2016-17

International Journal of Computer & Organization Trends (IJCOT) – Volume 7 Issue 5 – Sep to Oct 2017

A Comparative Study on Reversible Data Hiding in Encrypted Images using Various Frameworks

Sayeesh[#], Manjunath Kotari[&], Harish Kunder[$], Chanchal Antony[%]

#PG Scholar, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka,India *Professor & Head, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka,India

$Associate Professor, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka,India

%Senior Asst. Professor, Dept. of CSE, Alva's Institute of Engineering & Technology, Mijar, Moodbidri (D.K), Karnataka, India

Abstract

We need more security for data transmission in computer networks. Nowadays most popularly we store and manage variety of data in cloud server. We need to protect the privacy of the data that is stored in cloud server. Many robust message encryption methods have been developed to such methods. Reversible data hiding in encrypted images is form of steganography in which we hide data within images. In this paper, we compare vacating room after encryption (VRAE), reserving room before encryption (RRBE) and reversible image transformation (RIT) frameworks for reversible data hiding in encrypted images. In the framework VRAE, the cloud server embeds data by losslessly vacating room from the encrypted images by using the idea of compressing encrypted images. In the framework RRBE, the image owner first empties out room by using reversible data hiding method in the plain images. After that, the image is encrypted and outsourced to the cloud and the cloud server can freely embed data into the reserved room of the encrypted image. RIT-based framework allows the user to transform the content of original image into the content of another target image with the same size. The transformed image, which looks like the target image, is used as the encrypted image and is outsourced to the cloud.

Keywords: *Reversible data hiding (RDH), vacating room after encryption (VRAE), reserving room before encryption (RRBE), reversible image transformation (RIT), image encryption, privacy protection*

I. INTRODUCTION

Communication is one of the most important needs of human beings. For communication purpose, most of the people are using different devices like mobile phones, phones, laptops etc. Most of these devices use certain network to make the communication easier. Device level security can be ensured by using facilities like setting passwords, biometric authentication schemes etc. But while coming to the network level security the most important challenge that world faces today is to ensure data security. Data security basically means protection of data from unauthorized users or hackers and providing high-level security to prevent data modification. The area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features of data transfers over the internet, many techniques have been developed like steganography, digital watermarking and image cryptography.

The protection of these types of multimedia data can be done with the help of cryptographic techniques such as encryption and data hiding algorithms. While the encryption techniques convert plaintext content into unreadable ciphertext, the data-hiding techniques embed additional data into cover media by introducing slight modifications. In recent years, more attention is paid to reversible data hiding in images, since it maintains the excellent property that the recovered original cover image is lossless after embedded secret data is extracted. This important technique is widely used in military images, medical images and law forensics, where no distortion of original cover is allowed.

Data hiding techniques are required these days due to rapid development of internet. A large amount of data is transferred using internet. Data hiding is technique in which secret data is hidden in some cover media like image, audio, video files etc. Generally images are preferred cover media due to large transmission of images over internet. Two main types of data hiding techniques exist: Irreversible data hiding and Reversible data hiding. In case of irreversible data hiding at the extraction side only secret message is

International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244
Impact Factor: 6.111

CHARM: A Survey on Multi-Cloud Hosting for Performance and Cost-efficient in Cloud Computing

Mallikarjunaiah K M, (M.Tech) Dept. of CSE, AIET, Moodbidri

Harish Kunder, Assistant Professor, Dept. of CSE, AIET, Moodbidri

Abstract: ***Cloud computing is used to store data from various resources by the user. It is difficult for the user to store entire data within the system; therefore clouds are formed to store the user data. More enterprises and organizations are hosting their data into the cloud, in order to reduce the IT maintenance cost and enhance the data reliability. IT resources are rapidly and elastically provisioned and provided as standardized subscription to users over the internet in a flexible pricing model and effort by interacting with the service provider. Cost is also a major issue in cloud computing when we are switching to multi cloud. Based on comprehensive analysis of various state of the art cloud vendors, this paper proposes a novel data hosting scheme (CHARM) which integrates two key functions desired. The first is selecting several suitable clouds and an appropriate redundancy strategy to store data with minimized monetary cost and guaranteed availability. The second is triggering a transition process to re-distribute data according to the variations of data access pattern and pricing of clouds. While sending data to third party administrative control in cloud, it also becomes an issue in cloud related to security. The efficient dynamic collaboration of multiple clouds provide several potential benefits, such as high availability, scalability, fault tolerance and reduced infrastructural cost.***

Keywords: Multi-cloud, data hosting, cloud storage.

