human intelligence.
- Extensity of ,,Human Intelligence.
- Possible metrics and Relative methods to measure human intelligence.
- Discourse on scale type, meaningfulness, weakness in conjunction with strengths for the possible metrics and finally the reflections.

KEYWORDS:

HUMINT- Human Intelligence
NATO-North Atlantic Treaty Organization
SBIS- Stanford-Binet Intelligence Scale
WISC- David Wechsler Intelligence Scale
CTONI- Comprehensive Test of Non Verbal Intelligence
IQ-Intelligence Quotient

1. INTRODUCTION:

The word ,,intelligence was actually originated from the Latin verb intelligere [1], which means understanding which is capable of adjusting to the environment. There exist different species of creatures in the universe; and it is a well-known fact that the,,social animal is the axial part of the existing universe.

Animals merely feed to survive and reproduce, whereas humans on the other hand are known for their curiosity to understand and are more influential in changing their environment. Human Intelligence can be calibrated by the use of intuitive measures, since intelligence varies from one person to the other which ismore dependent on the environment [2]. The major criteria which separate us from the animals are [3]:

- The potential to reason, converse and make deductive decisions in an environment of imprecision, uncertainty, scarcity of information and partiality of truth and possibility.
- The potential to perform a wide range of physical and mental activities without any measurements and complex computations.

According to the general intelligence theory proposed by Francis Galton intelligence means a genuine, anatomical-based mental faculty that can be analyzed by quantifying a persons reactive times to emotional situations.

2. HUMAN INTELLIGENCE:

There is no exact definition for the term ,,intelligence [4], rightly so it makes sense that trying to define the true meaning of the word intelligence is too ambiguous.

2.1 Defining Human Intelligence:

According to Cambridge online dictionary ,,intelligence is defined as "the ability to learn, understand and make judgments or have opinions that are based on reason" [5].According to psychologists perspective of intelligence is "intelligence is considered as a mental trait, is the capacity to make impulses focal at their early, unfinished stage of information.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Intelligence is therefore the capacity for abstraction which is an inhibitory process" [6].According to researchers, the perspective of intelligence is "intelligence is the power to rapidly find an adequate solution in what appears priori to be an immense search space" [7].

3. MEASURING HUMAN INTELLIGENCE:

„HUMINT which is the syllabic abbreviation for human intelligence, means intelligence gathering by means of interpersonal contact. „NATO defines „HUMINT as "a category of intelligence derived from information collected and provided by human sources" [8]. In the present world, human intelligence plays a major role as it is a more generalized concept and has wide range perspectives. The invention of autonomous systems simplified the way humans lived [9], but trying to understand and validate the level of intelligence embedded in these systems ismore complex and much more complicated to understand. According to Galileo Galilei, "what is not measurable make measurable" [10], but measuring intelligence is not same as measuring a physical entity. Intelligence is indeterminate, invisible and a physical phenomenon which makes it more complex and difficult to understand and measure. There different models that are proposed to measure human intelligence. Intelligence quotient is one of the extensively used measurement techniques since it gives some kind of quantitative value.

4. HUMAN INTELLIGENCE TEST MODELS:

Human intelligence models are created by considering various hominid factors such as environment, experience and age. According to [11] different standardized tests are recommended to measure intelligence for different age groups. Some of the important models are discussed below:

- Binet and Simon scale.
- Stanford-Binet intelligence scale (SBIS).
- David Wechsler intelligence scale (WISC).
- Comprehensive test of non verbal intelligence (CTONI).

4.1 Binet and Simon Scale:

Binet and Simon invented this scale to measure the intelligence of children between 2 to 23 years. This scale was designed based on [12] which is used to measure the person□s ability and to identify the problems faced by them in grasping knowledge at schools. This scale consists of a set of questions which focuses more general knowledge and reasoning ability. For instance, assume that a person who is x years old solves a question thatwas mainly intended for a person x+y, then comparatively both have the same mental age, where x is the age of the person and y is a finite number which is greater than one.

4.2 Stanford Binet Intelligence Scale:

This scale is major revision of Binet and Simon scale proposed by Lewis Terman. This scale assesses the intelligence and emotional competence in children starting from two years and in adults. The Stanford-Binet scale tests intelligence across six areas: general intelligence, knowledge, fluid reasoning, quantitative reasoning, visual-spatial processing, and working memory [13].This scale consists of a new measure called Intelligence Quotient given by the formula [13]:

IQ= (Mental age/chorological age)*10

4.3 David Wechsler Scale:

Consistent with Wechsler□s theoretical notions, construct and predictive validity of the Wechsler scales are greatest at the more global IQ level. The different types of human intelligence measuring scales are:

- Wechsler Intelligence Scale for Children (WISC), age group between 2 to 16 yrs.
- Wechsler Intelligence Scale (WAIS), age group 2 to 90 yrs.

IQ is the measure of Normal Curve with standard deviation.

4.4 Comprehensive Test Of Non VerbalIntelligence:

This test is intended to assess learning skills, reasoning skills for physically challenged students.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

5. INTELLIGENCE SUB-ATTRIBUTES:

The oxford dictionary justifies of the term attribute as "a quality or feature regarded as a characteristic or inherent part of someone or something" [14]. The attributes of a car can be color, shape, etc, which can be easily measured but contemporarily it is not that easy in case of intelligence. Measurement is an operation performed to establish relationship from empirical world to real world. In the present world IQ tests are broadly used to measure intelligence. According to Nikola kasabov, mentioned the following properties of human intelligence in his ,,Evolving intelligence in humans and machines [15]: adaptive learning, associative memory, pattern recognition, language communication, concept formation, abstract thinking, common sense knowledge, consciousness.

6. SCALE TYPES, WEAKNESS AND STRENGHTS of MEASURES:

The tests that are proposed to measure human intelligence givequantifiable results to some extent but have pros and cons which are discussed further in the document. It is difficult to measure human intelligence quantitatively as decision making is a complex phenomenon [15]. The constraints in measuring the intelligence of a person is that it can be broadly affected by social and environmental factors which are not simple to understand. Referring to Gencel Cigdem, lecture 2 [10] there are various types of basic measurement scales: Nominal, Ordinal, Interval, Ratio and Absolute, depending on their strength in increasing order. Intelligence quotient (IQ) tests are the most researched approach to intelligence and most extensively used in practical setting. But the weakness of this test is that it concentrates only on attenuated aspects of human intelligence but not the broader perspective. These tests are based on psychometric approach hence an ordinal scale is involved. The Binet and Simon scale, Stanford-Binet intelligence scales are used to measure the intelligence of children [12]. The weakness associated with this measure is that the decision of concluding the status of mental ability of the child belonging to a particular age depends on the score gained on solving the question which might not be true at all times hence these measures are classified into Ratio scale.

Stanford Biet intelligence is advantageous because it focuses on broader aspects like reasoning, verbal and non verbal skill. Comprehensive test of non verbal intelligence focuses more on non verbal reasoning skills of physically challenged persons.

7. REFLECTIONS:

We as students observed that there is no definite definition for the term intelligence. We came across intelligence measure tests such as GRE, TOEFL which are being used in the present education system to judge the aptitude and commutation level. We also understand that tests do not measure intelligence accurately but to some extent provide us plausible results. In the present world software organizations follow a traditional approach for recruiting people which involves a screening test which filters people based on their aptitude and mental ability. The score obtained determines the ability of the person, this approach to some extent is quantitative but not fruitful at all times.

8. CONCLUSION:

This report describes the importance of measurement in various aspects of life. The non deterministic nature of intelligence makes it difficult to measure it. As the concept of intelligence is more complex and complicated we need to use experimental comparative values. These scales measure intelligence quantitatively but only to some extent. It also explains the various intelligence scale types, strengths and weakness. Finally we came to an understanding that intelligence is a concept which keeps on changing dynamically.

9. ACKNOWLEDGEMENT:

On reaching the verge of completion of our papper we came up with some fascinating facts like importance of metrics in other fields such as psychology, different intelligent scales, strengths and weaknesses.

10. REFERENCES:

[1] Oxford Dictionaries, http://oxforddictionaries.com/view/entry/m_en_gb0415230# m_en_gb0415230

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[2]Albus, J.S.; , "Outline for a theory of intelligence," Systems, Man and Cybernetics, IEEE Transactions on , vol.21, no.3, pp.473-509, May/Jun 1991doi: 10.1109/21.97471URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnu mber=97471&isnumber=3093

[3]Zadeh, L.A.; , "Toward human level machine intelligence-isitachievable?,"CognitiveInformatics,2008.ICCI 2008.7thIEEEInternationalConferenceon,vol.,no.,pp.1, 14-16 Aug. 2008doi: 10.1109/COGINF.2008.4639144URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4639144&isnumber=4639143

[4]Shane LEGG and Marcus HUTTER, "A collection of Definitions of Intelligence", IOS press,2007.

[5]Cambridge Dictionary http://dictionary.cambridge.org/dictionary/british/intelli genc e_1

[6]L.L.Thurstone, "The nature of intelligence", Routledge,London,1924.

[7]D.Lenat and E.Feigenbaum, "On the thresholds of knowledge, Artificial intelligence", 1991.

[8]AAP-6 (2004) - NATO Glossary of terms and definitions.

[9] Zhongzhi Shi; "On Intelligence Science and Recent Progresses," Cognitive Informatics, 2006. ICCI 2006. 5th IEEE International Conference on, vol., no., pp.16-16, 17-19July 2006.

[10] Gencel Cigdem, Lecture-2, Fundamentals of measurement "Theory of Measurement", in software metrics course, blekinge institute of technology, karlskrona,2011.

[11] Individually administered Intelligence Tests, available at http://www.indiana.edu/~intell/intelligenceTests.shtml

[12] Wechsler's Intelligence Scales: Theoretical and Practical Considerations ,Robert A. Zachary, The Psychological Corporation, San Antonio, Texas, Journal of Psycho educational Assessment, Vol. 8, No. 3, 276-289 (1990).

[13] Stanford-Binet Intelligence scale, http://www.healthofchildren.com/S/Stanford-Binet- Intelligence-Scales.html.

[14]AccordingtoOxfordDictionary,http://www.oxford-dictionaries.com/view/entry/m_en_gb0048020#m_en_gb0048020.

[15] Kasabov, N.; "Evolving Intelligence in Humans and Machines: Integrative Evolving Connectionist Systems Approach, "computational intelligence Magazine, IEEE, vol.3, no.3, pp.23-37, August 2008.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

An Automatic Method of Filtering Unwanted Messages from Online Social Network User Walls

G.Sindhuja
M.Tech (CSE)
Dept of CSE,
KBR Engineering College,
Pagidipally Bhongir, Nalgonda ,Telangana.

S. Siva Kumar
Associate professor, 8 Years Exp,
Dept of CSE,
KBR Engineering College,
Pagidipally Bhongir, Nalgonda ,Telangana.

Abstract:

The very basic requirement in present days Online Social Networks (OSNs) or Mobile Social Networks (MSNs) is to enable users with the facility to filter and moderate the messages posted on their own private space(like Profile pages, walls etc) to evade that unnecessary content is displayed. As of now Online Social Networks (OSNs) do not provide any kind options in order to fill this user requirement. To address this issue, in this paper, we propose a system allowing Online Social Networks (OSNs) users to have a direct control on the messages posted on their profiles and walls. This is accomplished through a flexible rule-based system, that permits registered users to modify the filtering criteria to be applied to their walls, and a Machine Learning based soft classifier automatically labeling messages in support of content-based filtering.

Keywords:

Online Social Networks, Information Filtering, Short Text Classification, Policy-based Personalization, User Profile Page.

Introduction:

A social networking service is a platform to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services.

Social networks are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging.More and more, the line between mobile and web is being blurred as mobile apps use existing social networks to create native communities and promote discovery, and web-based social networks take advantage of mobile features and accessibility. As mobile web evolved from proprietary mobile technologies and networks, to full mobile access to the Internet, the distinction changed to the following types:

1) Web based social networks being extended for mobile access through mobile browsers and smartphone apps, and
2) Native mobile social networks with dedicated focus on mobile use like mobile communication,location-based services, and augmented reality, requiring mobile devices and technology.

However, mobile and web-based social networking systems often work symbiotically to spread content, increase accessibility and connect users from wherever they are. Users of these online networking sites form a social network, which provides a powerful means of organizing and finding useful information. This communication involves exchange of several types of content including text, image, audio and video data.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Therefore in Online Social Networks (OSN), there is a chance of posting unwanted content on particular public/private areas, called in general walls.Information filtering has been greatly explored for what concerns textual documents and, more recently, web content. It can be used to give users the ability to automatically control the messages written on their own walls, by filtering out unwanted messages. In this paper, our main aim is to survey the classification technique and to study the design of system to filter the undesired messages from OSN user wall.

Existing System:

We believe that this is a key OSN service that has not been provided so far. Indeed, today OSNs provide very little support to prevent unwanted messages on user walls. For example, Face book allows users to state who is allowed to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends). However, no content-based preferences are supported and therefore it is not possible to prevent undesired messages, such as political or vulgar ones, no matter of the user who posts them. Providing this service is not only a matter of using previously defined web content mining techniques for a different application, rather it requires to design ad-hoc classification strategies. This is because wall messages are Constituted by short text for which traditional classification Methods have serious limitations since short texts do not Provide sufficient word occurrences.

Disadvantages of Existing System:

• However, no content-based preferences are supported and therefore it is not possible to prevent undesired messages, such as political or vulgar ones, no matter of the user who posts them.

• Providing this service is not only a matter of using previously defined web content mining techniques for a different application, rather it requires to design ad hoc classification strategies.

• This is because wall messages are constituted by short text for which traditional classification methods have serious limitations since short texts do not provide sufficient word occurrences.

Proposed System:

The aim of the present work is therefore to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. We exploit Machine Learning (ML) text categorization techniques to automatically assign with each short text message a set of categories based on its content. The major efforts in building a robust short text classifier (STC) are concentrated in the extraction and selection of a set of characterizing and discriminant features. The solutions investigated in this paper are an extension of those adopted in a previous work by us from which we inheritthe learning model and the elicitation procedure for generating preclassified data. The original set of features, derived from endogenous properties of short texts, is enlarged here including exogenous knowledge related to the context from which the messages originate. As far as the learning model is concerned, we confirm in the current paper the use of neural learning which is today recognized as one of the most efficient solutions in text classification.In particular, we base the overall short text classification strategy on Radial Basis Function Networks (RBFN) for their proven capabilities in acting as soft classifiers, in managing noisy data and intrinsically vague classes. Moreover, the speed in performing the learning phase creates the premise for an adequate use in OSN domains, as well as facilitates the experimental evaluation tasks. We insert the neural model within a hierarchical two level classification strategy. In the first level, the RBFN categorizes short messages as Neutral and Nonneutral; in the second stage, Nonneutral messages are classified producing gradual estimates of appropriateness to each of the considered category. Besides classification facilities, the system provides a powerful rule layer exploiting a flexible language to specify Filtering Rules (FRs), by which users can state what contents, should not be displayed on their walls. FRs can support a variety of different filtering criteria that can be combined and customized according to the user needs. More precisely, FRs exploit user profiles, user relationships as well as the output of the ML categorization process to state the filtering criteria to be enforced. In addition, the system provides the support for user-defined Blacklists (BLs), that is, lists of users that are temporarily prevented to post any kind of messages on a user wall.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

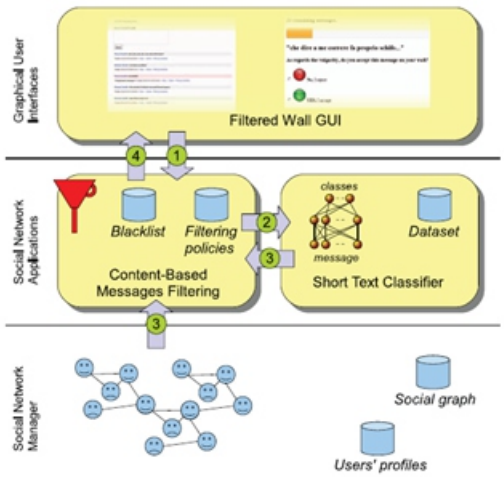
Advantages of Proposed System:

• A system to automatically filter unwanted messages from OSN user walls on the basis of both message content and the message creator relationships and characteristics.
• The current paper substantially extends for what concerns both the rule layer and the classification module.
• Major differences include, a different semantics for filtering rules to better fit the considered domain, an online setup assistant (OSA) to help users in FR specification, the extension of the set of features considered in the classification process, a more deep performance evaluation study and an update of the prototype implementation to reflect the changes made to the classification techniques.

Implementation:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

System Architecture:



Modules:

1. Filtering rules :

In defining the language for FRs specification, we consider three main issues that, in our opinion, should affect a message filtering decision. First of all, in OSNs like in everyday life, the same message may have different meanings and relevance based on who writes it. As a consequence, FRs should allow users to state constraints on message creators. Creators on which a FR applies can be selected on the basis of several different criteria; one of the most relevant is by imposing conditions on their profile's attributes. In such a way it is, for instance, possible to define rules applying only to young creators or to creators with a given religious/political view. Given the social network scenario, creators may also be identified by exploiting information on their social graph. This implies to state conditions on type, depth and trust values of the relationship(s) creators should be involved in order to apply them the specified rules. All these options are formalizedby the notion of creator specification, defined as follows.

2. Online setup assistant for FRs thresholds:

As mentioned in the previous section, we address the problem of setting thresholds to filter rules, by conceiving and implementing within FW, an Online Setup Assistant (OSA) procedure. OSA presents the user with a set of messages selected from the dataset discussed in Section VI-A. For each message, the user tells the system the decision to accept or reject the message. The collection and processing of user decisions on an adequate set of messages distributed over all the classes allows to compute customized thresholds representing the user attitude in accepting or rejecting certain contents. Such messages are selected according to the following process. A certain amount of non neutral messages taken from a fraction of the dataset and not belonging to the training/test sets, are classified by the ML in order to have, for each message, the second level class membership values.

3. Blacklists:

A further component of our system is a BL mechanism to avoid messages from undesired creators,

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

independent from their contents.BLs are directly managed by the system, which should be able to determine who are the users to be inserted in the BL and decide when users retention in the BL is finished. To enhance flexibility, such information are given to the system through a set of rules, hereafter called BL rules. Such rules are not defined by the SNM, therefore they are not meant as general high level directives to be applied to the whole community. Rather, we decide to let the users themselves, i.e., the wall's owners to specify BL rules regulating who has to be banned from their walls and for how long. Therefore, a user might be banned from a wall, by, at the same time, being able to post in other walls.