I. INTRODUCTION

Cloud computing gets its name as a metaphor for today's internet world. Cloud typically contains an outstanding pool of resources, which can be reallocated to different purposes within short span of frames. The process is typically automated and takes minute. Recent years have witnessed online data hosting services such as Amazon S3, Windows Azure, Google Cloud Storage, Aliyun OSS [1], and so forth. These services provide customers with reliable, scalable, and low-cost data hosting functionality. To accessed these cloud services security and reliability we are using different models like: i) Using single service provider. ii) Using multiple service providers. The weakness of single service provider is that it can be easily be hacked by intruders and if the service provider fails or down for some technical reasons than client will not at all access his/her data. The problem in multiple service provider models is to compromise the security because there is lack of security techniques. More and more enterprises and organizations are hosting all or part of their data into the cloud, in order to reduce the IT maintenance cost and enhance the data reliability [2], [3], [4]. For example, the United States Library of Congress had moved its digitized content to the cloud, followed by the New York Public Library and Biodiversity Heritage Library [5]. Now they only have to pay for exactly how much they have used.

In Cloud computing storing and sharing of data is been done via trusted third party. For a cloud to be secure, all of the participating entities must be secure. The highest level of the system's security is equal to the security level of the weakest entity. Therefore, in a cloud, the security of data does not solely depend on an individual's security measures. The neighbouring entities are also responsible to provide an opportunity to an attacker to tackle the user's defences. The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes whether it may be accidental or deliberate must be protected. For a cloud provider, such answers can point it in the right direction for improvements. For instance, a provider should pour more resources into optimizing table storage if the performance of its store lags behind competitors.

Multi-cloud data hosting has received wide attention from researchers, customers, and start-ups. The basic principle of multi-cloud (data hosting) is to distribute data across multiple clouds to gain enhanced redundancy and prevent the vendor lock-in risk, as shown in Figure 1. The "proxy" component plays a key role by redirecting requests from client applications and coordinating data distribution among multiple clouds. The potential prevalence of multi-cloud is illustrated in three folds. First, there have been a few researches conducted on multi-cloud.

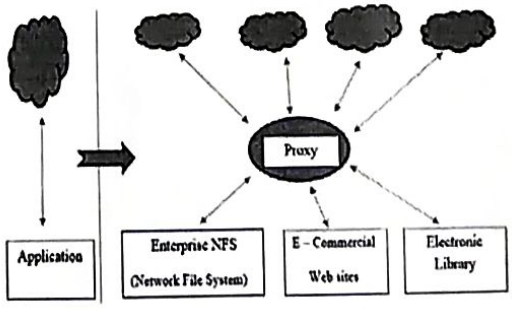

Figure 1: Basic principle of multi cloud data hosting

The proposed CHARM scheme. In this paper, we propose a novel cost-efficient data hosting scheme with high

Masking Selected Region of Moving Object using RGB Masking Technique

Shilpa
Dept. of CS&E
A.I.T, Chikkamagalur,
Karnataka, India.
shilpaygowda@gmail.com

Sunitha M.R
Dept. of CS&E
A.I.T, Chikkamagalur,
Karnataka, India.
sunithamr2310@gmail.com

Abstract

Moving object tracking and masking have become more inspiring and significant task in computer vision and surveillance application. Key step towards tracking is detection. The next and main step is tracking, which is the process of finding the path of the object across the video sequence. Masking is the novel approach in video analysis. Masking is the process of discerning the region of moving object which is not to be revealed. Masking of particular object can be used in various applications like media conversation, Traffic monitoring, video conferencing. In the proposed system background subtraction algorithm is used for detecting moving objects in video, which is the most widely used approach. Tracking is done by using mean-shift tracking technique, in which the target region is tracked. Finally in the masking phase the selected tracked frames are processed and RGB masking is applied to every frame. Experimental result shows that the proposed method masks the target region efficiently.