Similar to FRs, our BL rules make the wall owner able to identify users to be blocked according to their profiles as well as their relationships in the OSN. Therefore, by means of a BL rule, wall owners are for example able to ban from their walls users they do not directly know (i.e., with which they have only indirect relationships), or users that are friend of a given person as they may have a bad opinion of this person. This banning can be adopted for an undetermined time period or for a specific time window. Moreover, banning criteria may also take into account users' behavior in the OSN. More precisely, among possible information denoting users' bad behavior we have focused on two main measures. The first is related to the principle that if within a given time interval a user has been inserted into a BL for several times, say greater than a given threshold, he/she might deserve to stay in the BL for another while, as his/her behavior is not improved. This principle works for those users that have been already inserted in the considered BL at least one time. In contrast, to catch new bad behaviors, we use the Relative Frequency (RF) that let the system be able to detect those users whose messages continue to fail the FRs. The two measures can be computed either locally, that is, by considering only the messages and/or the BL of the user specifying the BL rule or globally, that is, by considering all OSN users walls and/or BLs.

Conclusion:

In this paper, we have presented a system to filter undesired messages from OSN walls. The system develops a ML soft classifier to implement customizable content-dependent FRs. In particular, we aim at investigating a tool able to automatically recommend trust values for those contacts user does not individually identified. We do consider that such a tool should propose expectation assessment based on users procedures, performances, and reputation in OSN, which might involve enhancing OSN with assessment methods. Though, the propose of these assessment-based tools is difficult by several concerns, like the suggestions an assessment system might have on users' confidentiality and/or the restrictions on what it is possible to audit in present OSNs. An introduction work in this direction has been prepared in the context of expectation values used for OSN access control purposes. However, we would like to remark that the system proposed in this paper represents just the core set of functionalities needed to provide a sophisticated tool for OSN message filtering. Still if we have balanced our system with an online associate to set FR thresholds, the improvement of a absolute system effortlessly exploitable by average OSN users is a wide topic which is out of the scope of the present paper.

References:

[1] Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, and Moreno Carullo "A System to Filter Unwanted Messages from OSN User Walls"- Ieee Transactions On Knowledge And Data Engineering, Vol. 25, No. 2, February 2013.

[2] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo and E. Ferrari, Content-based Filtering in On-line Social Networks

[3] A. Adomavicius, G.and Tuzhilin, "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions," IEEE Transaction on Knowledge and Data Engineering,vol. 17, no. 6, pp. 734–749, 2005.

[4] M. Chau and H. Chen, "A machine learning approach to web page filtering using content and structure analysis," Decision Support Systems, vol. 44, no. 2, pp. 482–494, 2008.

[5] B. Sriram, D. Fuhry, E. Demir, H. Ferhatosmanoglu, and M. Demirbas, "Short text classification in twitter

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

to improve information filtering,"in Proceeding of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval, SIGIR 2010, 2010, pp. 841–842.

[6] K. Nirmala, S. Satheesh kumar, "A Survey on Text Categorization in Online Social Networks," in Proceedings ofInternational Journal of Emerging Technology and Advanced Engineering,Volume 3, Issue 9, September 2013.

[7] A. K. Jain, R. P.W. Duin, and J. Mao, "Statistical pattern recognition:A review," IEEE Transactions on Pattern Analysis and MachineIntelligence, vol. 22, pp. 4–37, 2000.

[8] F. Sebastiani, "Machine learning in automated text categorization,"ACM Computing Surveys, vol. 34, no. 1, pp. 1–47, 2002.

[9] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, and E. Ferrari,"Content-based filtering in on-line social networks," in Proceedings of ECML/PKDD Workshop on Privacy and Security issues in Data Mining and Machine Learning (PSDML 2010), 2010.

[10]P.W. Foltz and S.T. Dumais, "Personalized Information Delivery: An Analysis of Information Filtering Methods," Comm. ACM,vol. 35, no. 12, pp. 51-60, 1992.

[11] S. Zelikovitz and H. Hirsh, "Improving short text classification using unlabeled background knowledge," in Proceedings of 17th International Conference on Machine Learning (ICML-00), P. Langley, Ed.Stanford, US: Morgan Kaufmann Publishers, San Francisco, US,2000

[12] S. Pollock, "A rule-based message filtering system," ACM Transactions on Office Information Systems, vol. 6, no. 3, pp. 232–254,1988.

[13] J. Moody and C. Darken, "Fast learning in networks of locally-tuned processing units," Neural Computation, vol. 1, p. 281, 1989.

[14] W. B. Frakes and R. A. Baeza-Yates, Eds., Information Retrieval:Data Structures & Algorithms. Prentice-Hall, 1992.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Providing Security and Confidentiality in a Credential Based Publisher/Subscriber Environment

A.Shirisha
M.Tech,
Dept of CSE,
Swami Ramananda Tirtha Institute of Science and Technology, Nalgonda.

B.Srikanth Reddy, M.Tech
Assistant Professor,
Dept of CSE,
Swami Ramananda Tirtha Institute of Science and Technology, Nalgonda.

T. Madhu, M.Tech, Ph.D
Head of the Dept,
Dept of CSE,
Swami Ramananda Tirtha Institute of Science and Technology, Nalgonda.

Abstract:

Identification and confidentiality are the main objective of any distributed system. Provision of security operations such as authentication and confidentiality is highly challenging in a content based publish/ subscribe system. Identification is an essential mechanism in distributed information systems. The main concept is to share the secured data between the subscribers using attributes,it may a weak notion but the concept of multi-credential routing makes it robust. This paper presents the mainly 1)The idea of identity (ID)-based public key cryptosystem, which enables users to communicate, a publisher which acts as an admin uses a private key to each user when first joins the networks.2) It provides the pairing based cryptography to maintain the authenticity and confidentiality of the publisher and subscribers by maintaining the secure layer maintenance protocol.3)The attributes helps to share data by generating a secure route between the publisher and subscriber.4) The provision to attempt the three goals of secure pub/sub system i.e. authentication, confidentiality, scalability by performing hard encryptions on the data to prevent thes malicious publishers to enter in the network,a thorough analysis of attacks is performed on the system.

Keywords:

confidentiality, security, identity based encryption, multicredential routing

I. INTRODUCTION:

In Pub/sub system access control is possible only to the authorized users. Personal details should kept hidden from the other subscriber in the network and a subscriber should receive all relevant events without revealing its subscription to the system. Afterwards the idea of the identity based encryption is implemented in the system. For PKI, publishers must maintain the public keys of all interested subscribers to encrypt events. Subscribers must know the public keys of all relevant publishers to verify the authenticity of the receive events. This paper allows subscribers to maintain credentials according to their subscriptions. Private keys assigned to the subscribers are labeled with the credentials. A publisher encrypts all the set of events with the help of credentials. We adapted identity-based encryption (IBE) mechanisms[1][2] 1) to ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and the key; and 2) to allow subscribers to verify the authenticity of received events . Steps are taken to improve the weaker subscription between the publisher and subscriber by implementing the secure maintenance protocol .The paper also present the three objectives in the system [3][6]1) to implement the searchable encryption method by using the identity based encryption 2)to implement the phenomenon of "multicredential routing" which improves the weak subscription. 3) analysis of different attacks to improve confidentiality and authentication. There are three major goals for the proposed secure pub/sub system, namely to support authentication, confidentiality, and, scala- bility [3].

Authentication:

To avoid noneligible publications, only authorized publishers should be able to publish events in the system. Similarly, subscribers should only receive those messages to which they are authorized to subscribe[1].

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Confidentiality:

In a broker-less environment, two aspects of confidentiality are of interest that the events are only visible to authorized subscribers and are protected from illegal modifications, and the

II RELATED WORK:

However, malicious publishers may masquerade the authorized publishers and spam the overlay network with fake and duplicate events. We do not intend to solve the digital copyright problem; therefore, authorized subscribers do not reveal the contentsubscriptions of subscribers are confidential and unforgeable[1].

Scalability:

The secure pub/sub system should scale with the number of subscribers in the system. Three aspects are important to preserve scalability[1]:
1) the number of keys to be managed and the cost of subscription should be independent of the number of subscribers in the system,
2) the key server and subscribers should maintain small and constant numbers of keys per subscription, and 3) the overhead because of rekeying should be minimized without compromising the fine-grained access control. of successfully decrypted events to other subscribers.

A. Publisher subscriber technique :

Publishers and subscribers interact with a key server. They provide credentials to the key server and in turn receive keys which fit the expressed capabilities in the credentials. Subsequently, those keys can be used to encrypt, decrypt, and sign relevant messages in the content based pub/sub system, i.e., the credential becomes authorized by the key server. A credential consists of two parts: 1) a binary string which describes the capability of a peer in publishing and receiving events, and 2) a proof of its identity [1].

B. Identity based encryption:

Identity (ID)-based public key cryptosystem, which enables any pair of users to communicate securely with out exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted key generation center issues a private key to each user when he first joins the network [2].

C. Identity Handling:

Identification provides an essential building block for a large number of services and functionalities in distributed Information systems. In its simplest form, identification Is used to uniquely denote computers on the Internet By IP addresses in combination with the Domain Name System (DNS) as a mapping service between symbolic Names and IP addresses. Thus, computers can conveniently Be referred to by their symbolic names, whereas, in The routing process, their IP addresses must be used.[3] Higher-level directories, such as X.500/LDAP, consistently Map properties to objects which are uniquely identified by Their distinguished name (DN), i.e., their position in the X.500 tree [4].

D. Content based publish/subscribe:

Content-based networking is a generali- zation of the content based publish/subscribe model. [4] In content-based networking, messages are no longer addressed to the communication end-points . Instead, they are published to a distributed information space and routed by the networking sub -strate to the "interested" communication end-points. In most cases, the same substrate is responsible for realizing naming, binding and the actual content delivery [5].

E. Secure Key Exchange:

A key-exchange (KE) protocol is run in a network of interconnected parties where each party can be activated to run an instance of the protocol called a session [6]. Within a session a party can be activated to initiate the session or to respond to an incoming message. As a result of these activations, and according to the specification of the protocol, the party creates and maintains a session state, generates outgoing messages, and eventually completes the session by outputting a session-key and erasing the session state [7].

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

III. PROPOSED WORK:

Subscribers will interact with the publisher. Subscriber will provide credentials to the publisher and in turn receive keys which fit the expressed capabilities in the credentials. The keys are generated using checksum algorithm and it is distributed to the publisher and subscriber. Publisher will encrypt the data with the encryption decryption algorithm and embedded the key with data. The subscriber will login as the publisher sends the acknowledgement by means of email. The subscriber gets the private key to decrypt the data in the email. The various data sharing techniques by which the data will get shared by the publisher to the subscriber are:

A. Numerals attribute:

In this type of attribute the data is distributed in the forms of the spaces. The spaces are decomposed into the subspaces which serve the limited range of enclosure between the publisher and subscriber. Subspaces are denoted by 0 & 1. For example, an event 0010 is enclosed by the five subspaces 0010, 001, 00, 0,hence we have to generate the ciphertext according to the events of the subspaces.

B. Alphastring attribute:

Credentials for alphastring string operations are performed by using the process of prefixing the node using a trie. The root will be given a particular string and same string is given to the descendants using the different prefixes. Each peer is assigned a single credential, which is same as its subscription or advertisement.

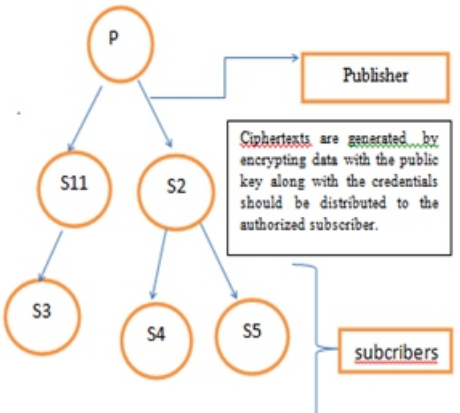


Fig: Data sharing between publisher and subscriber using identity based encryption

IV. CONCLUSION :

Scalability is achieved by increasing the number of subscribers .Using public key cryptography the publisher can distribute the private keys to the subscribers once they submitted the credentials, as cipher text are labeled with the credentials to maintain the authenticity in the system. We have adapted a technique from identity based encryption to ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and its private keys to maintain the confidentiality of the subscribers.

REFERENCES:

[1] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel" Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption" IEEE transactions on parallel and distributed systems, vol. 25, no. 2, February 2014.

[2] D. Boneh and M.K. Franklin, "Identity-Based Encryption from theWeil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2011.

[3] Karl aberer, Aniwitaman datta and Manfred Hauswirth "Efficient Self Contained Handling of Identity in Peer to Peer System"IEEE transaction on know- ledge and data engineering,2004.

[4] Sean O,Mealia and Adam J.Elbirt "Enhancing the Performance of Symmetric –key cryptography via Instruction set instruction" IEEE transactions on very large scale integeration vol.18 no.11 november 2011.

[5] Ming li,Shucheng Yu.Yao Zheng,Kui Reng, Weiging Lou "Scalable and secure sharing of personal data in cloud computing using attribute-based encryption"IEEE transaction on paralllel and distributed computing 2013

[6] Legathaux Martins and Sergio Duarte "Routing Algorithms for Content based publish/subscribe system"IEEE commm- unications and tutorials first quarte 2010. [7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2010.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

An Innovative Framework for Resource Allocation Based on Virtual Machines(VMs) in the Cloud

Ch.Anusha
M.Tech,
Dept of CSE,
Prasad Engineering College,
Jangom (PECJ).

Dr.K.Babu Rao, M.Tech, Ph.D
Professor,
Dept of CSE,
Prasad Engineering College,
Jangom (PECJ).

MR. M.Srikanth
Asst Professor & HOD,
Dept of CSE,
Prasad Engineering College,
Jangom (PECJ).

Abstract:

Cloud computing allows business customers to scale up and down their resource usage based on needs. Many of the touted gains in the cloud model come from resource multiplexing through virtualization technology. In this paper, we present a system that uses virtualization technology to allocate data center resources dynamically based on application demands and support green computing by optimizing the number of servers in use. We introduce the concept of "skewness" to measure the u nevenness in the multi-dimensional resource utilization of a server. By minimizing skewness, we can combine different types of workloads nicely and improve the overall utilization of server resources. We develop a set of heuristics that prevent overload in the system effectively while saving energy used. Trace driven simulation and experiment results demonstrate that our algorithm achieves good performance

Index Terms:

Cloud computing, Green computing, Resource, Skewness, Virtual machine.

I. INTRODUCTION:

Cloud computing is the delivery of computing and storage capacity as a service to a community of end recipients. The name comes from the use of a cloud shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts services with a user's data, software and computation over a network. The remote accessibility enables us to access the cloud services from anywhere at any time. To gain the maximum degree of the above mentioned benefits, the services offered in terms of resources should be allocated optimally to the applications running in the cloud.

The elasticity and the lack of upfront capital investment offered by cloud computing is appealing to any businesses. In this paper, we discuss how the cloud service provider can best multiplex the available virtual resources onto the physical hardware. This is important because much of the touted gains in the cloud model come from such multiplexing. Virtual Machine Monitors (VMMs) like Xen provide a mechanism for mapping Virtual Machines (VMs) to Physical Resources [3]. This mapping is hidden from the cloud users. Users with the Amazon EC2 service [4], for example, do not know where their VM instances run. It is up to the Cloud Service Provider to make sure the underlying Physical Machines (PMs) has sufficient resources to meet their needs VM live migration technology makes it possible to change the mapping between VMs and PMs While applications are running [5], but,a policy issue remains as how to decide the mapping adaptively so that the resource demands of VMs are met while the number of PMs used is minimized.

This is challenging when the resource needs of VMs are heterogeneous due to the diverse set of applications they run and vary with time as the workloads grow and shrink. The capacity of PMs can also be heterogeneous because multiple generations of hardware co-exist in a data center. To achieve the overload avoidance that is the capacity of a PM should be sufficient to satisfy the resource needs of all VMs running on it. Otherwise, the PM is overloaded and can lead to degraded performance of its VMs. And also the number of PMs used should be minimized as long as they can still satisfy the needs of all VMs. Idle PMs can be turned off to save energy. In this paper, we presented the design and implementation of dynamic resource allocation in the Virtualized Cloud Environment which maintains the balance between the following two goals.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Goals to Achieve:

Overload Avoidance. The capacity of a PM must satisfy the resource needs from all VMs running on it. Or else, the PM is overloaded and leads to provide less performance of its VMs. Green computing. The number of PMs used should be optimized as long as they could satisfy the needs of all VMs. And Idle PMs can be turned off to save energy. There is an in depth tradeoff between the two goals in the face of changing resource needs from all VMs. To avoid the overload, should keep the utilization of PMs low to reduce the possibility of overload in case the resource needs of VMs increase later. For green computing, should keep the utilization of PMs reasonably high to make efficiency in energy [7]. A VM Monitor manages and multiplexes access to the physical resources, maintaining isolation between VMs at all times. As the physical resources are virtualized, several VMs, each of which is self-contained with its own operating system, can execute on a physical machine (PM). The hypervisor, which arbitrates access to physical resources, can manipulate the extent of access to a resource (memory allocated or CPU allocated to a VM, etc.).

II. RELATED WORK:

In [2] author proposed architecture, using feedback control theory, for adaptive management of virtualized resources, which is based on VM. In this VM-based architecture all hardware resources are pooled into common shared space in cloud computing infrastructure so that hosted application can access the required resources as per there need to meet Service Level Objective (SLOs) of application. The adaptive manager use in this architecture is multi-input multi-output (MIMO) resource manager, which includes 3 controllers:CPU controller, memory controller and I/O controller, its goal is regulate multiple virtualized resources utilization to achieve SLOs of application by using control inputs per-VM CPU, memory and I/O allocation. The seminal work of Walsh et al. [3], proposed a general two-layer architecture that uses utility functions, adopted in the context of dynamic and autonomous resource allocation, which consists of local agents and global arbiter. The responsibility of local agents is to calculate utilities, for given current or forecasted workload and range of resources, for each AE and results are transfer to global arbiter.