Keyword: Background subtraction, Mean-shift tracking, Masking.

I. *Introduction*

Video is a sequence of images. Each such images are referred to as frame in image processing field. Since more and more cameras are attached for security reason in sensitive areas like border, banks, colleges and streets surveillance of video is emerging as important task in research areas. Video surveillance is the technique of observing behaviour and other evidences mainly for human for protecting people. Surveillance is most commonly used by government for collecting the necessary information and investigates and prevents crime. Video surveillance are of three types most commonly used is semi-automatic video surveillance in which the video is analysed with the human interaction whenever necessary. In manual video surveillance system, video is analysed by the human only without system being involved. In Fully-autonomous system, video is analysed without the need for the human that is system itself performs every task. Object tracking and masking must deal with several illumination changes and occlusion condition. Intelligence Visual Surveillance comprises of scrutiny and analysis of objects activities, along with the object detection and tracking to diagnose the visual actions of the prospect. Video analysis is encompasses three basic stages: First and most important step is to detect the moving objects. Next is tracking the non-stationary objects from one frame to another and also to analyse the object tracks to recognize their performance. Tracking and masking the object in static environment is easier as there will be only little change in background. But in dynamic environment tracking and masking both becomes difficult as the background varies similar to foreground. In principle, to solve this general unconstrained problem is hard. One can put set of constraint to make this problem solvable. More the constraints, the problem is easier to solve.

The paper is organized as follows Section II illustrates literature review. Section III describes the proposed system. Section IV presents Performance analysis of the proposed system. Section V presents Conclusion about the paper.

II. Literature Review

M.Besita Augustin et al. offered a system in which the moving objects are precisely extracted by determining its motion, for supplementary dispensation. Precise moving objects are determined during background subtraction by averaging the scene illumination changes and color information of the non-stationary objects are used to accurately distinguish between objects [1].

Mahesh C. Pawaskar et al. proposed a method to detect the non-stationary substances established on the background subtraction method convolved with the 3x3 mask and some morphological operations like closing to denoise and to reserve the shape of the object. Convolution operation is applied to the binary image so that parallel architecture of embedded system will produce result very quickly [2].

S.Bhuvaneswari et al. developed a system in which the manually selected object is tracked in two steps. In first step object is identified using 64 bin color histogram matching. Then the distance between the object positions is determined by using the Euclidean distance among the selected region and tracked objects [3].

Pallavi M. Sune et al. designed a tracking algorithm which uses both texture and color histogram to represent the

978-1-5090-2399-8/16/$31.00 ©2016 IEEE

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Localized Encryption and Authentication Protocol for Secure Key Management in Wireless Sensor Networks

Arundhati Nelli [1], Sushant Mangasuli [2] Manasa N [3]

Assistant Professor, Dept. of CSE, Alva's Institute of Engineering and Technology, Mijar, Karnataka, India [1]

Assistant Professor, Dept. of CSE, Alva's Institute of Engineering and Technology, Mijar, Karnataka, India [2]

P.G Student (M. Tech.), Dept. of CSE, Alva's Institute of Engineering and Technology, Mijar, Karnataka, India [3]

ABSTRACT: Wireless Sensor Networks (WSNs) are spread widely and rapidly due its unique features, such as their light weight low-cost, and adhoc nature. However, this network is vulnerable to several attacks that affect its security. The security of WSN has very crucial issue nowadays in transmitting data over network. Due to the resource limitations of sensor nodes, providing security protocols is a particular challenge in sensor networks. A popular proposed method is Localized Encryption and Authentication Protocol (LEAP), is an efficient and light-weight protocol, but includes loopholes through which adversaries may launch replay attack by successfully masquerading as legitimate nodes and thereby compromise the communications over the network. LEAP supports the establishment of four types of keys. The security of these keys is under the assumption that the initial deployment phase is secure and the initial key is erased from sensor nodes after the initialization phase. However, the initial key is used again for node addition after the initialization phase whereas the new node can be compromised before erasing the key. A time based key management scheme rethought the security of LEAP. This paper gives brief description about strength and weaknesses of LEAP.