Where, global arbiter computes near-optimal configuration of resources based on the results provided by the local agents. In [4], authors propose an adaptive resource allocation algorithm for the cloud system with preempt able tasks in which algorithms adjust the resource allocation adaptively based on the updated of the actual task executions. Adaptive list scheduling (ALS) and adaptive min-min scheduling (AMMS) algorithms are use for task scheduling which includes static task scheduling, for static resource allocation, is generated offline. The online adaptive procedure is use for re-evaluating the remaining static resource allocation repeatedly with predefined frequency. The dynamic resource allocation based on distributed multiple criteria decisions in computing cloud explain in [6]. In it author contribution is tow-fold, first distributed architecture is adopted, in which resource management is divided into independent tasks, each of which is performed by Autonomous Node Agents (NA) in ac cycle of three activities:(1) VM Placement, in it suitable physical machine (PM) is found which is capable of running given VM and then assigned VM to that PM, (2) Monitoring, in it total resources use by hosted VM are monitored by NA, (3) In VM selection, if local accommodation is not possible, a VM need to migrate at another PM and process loops back to into placement and second, using PROMETHEE method, NA carry out configuration in parallel through multiple criteria decision analysis. This approach is potentially more feasible in large data centers than centralized approaches.

III.PROPOSED SYSTEM:

This proposed system consists of number of servers, predictor, hotspot and cold spot solvers and migration list. Set of servers used for running different applications. Predictor is used to execute periodically to evaluate the resource allocation status based on the predicted future demands of virtual machines.

A. System Overview:

The architecture of the system is presented in Figure 1. Each physical machine (PM) runs the Xen hypervisor (VMM) which supports a privileged domain 0 and one or more domain U [7]. Each VM in domain U encapsulates one or more applications such as Web server, remote desktop, DNS, Mail, Map/Reduce, etc.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

We assume all PMs share a backend storage. The multiplexing of VMs to PMs is managed using the Usher framework [8]. The main logic of our system is implemented as a set of plug-ins to Usher. Each node runs an Usher local node manager (LNM) on domain o which collects the usage statistics of resources for each VM on that node. The statistics collected at each PM are forwarded to the Ushercentral controller (Usher CTRL) where our VM scheduler runs.

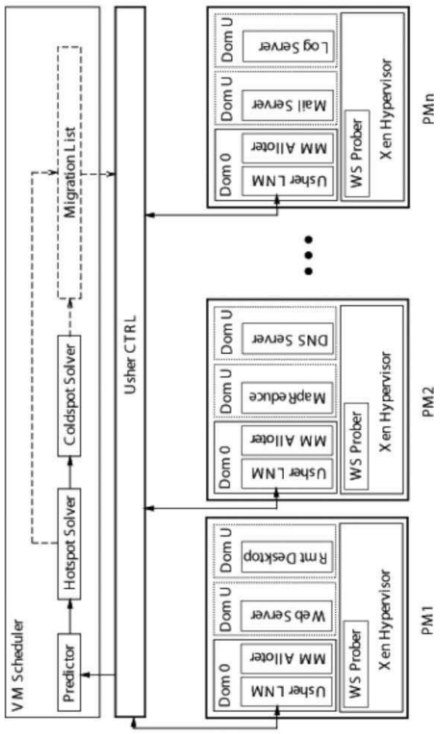


Fig. 1 System Architecture

The VM Scheduler is invoked periodically and receives from the LNM the resource demand history of VMs, the capacity and the load history of PMs, and the current layout of VMs on PMs. The scheduler has several components. The predictor predicts the future resource demands of VMs and the future load of PMs based on past statistics. We compute the load of a PM by aggregating the resource usage of its VMs. The LNM at each node first attempts to satisfy the new demands locally by adjusting the resource allocation of VMs sharing the same VMM. The MM Alloter on domain o of each node is responsible for adjusting the local memory allocation. The hot spot solver in our VM Scheduler detects if the resource utilization of any PM is above the hot threshold (i.e., a hot spot). The cold spot solver checks if the average utilization of actively used PMs (APMs) is below the green computing threshold.

B. Skewness Algorithm:

We introduce the concept of "skewness" to measure t he unevenness in the multi-dimensional resource utilization of a server. By minimizing skewness, we can combine different types of workloads nicely and improve the overall utilization of server resources. Let n be the number of resources we consider and ri be the utilization of the i-th resource. We define the resource skewness of a server p as

$$skewness(p) = \sqrt{\sum_{i=1}^{n}(\frac{r_i}{\overline{r}} - 1)^2}$$

where r is the average utilization of all resources for server p. In practice, not all types of resources are performance critical and hence we only need to consider bottleneck resources in the above calculation. By minimizing the skewness, we can combine different types of workloads nicely and improve the overall utilization of server resources.

The flow chart represents the flow of an algorithm in Fig 2. Our algorithm executes periodically to evaluate the resource allocation status based on the predicted future resource demands of VMs. We define a server as a hot spot if the utilization of any of its resources is above a hot threshold. We define thetemperature of a hot spot p as the square sum of its resource utilization beyond the hot threshold:

$$temperature(p) = \sum_{r \in R}(r - r_t)^2$$

Where R is the set of overloaded resources in server p and rt is the hot threshold for resource r. We define a server as a cold spot if the utilizations of all its resources are below a cold threshold. This indicates that the server is mostly idle and a potential candidate to turn off to save energy.

Finally, we define the warm threshold to be a level of resource utilization that is sufficiently high to justify having the server running but not as high as to risk becoming a hot spot in the face of temporary fluctuation of application resource demands.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

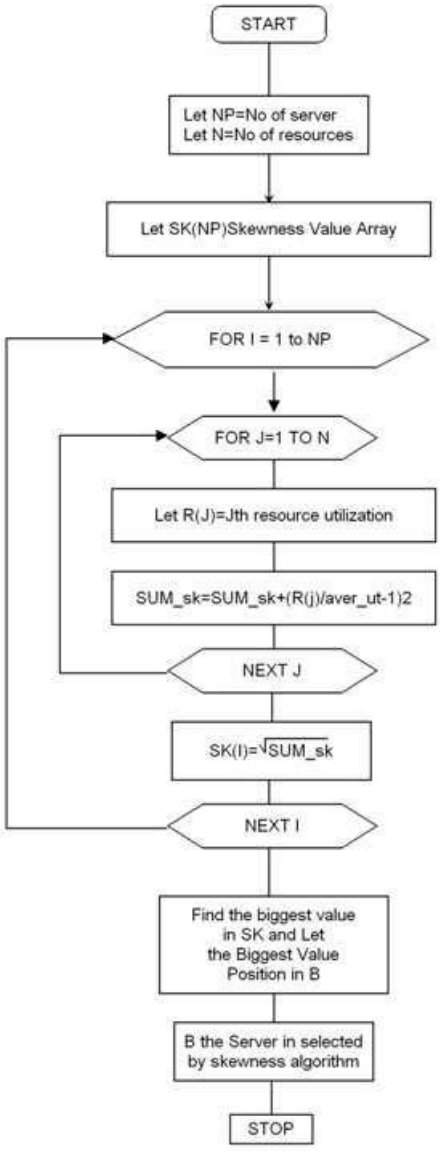


Fig. 2 Flow Chart of Skewness

C. Hotspot Mitigation:

We handle the hottest one first I.e. sort the list of hot spots in the system Otherwise, keep their temperature as low as possible. Our aim is to migrate the VM that can reduce the server's temperature. In case of ties, the VM whose removal can reduce the skewness of the server the most is selected. We first decide for each server p which of its VMs should be migrated away. Based on the resulting temperature we sort list the VMs of the server if that VM is migrated away. We see if we can find a destination server to accommodate it for each list of in the VM.

After accepting this VM the server should not become hot spot. We select one skewness which can be reduced the most by accepting this VM among all servers. We record the migration of the VM to that server and update the predicted load of related servers when the destination server is found. Else we move on to the next VM in the list and try to find a destination server for it. D .Green ComputingWhen the resource utilization of active servers is too low, some of them can be turned off to save energy. This is handledin our green computing algorithm. Our green computing algorithm is invoked when the average utilizations of all resources on active servers are below the green computing threshold. We check if we can migrate all its VMs somewhere else for a cold spot p. For each VM on p, we try to find a destination server to accommodate it. The utilizations of resources of the server after accepting the VM must be below the warm threshold. Section 7 in the supplementary file explains why the memory is a good measure in depth. We try to eliminate the cold spot with the lowest cost first. We select a server whose skewness can be reduced the most. If we can find destination servers for all VMs on a cold spot, we record the sequence of migrations and update the predicted load of related servers. Otherwise, we do not migrate any of its VMs.

IV.RESULTS AND DISCUSSION:

The goal of the skewness algorithm is to mix workloads with different resource requirements together so that the overall utilization of server capacity is improved. In this experiment, we see how our algorithm handles a mix of CPU, memory, and network intensive workloads. Resource allocation status of three servers A, B, C has total memory allocated 500KB and resource used memory for serverA 80KB,serverB 170KB and serverC 80K. In Fig. 4 each cloud users provide cloud service Resource allocation in green computing. In Fig.5 display Server usage and resource allocation status for user1 using Bar Chart. The cloud computing is a model which enables on demand network access to a shared pool computing resources. Cloud computing environment consists of multiple customers requesting for resources in a dynamic environment with their many possible constraints. The virtualization can be the solution for it. It can be used to reduce power consumption by data centers. The main purpose of the virtualization is that to make the most efficient use of available system resources, including energy.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A data center, installing virtual infrastructure allows several operating systems and applications to run on a lesser number of servers, it can help to reduce the overall energy used for the data center and the energy consumed for its cooling. Once the number of servers is reduced, it also means that data center can reduce the building size as well. Some of the advantages of Virtualization which directly impacts efficiency and contributes to the environment include: Workload balancing across servers, Resource allocation and sharing are better monitored and managed and the Server utilization rates can be increased up to 80% as compared to initial 10-15%.

Fig. 3 Resource Allocation Status

Fig. 4 View Resource Allocation Status using Bar Chart

The results are clear and having good contribution:

1)Allocation of resource is done dynamically.

2)Saves the energy using the green computing concept

3)Proper utilization of servers and memory utilization is taken care using skewness.

4)Minimize the total cost of both the cloud computing infrastructure and running application.

V.CONCLUSION:

We have presented the design, implementation, and evaluation of a resource management system for cloud computing services. Our system multiplexes virtual to physical resources adaptively based on the changing demand. We use the skewness metric to combine VMs with different resource characteristics appropriately so that the capacities of servers are well utilized. Our algorithm achieves both overload avoidance and green computing for systems with multi resource constraints.

VI. REFERENCES:

[1]M. Armbrust et al., "Above the Clouds: A Berkeley V iew of Cloud Computing," technical report, Univ. o California, B erkeley, Feb. 2009.
[2]L. Siegele, "Let It Rise: A Special Report on Corpo rate IT," The Economist, vol. 389, pp. 3-16, Oct. 2008.
[3]P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the Art of Virtualization," Proc. ACM Symp. Operating Systems Principles (SOSP '03), Oct. 2003E. H. Miller, "A note on refle ctor arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.
[4]"Amazon elastic compute cloud (Amazon EC2)," http://aws. amazon.com/ec2/, 2012.
[5]C. Clark, K. Fraser, S. Hand, J.G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, "Live Migration of Virtual Machine s," Proc. Symp. Networked Systems Design and Implementation (NSDI '05), May 2005..
[6]M. Nelson, B.-H. Lim, and G. Hutchins, "Fast Trans parent Migration for Virtual Machines," Proc. USENIX Ann. Technical Conf., 2005.M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.
[7]N. Bobroff, A. Kochut, and K. Beaty, "Dynamic Place ment of Virtual Machines for Managing SLA Violations," Proc. IFIP/I EEE Int'l Symp. Integrated Network Management (IM '07), 2007 .
[8]T. Wood, P. Shenoy, A. Venkataramani, and M. Yousif, "Black-Box and Gray-Box Strategies for Virtual Machine Migration," Proc. Symp. Networked Systems Design and Implementation (NSDI '07), Apr. 2007.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Authenticity Verification for Storing Information without Knowing User's Identity in Cloud

M.Harshini Sharma
M.Tech Student,
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

P. Dharshan
Associate Professor & HOD of CSE,
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

Abstract:

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. In this paper, we propose the secure data storage in clouds for a new decentralized access. The cloud verifies the authenticity of the series without knowing the user's identity in the proposed scheme. Our feature is that only valid users can able to decrypt the stored information. It prevents from the replay attack. This scheme supports creation, modification, and reading the data stored in the cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.

Keywords:

Decentralized access, Access control, authentication of user, cloud storage, Privacy Preserving, Anonymous authentication.

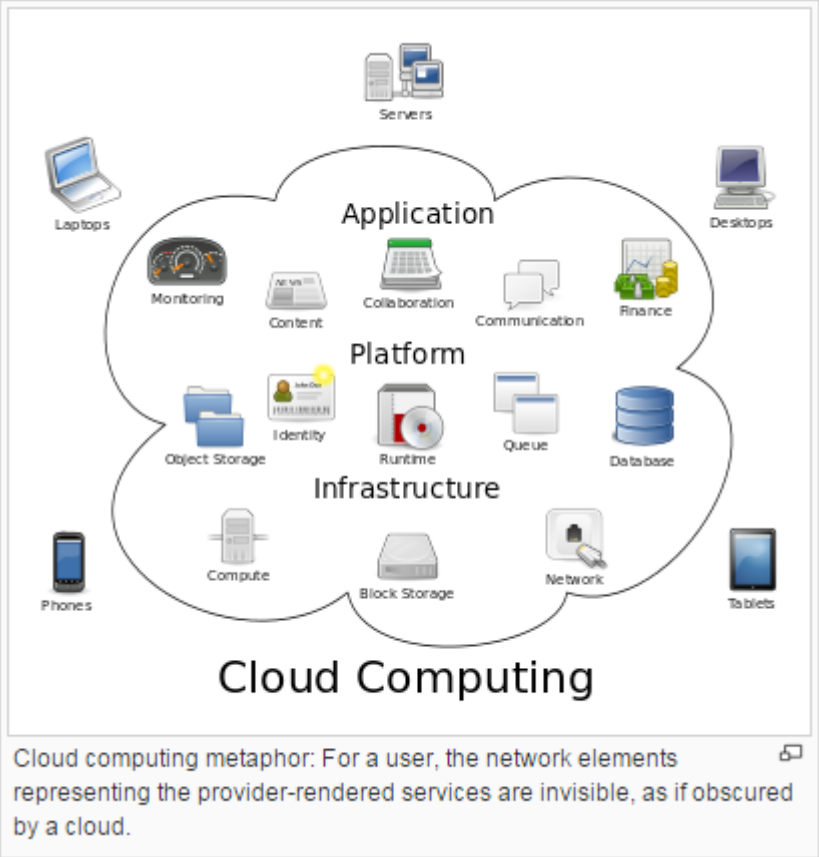
Introduction:

Cloud computing allows application software to be operated using internet-enabled devices. Clouds can be classified as public, private, and hybrid.

Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as one uses it).Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Companies can scale up as computing needs increase and then scale down again as demands decrease.



Cloud computing metaphor: For a user, the network elements representing the provider-rendered services are invisible, as if obscured by a cloud.

Cloud computing exhibits the following key characteristics:

Agility improves with users' ability to re-provision technological infrastructure resources.Cost reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house. Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.

Security and Privacy:

Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

have to agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.According to the Cloud Security Alliance, the top three threats in the cloud are "Insecure Interfaces and API's", "Data Loss & Leakage", and "Hardware Failure" which accounted for 29%, 25% and 10% of all cloud security outages respectively — together these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Therefore Information leakage may arise by mistake when information for one customer is given to other. Additionally, Eugene Schultz, chief technology officer at Emagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack — a process he called "hyperjacking".

RELATED WORK:

Access control in clouds is gaining consideration on the grounds that it is imperative that just authorized clients have access to services. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access strategy furthermore saved in the cloud. Clients are given sets of traits and corresponding keys. Just when the clients have matching set of attributes, would they be able to decrypt the data saved in the cloud. Access control is likewise gaining imperativeness in online social networking where users store their personal data, pictures, films and shares them with selected group of users they belong. Access control in online social networking has been studied in [S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in ACM ASIACCS, 2011].The work done by [F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.] gives privacy preserving authenticated access control in cloud. Nonetheless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients. Unfortunately, a single KDC is not just a single point of failure however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain. The scheme In [W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in ACM Cloud Computing Security Workshop (CCSW), 2009.] uses a symmetric key approach and does not support authentication. Multi-authority ABE principle was concentrated on in [M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.], which obliged no trusted power which requires each client to have characteristics from at all the KDCs. In spite of the fact that Yang et al. proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while accessing the cloud. Ruj et al. proposed a distributed access control module in clouds. On the other hand, the approach did not provide client verification. The other weakness was that a client can make and store an record and different clients can just read the record. write access was not allowed to clients other than the originator.Time-based file assured deletion, which is initially presented in [Perlman, "File System Design with Assured Delete," Proc.Network and Distributed System Security Symp. ISOC (NDSS), 2007.], implies that records could be safely erased and remain forever difficult to reach after a predefined time. The primary thought is that a record is encrypted with an information key by the possessor of the record, and this information key is further encrypted with a control key by a separate key Manager.

EXISTING SYSTEM:

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement. Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query.

DISADVANTAGES OF EXISTING SYSTEM:

- It is unsecure.
- No privacy.
- Anyone can able to access and modify the data.
- Problem here is that the data records should have keywords associated with them to enable the search.

PROPOSED SYSTEM:

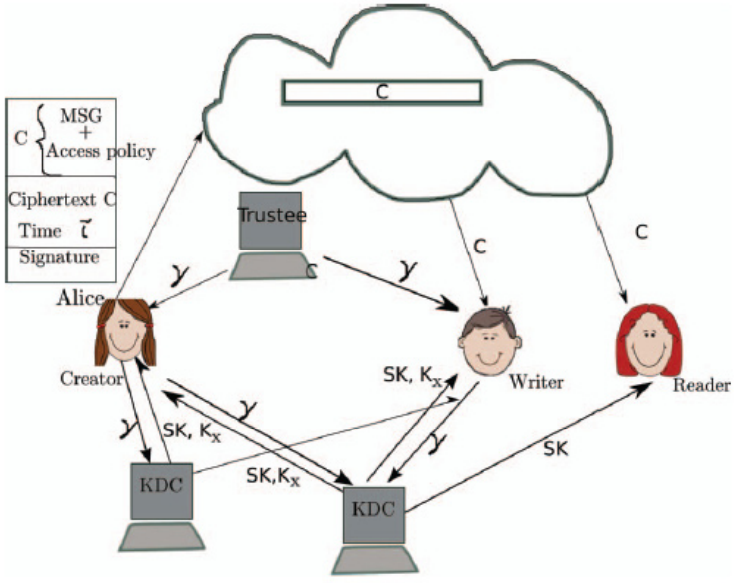
Although we proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication.