KEYWORDS: WSN, LEAP, Security, Key Management

I. INTRODUCTION

Wireless sensor networks (WSNs) are distributed systems consisting of a large number of sensor nodes and a base station as a controller which interface the sensor network to the outside network. WSNs may be deployed in unattended and adversarial environments such as battlefields. Compared to conventional networks, they are more vulnerable to physical destruction and man-made threats. Therefore, providing security is a particular challenge in sensor networks due to the resource limitations of sensor nodes, wireless communications and other related concerns. As a specific example, it is impractical to use asymmetric cryptosystems in sensor networks in which each node has low operational capability and insufficient memory. In a WSN , various types of communication may happen. The base station broadcasts control commands to the whole network. Control node multicasts messages within the cluster. A node communicates with its neighboring nodes by unicasting. Therefore, network-wide key, cluster key, and pairwise key are required to satisfy different types of secure communication. Therefore Adevised a scheme called localized encryption and authentication protocol (LEAP) for WSNs. LEAP (Localized Encryption and Authentication Protocol) is a protocol with key management scheme that is very efficient with its security mechanisms used for large scale distributed sensor networks. It generally supports for inside network processing such as data aggregation. In-network processing results in reduction of the energy consumption in network. To provide the confidentiality and authentication to the data packet, LEAP uses multiple keys mechanism. For each node four keys are used known as individual, pair wise, cluster and group key. All are symmetric keys and use as follows:

Individual Key: It is the unique key used for the communication between source node and the sink node.

Pairwise Key: It is shared with another sensor nodes.

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

www.ajcse.info

Asian Journal of Computer Science Engineering 2016; 1(2):29-34

REVIEW ARTICLE

Wireless Sensor Networks: An Overview on Security Issues and Challenges

***Arundhati Nelli[1], Sushant Mangasuli[2]**

[1,2] *Visvesvaraya Technological University BELGAUM*

Received on: 20/10/2016, Revised on: 14/11/2016, Accepted on: 01/12/2016

ABSTRACT

Wireless Sensor Networks (WSNs) are formed by deploying as large number of sensor nodes in an area for the surveillance of generally remote locations. A typical sensor node is made up of different components to perform the task of sensing, processing and transmitting data. WSNs are used for many applications in diverse forms from indoor deployment to outdoor deployment. The basic requirement of every application is to use the secured network. Providing security to the sensor network is a very challenging issue along with saving its energy. Many security threats may affect the functioning of these networks. WSNs must be secured to keep an attacker from hindering the delivery of sensor information and from forging sensor information as these networks are build for remote surveillance and unauthorized changes in the sensed data may lead to wrong information to the decision makers. This paper gives brief description about various security issues and security threats in WSNs.

Keywords: Sensor, Security, Threats, wireless, overview, Challenges.

INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors . The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Wireless Sensor Networks (WSNs) are the collectors of information from the physical world in the form of sensed data according to the requirement like temperature, pressure, humidity, level, movement etc. This data is available to the sink through gateway. Sensors are deployed in extensive numbers and on account of its wireless nature; it is easily works in any type of environment. Although sensor nodes are deployed in a random manner still it's important to deploy them carefully. Deploying few nodes may raise the issue of coverage and deploying too many nodes may result in an inefficient network because of more collision and interference. Wireless Sensor Networks (WSNs) need effective security mechanisms because these networks deployed in hostel unattended environments. Due to inherent limitations in wireless sensor networks, security is a crucial issue. While research in WSN security is progressing at tremendous pace, no comprehensive document lists the security issues and the threat models which pose unique threats to the wireless sensor networks.

We identify the security threats, review proposed security mechanisms for wireless sensor networks. Security in the Wireless Sensor Networks has various difficulties, some common are: dynamically changing topology, wireless communication among the sensor nodes, infrastructure-less framework, and limited physical resources like energy source, memory capacity and very low communication bandwidth . Numerous analysts proposed so many threats handling models and diverse security protocols for secure data communication and routing in WSN.

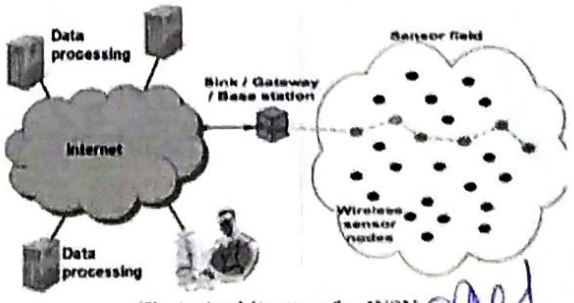

Fig 1: Architecture for WSN

***Corresponding Author:** Arundhati Nelli, **Email**: arundhati.nelli007@gmail.com

International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 6, June 2017 ISSN 2319 - 4847

Drifting Approach for Energy Consumption in Wireless- Sensor Networks

Dr. Mahesh.K.Kaluti[1], Mr. Vivek Sharma[2], Mr. Sudarshana K[3]

Associate Prof, Dept. of CSE[1], AIET, Moodbidri, VTU Belagavi

Assistant Prof Dept. of CSE[2], AIET, Moodbidri, VTU Belagavi

Associate Prof, Dept. of ISE[3], AIET, Moodbidri, VTU Belagavi

Abstract

The growing technologies and several issues concerned to the wireless sensor networks keeps the remarkable change in the existing technologies of wireless sensor networks and most of the concerned issues are related to the consumption of power and crucial part of the networks are mainly deal with properties like sensing, computing, and radio but this paper mainly concerned about the a novel sleep scheduling technique and virtual backbone Scheduling where traffic is only forwarded by backbone sensor nodes, and the rest of the sensor nodes turn off their radios to save energy. In this paper, the main focusing is concerned with two approaches in which first one is deal with rotation of multiple backbones which can makes sure that the energy consumption of all sensor nodes is balanced and fully utilized inside the network and second approach is the efficient routing with minimum energy consumption of nodes where each node in the network is equipped with a learning automaton to collectively learn the path of aggregation with minimum consumption energy for each node in the network where one can achieve the remarkable drift in energy consumption at very minute level of the network.

Keywords: Remarkable, Sensing, Rotation, Automaton, Drift

1. INTRODUCTION

In real time applications of the wireless sensor network it is necessary for the nodes to achieve two things the first one is Quality of Service as well as fault tolerance for the sensing In this concept, we are dealing with the novel sleep-scheduling technique called Virtual Backbone Scheduling[1]. Where actually VBS is designed for WSNs with redundant nodes, where VBS forms multiple overlapped backbones which work alternatively to prolong the network lifetime. As concerned to this approach traffic is only forwarded by backbone sensor nodes, and the rest of the sensor nodes turn off their radios to save energy. And the second approach is mainly concerned with efficient routing with minimum energy consumption of nodes where each node in the network is equipped with a learning automaton to collectively learn the path of aggregation with minimum consumption energy for each node in the network [2]. This concept is an adaptive decision-making unit situated in a random environment of the wireless sensor network that learns the optimal action through repeated interactions with its environment. The concept of automaton reads an input from its environment existing paths to forward the traffic and then it updates n (t) to n (t+1) after choosing a successor state according to the probabilities and outputs the corresponding to the particular action. Further the automaton's environment, in turn, reads the action and sends the next input to the automaton.