The other drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator.In the preliminary version of this paper, we extend our previous work with added features that enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud.In this version we also address user revocation, that was not addressed. We use ABS scheme to achieve authenticity and privacy. Unlike our scheme is resistant to replay attacks, in which a user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. We, therefore, add this extra feature in our scheme and modify appropriately. Our scheme also allows writing multiple times which was not permitted in our earlier work.

ADVANTAGES OF PROPOSED SYSTEM:

- It provides authentication of users who store and modify their data on the cloud.
- It revoked users cannot access data after they have been revoked.
- Costs are comparable to the existing centralized approaches.

SYSTEM ARCHITECTURE:



Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

PROPOSED METHODOLOGY:

A. Distributed Key Policy Attribute Based Encryption:

KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed scheme consists of four algorithms which is defined as follows

Setup:

This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption:

It takes a message, public key and set of attributes. It outputs a cipher text.

Key Generation:

It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption:

It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

B. File Assured Deletion:

The policy of a file may be denied under the request bythe customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased.

To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption.

Conclusion:

Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle. We propose secure cloud storage using decentralized access control with anonymous authentication.

The files are associated with file access policies, that used to access the files placed on the cloud. We have introduced a decentralized access control system with anonymous authentication, which gives client renouncement also prevents replay attacks. The cloud does not know the identity of the client who saves data, however just checks the client's certifications. Key dissemination is carried out in a decentralized manner. One limit is that the cloud knows the access strategy for each one record saved in the cloud.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

References:

[1] Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, IEEE, Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,"Proc. IEEE INFOCOM, pp.441-445, 2010.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp.157-166, 2009.

[6] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/craig, 2009.

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp.417-429, 2010.

[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Frameworkfor Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc.15th Nat'l Computer Security Conf., 1992.

[11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81,June 2010.

[12] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Texture Enhancement Using fractional Brownian Motion Evaluation Method

Tanveer Begum
M.Tech,
Dept of CSE,
Shadan Women's College of Engineering and Technology,
Hyderabad.

Ms. Amena Sayeed
Assistant Professor,
Dept of CSE,
Shadan Women's College of Engineering and Technology,
Hyderabad.

Ms. Saleha Farha
HOD,
Dept of CSE,
Shadan Women's College of Engineering and Technology,
Hyderabad.

ABSTRACT:

Single image super resolution has attracted attention in recent years. Moving to texture enhancement it is still an ongoing challenge, even though considerable progress was made in recent years. More effort is devoted to enhancement of regular textures, but stochastic textures that are in natural images are posing difficulty. The objective of this method is to restore lost image details while acquisition. Based on fractional brownian motion (FBM) a texture model is used. This model is global in entire image and does not entail using patches present in image.

The FBM is stochastic process with properties like self-similarity and long range dependencies between pixels. Self similarity is used to characterize a wide range of natural textures. This model based on FBM is evaluated and regularized super resolution algorithm with only one image as input is derived. A wide range of textures and images can be enhanced by applying this algorithm. An algorithm which increases the further performance is proposed by changing the parameters involved in diffusion process. Finally by the help of quality assessment parameters like Structural similarity Index Matrix, Peak Signal To Noise Ratio, Correlation Coefficient quality of image evaluated with reference to the input image.

KEYWORDS:

Stochastic Texture, Super resolution, Fractional Brownian Motion.

INTRODUCTION:

Super Resolution of natural images has conquered great advancement where as coming to textures it's an ongoing challenge. Specifically stochastic texture enhancement provides the opportunity to recover lost details during acquisition time[1]. Traditional approaches often yield cartoon like images and even quality may be compromised. So an approach using Fractional Brownian Motion (FBM) for characterizing stochastic textures is proposed in this paper. This has wide range of applicability in Satellite Imaging and many other applications. In satellite imaging for any object identification and classification the image must be of more clarity. By super resolution it can be made easy. Super resolution concept has significant scope in medical imaging and also in forensic analysis. For textured images, State- of- art methods like example- based super resolution[9], sample patch algorithm etc mainly emphasizes edges but do not restore other textural missing details.

A.Texture and its types :

Texture is an important cue in human visual perception, texture processing has become more important in computer graphics, computer graphics, computer vision and image processing. . A texture is a measure of the variation of the surface intensity, and quantifying properties such as density, regularity. Image texture is defined as the function of the spatial variation in pixel intensities (gray values). In image processing texture is a bunch of metrics calculated and designed to quantify the perceived texture of image.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The spatial arrangement of colour or intensities in an image or selected region of an image is obtained by texture. Textures in general can be classified into two classes: Regular, or structured and stochastic[2]. The initial one is defined as spatially resembled parts of a single or several repetitive patterns. One example of regular texture is a brick wall. Stochastic textures don't contain a specific pattern and these textures are not modelled as same as regular textures. As conceptually and visually two textures are different enhancement techniques are also differed. Unlike regular textures, [3]stochastic textures are not characterized by repetitive patterns, instead defined by their statistical properties. This stochastic texture exhibits statistical properties such as non-local, long-range dependencies and self-similarity, as their pixel distribution remains the same across.Regular textures are enhanced by using methods of edge enhancement, in the stochastic texture such edges don't exist.

So by attempting to apply edge enhancement to such a texture , might in some cases create a stair casing effect, while smoothens out the clear details in the neighbourhood of the newly-created edge. Regular and stochastic texture enhancement is differed by a different approach called texture synthesis. Texture synthesis is a process where a patch is utilized to create a new image of bigger size and visually same as the original one. Even though such methods show similar results to the original visually, they are less effective in de convolution problems such as super resolution, in which the high resolution estimate has to represent the low resolution image. Further in case of stochastic textures such synthesis based on local-dependencies may fail to capture the every detail in the texture. Example based techniques combined with texture synthesis also exist for texture enhancement.

PROBLEM STATEMENT:

The theoretical framework and algorithms presented in this study are concerned with superresolution of fully textured images, wherein the texture incorporates both stochastic and structured elements. The superresolution paradigm considered here is the so-called single-image superresolution, where only one image is available as an input. Considering first the more challenging aspect of the granularity and non-stationarity of structures often encountered in natural textures, a stochastic texture model has been developed, based on fBm. PDE-based regularization has been introduced in order to capture anisotropic texture details, and a diffusion-based singleimage superresolution scheme was derived. As is the case in similar underdetermined problems, the emphasis is on side information, inherent in the underlying image model. The results obtained in our study, encourage the use of global fBm-based model (rather than patch-based) for natural textured images, as a method for reconstruction of degraded textures.

Drawbacks:

1)The empirical image, $Y\varphi(\eta_1, \eta_2)$, is initially derived from the degraded image, $Y(\eta_1, \eta_2)$. However, as the diffusion advances and the image is refined, it is beneficial to update $Y\varphi(\eta_1, \eta_2)$ as well. Due to the time consuming LS it entails, this is performed periodically after several iterations of the diffusion process.

2) The parameters of this algorithm are H, α, β and the number of diffusion iterations or stopping condition. H is estimated based on the degraded image itself . The other parameters have fixed values for all images. The diffusion process is completed when H(i), estimated in the ith iteration, is equal to H

PROBLEM DEFINITION:

The proposed model and concomitant algorithm are based on the empirical observation that stochastic textures are characterized by the property of self-similarity. An appropriate random process is estimated with reference to the existing lowresolution image. The initial restoration of missing details is based on an arbitrary realization of an fBm image. One may, therefore, expect different results for different evaluations. However, due to the phase matching and optimization, results for different random seeds yield almost identical results. In our current study, we attempt to remove the formal dependency on an initial arbitrary image, and obtain a model which depends on the fBm statistics.

The following form of the superresolution problem is considered: A high-resolution (HR) image is degraded by a blurring filter, representing, for example, the PSF of an optical sensor. It is subsequently subsampled.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Noise is then additively mixed with the blurred and subsampled image to create the available low-resolution (LR) image. Let X(η1, η2) and Y (η1, η2) denote the original (HR) image and observed (LR) noisy image, respectively. The imaging model can be represented as follows:

$$Y(\eta_1, \eta_2) = D((X \; b)(\eta_1, \eta_2)) + N(\eta_1, \eta_2),$$

The proposed model has been exploited for solving the SR problem. It can also be used for other image enhancement problems, such as denoising or in-painting. This is a challenge in the case of textures, due to the overlap in the frequency range with that of the noise, and due to the lack of local, small-scale, smoothness.

It should be emphasized that existing denoising algorithms usually succeed in restoring edges and smooth segments, but not in the recovery of fine details. Preliminary results show that the fBm, used as a prior in MAP estimation, can effectively act as a regularizer which performs denoising on fBm-based images.

IMPLEMENTATION:

Anisotropic Diffusion:

A brief review of the anisotropic diffusion that will suffice for our application is provided. This diffusion, although commonly referred to anisotropic, is in fact non-linear but isotropic. This has been noted by Weickert, who introduced a truly anisotropic diffusion process, commonly referred to as tensor diffusion: This formulation allows for different types of diffusion to be performed in different orientations within the image. In edge enhancing diffusion, for instance, only the diffusion coefficient perpendicular to the edge orientation will assume a significant value.

This method further emphasizes edges while smoothing noisy image areas. Instead of a single diffusivity function,two functions are used - one for each eigenvalue.Using PDE-based methods allows for adaptive filtering of an image, with low computational complexity. The following PDE equation suitable for image processing was introduced in this context by Perona and Malik :

$$It = \nabla \cdot (g(\nabla I) \nabla I),$$

Texture-Based Tensor Diffusion:

One cannot expect to represent a natural texture using a single parameter. Instead of using a general function, we use a structure function generated from the degraded image itself. This yields an image which contains the details of the degraded image, along with correlations introduced according to the specific structure of the non-stationary field. We refer to the structure function derived from the degraded image as the empirical structure function (ESF). The method to recover the ESF from a given, degraded, image is based on an inverse procedure to the method of obtaining the image from the structure function. Using the ESF, it is possible to obtain an image,from the degraded image, by calculating the autocorrelation of the first- and second-order increments, solving the LS problem is to obtain a structure function and using the synthesis algorithm. The resulting image is referred to as the empirical image.The method to recover the ESF from a given, degraded, image is based on an inverse procedure to the method of obtaining the image from the structure function, devised in [36]. Let Y (η1, η2) be a degraded image. The increments in the x = η1 and y = η2 orientations are defined as:

$$Y_{\eta 1}(\eta_1,\eta_2)=Y(\eta_1,\eta_2)-Y(\eta_1-\eta_1,\eta_2),$$
$$Y_{\eta 2}(\eta_1,\eta_2)=Y(\eta_1,\eta_2)-Y(\eta_1,\eta_2-\eta_2).$$

To obtain the empirical structure function, it is therefore required to invert the equations, and produce φ(η1, η2), given the increment autocorrelation functions of Y (η1, η2).
Substitutingη1= η2 = 1, it follows that the 1D autocorrelation functions can be represented usingconvolution equations with derivative filters:

$$R_{\eta 1}(\eta_1, \eta_2) = (\varphi \; fd)(\eta_1, \eta_2),$$
$$R_{\eta 2}(\eta_1, \eta_2) = (\varphi \; f^T \; d)(\eta_1, \eta_2),$$

Tensor Diffusion:-

We now consider the modifications required to enable the tensor diffusion to perform superresolution on natural textures. This allows for the introduction of missing texture details, while still emphasizing the edges of a degraded texture image.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

We now consider the modifications required to enable the tensor diffusion to perform superresolution on natural textures. The tensor, D(I), introduced earlier, is set instead to be D((It + αYφ(η1, η2))), where Yφ(η1, η2) is the empirical image, and α is a weight parameter. This allows for the introduction of missing texture details, while still emphasizing the edges of a degraded texture image.The superresolution algorithm is presented by considering the following energy functional, in column-stacked image representation:

E(X, X) = (B X – Y) 2 + (Xˆ H P – HH P X) 2 + β(| X + αYφ| 2)dxdy

STRUCTURAL SIMILARITY BASED IMAGE QUALITY ASSESSMENT:

Natural image signals are highly structured: Their pixels exhibit strong dependencies, especially when they are spatially proximate, and these dependencies carry important information about the structure of the objects in the visual scene. The Minkowski error metric is based on point wise signal differences, which are independent of the underlying signal structure. Although most quality measures based on error sensitivity decompose image signals using linear transformations, these do not remove the strong dependencies, as discussed in the previous section. The motivation of our new approach is to find a more direct way to compare the structures of the reference and the distorted signals.

SSIM Index:

For image quality assessment, it is useful to apply the SSIM index locally rather than globally. The structure similarity index matrix (SSIM) is a method for measuring the similarity between two images. The SSIM index is a full reference metric in other words, the measuring of image quality based on an initial uncompressed or distortion free image as reference. It is designed to improve on traditional methods like peak signal to noise ratio whish have proven to be inconsistent with human eye perception. SSIM considers image degradation as perceived change in structural information which is the idea that the pixels have strong inter dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. The SSIM index can be viewed as a quality measure of one of the images being compared, provided the other image is regarded as of perfect quality. It is an improved version of the universal image quality index proposed before. First, image statistical features are usually highly spatially non-stationary. Second, image distortions, which may or may not depend on the local image statistics, may also be space-variant. Third, at typical viewing distances, only a local area in the image can be perceived with high resolution by the human observer at one time instance And finally, localized quality measurement can provide a spatially varying quality map of the image, which delivers more information about the quality degradation of the image and may be useful in some applications.The PSNR block computes the peak signal to noise ratio between two images. This ratio is often used as a quality measurement between the original and a compressed image.The higher the PSNR, the better the quality of the compressed or reconstructed image.Image enhancement or improving the visual quality of a digital image can be subjective, saying that one method provides a better quality image. For this reason, it is necessary to establish quantitative / empirical measures to compare the effects of image enhancement algorithms on image quality. The higher the PSNR, the better degraded image and better, the reconstructed to match the original image and the better the reconstructed image. In general, a higher PSNR value should correlate to a higher quality image. However PSNR is a popular quality metric because its easy and fast to calculate.

Example-based super resolution:

Example based super resolution refers to learning LR/HR patch correspondence from known LR/HR image pairs in a database, which provides a good prior on the predicted HR patch for a given LR patch. This technique is not guaranteed to recover the actual high frequency details and may lead to ‘hallucination’. Limitations of classical-SR can be overcome using example-based SR. In example based SR, correspondence between HR/LR patches is learned from a database of LR/HR image pairs. A new LR image can be resolved at higher scale by using the LR/HR correspondence learned. However, since enough patch repetitions occur across scales of an image, we can use different scales of the given input LR image to learn HR/LR patch correspondence without any external database.

Volume No:1, Issue No:2 (July-2015)
ISSN No : 2454-4221 (Print)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

CONCLUSION:

In this paper Fractional Brownian Motion is applied to stochastic textures and natural images also. There by considering every detail of the image natural images can also be further enhanced effectively. The parameters involved in FBM are modified and there by the processing time is reduced and the number of iterations are reduced. So by this proposed super resolution algorithm performance can be increased. In the future work this method can be extended to anisotropic textures. Fractional Brownian Motion has been widely used as a model of image structure, it is in fact suitable for modelling natural textures, but it is not congrous with image structures comprised of the edges and contours. Future work is nonetheless encouraged for in an attempt expand the model to better model anisotropic textures also.

FUTHER SCOPE:

Further research is nonetheless called for in an attempt to expand the model to better model anisotropic textures as well, and to minimize thereby the need for regularization. Such a model may yield other enhancement algorithms suitable for a broader class of stochastic textures. Despite of the above goal, yet to be accomplished, the proposed PDE-based regularization is interesting and important on its own merits The empirical structure function is obtained via an ill-posed scheme, and better solutions for this problem may result in better understanding of textures and yield thereby better enhancement results.

REFERENCES:

[1] D. Glasner, S. Bagon, and M. Irani, "Super-resolution from a single image," in Proc. IEEE 12th Int. Conf. Comput. Vis., Sep. 2009, pp. 349–356.

[2] K. Kim and Y. Kwon, "Example-based learning for single-image super-resolution," in Proc. Pattern Recognition. Berlin, Germany: Springer-Verlag, 2008, pp. 456–465.

[3] L. C. Pickup, S. J. Roberts, and A. Zisserman, "A sampled texture prior for image super-resolution," in Proc. Adv. Neural Inf. Process. Syst., 2003, pp. 1587–1594.

[4] D. Datsenko and M. Elad, "Example-based single document image super-resolution: A global map approach with outlier rejection," Multidimensional Syst. Signal Process., vol. 18, no. 2–3, pp. 103–121, 2007.

[5] J. Yang, J. Wright, T. Huang, and Y. Ma, "Image super-resolution via sparse representation," IEEE Trans. Image Process., vol. 19, no. 11, pp. 2861–2873, May 2010.

[6] K. I. Kim, and Y. Kwon, "Single-image super-resolution using sparse regression and natural image prior," IEEE Trans. Pattern Anal. Mach. Intell., vol. 32, no. 6, pp. 1127–1133, Jun. 2010.

[7] B. Goldluecke and D. Cremers, "Superresolution texture maps for multiview reconstruction," in Proc. IEEE 12th Int. Conf. Comput. Vis., Sep. 2009, pp. 1677–1684.

[8] Y.-W. Tai, S. Liu, M. S. Brown, and S. Lin, "Super resolution using edge prior and single image detail synthesis," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jun. 2010, pp. 2400–2407.

[9] C. Damkat, "Single image super-resolution using self-examples and texture synthesis," Signal, Image Video Process., vol. 5, no. 3, pp. 343–352, Jan. 2011.

[10] J. Yang, J. Wright, Y. Ma, and T. Huang, "Image super-resolution as sparse representation of raw image patches," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2008, pp. 1–8.

[11] M. Welk, D. Theis, T. Brox, and J. Weickert, "PDE-based deconvolution with forward-backward diffusivities and diffusion tensors," Scale Space PDE Methods Comput. Vis., pp. 585–597, 2005.

[12] Y. Gousseau and J.-M. Morel, "Are natural images of bounded variation?" SIAM J. Math. Anal., vol. 33, no. 3, pp. 634–648, Jan. 2001.

[13] A. S. Carasso, "Singular integrals, image smoothness, and the recovery of texture in image deblurring," SIAM J. Appl. Math., vol. 64, no. 5, pp. 1749–1774, 2004.