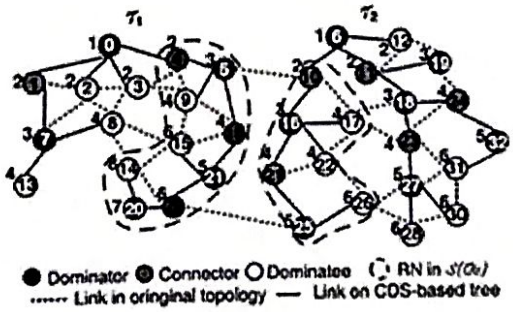

Figure 1: Link Stability in MANET

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

An Efficient Mining of Frequent Itemset Purchase on Retail Outlet using Frequent Itemset Ultrametric Tree on Hadoop

Manasa N[1], Venkatesh[2], Hemanth Kumar N P[3]

[1]*PG Student, Department of CSE, Alva's Institute Of Engineering and Technology, Moodbidri, DK, India*
[2]*Associate Professor, Department of CSE, Alva's Institute Of Engineering and Technology, Moodbidri, DK, India*
[3]*Assistant Professor, Department of CSE, Alva's Institute Of Engineering and Technology, Moodbidri, DK, India*

Abstract - *Mining frequent itemset purchase in a retail outlet is a very strenuous job. As extracting the frequently occurring itemsets over a large heterogeneous database is a core problem. Existing parallel mining algorithm for frequent itemsets does not support automatic parallelization, load balancing, synchronization and fault tolerance over a large cluster. Hence as a solution to these problem, an improvised algorithm called frequent itemset ultrametric tree algorithm using MapReduce programming model on Hadoop is used. Here in this technique, we implement three MapReduce jobs to perform the mining task.*

***Key Words*: Frequent Itemsets, Frequent Item ultrametric Tre(FIUT), Hadoop, MapReduce, Hadoop Distributed File System(HDFS).**

1. INTRODUCTION

Finding out the frequent Item-sets in large heterogeneous database is one of the core problem in data mining [1]. Existing data mining algorithm like Apriori [2] and FP-growth [3] algorithm fails to extract frequent item-sets when size of transactional database is too large to compute. Also these traditional mining algorithms were running only on single machine which results in performance deterioration

Apriori is a bottom-up, breadth-first search algorithm. It uses hash trees to store frequent itemsets and candidate frequent itemsets. This classic Apriori- like parallel FIM algorithm uses generate and test process that generates a large number of candidate itemsets. The major disadvantage of Apriori-like FIM algorithm is that the processor has to repeatedly scan the entire database. To reduce the time taken for scanning entire database multiple times, an approach called FP-growth algorithm was introduced. Though FP-growth algorithm addresses the scalability problem it fails to construct in-memory FP trees to accommodate large-scale database. Hence rather than considering Apriori and FP-growth algorithm we incorporate a new frequent itemset mining algorithm called Frequent itemset ultrametric tree(FIU-tree) [4]. This FIUT algorithm is mainly used because of its advantageous features like, reduced i/o overhead, natural way of partitioning a dataset, compressed storage and avoids recursive traverse. Most importantly it enables automatic parallelization, load balancing, data distribution and fault tolerance over a large cluster. This FIUT algorithm is designed over MapReduce programming model [5]. Hence FIUT on Hadoop has got many distinctive features.

The MapReduce framework on Hadoop [6] enables distributed processing of huge data on large clusters, provided with good scalability, robust and fault tolerance. FIUT running on this framework is described by two major functions map and reduce. The mapper independently and concurrently decompose itemsets and on otherhand reducer function aggregates all the values by constructing small ultrametric trees as well as mining these trees in parallel. Industries utilize these extracted frequent itemsets in decision making about the products. If a retail sector company wants to know about the customer nature, their buying habits and about the product which is on demand this FIUT mining technique on Hadoop helps them to do so in very efficient way, in turn it increases their profit indeed. [7].

2. BACKGROUND STUDY

Hadoop is an open source software framework used for distributed storage and to develop data processing applications which are executed on those distributed computing environment where huge data sets are distributed across nodes in a cluster. Their main characteristic is to partition the data and computes it over large cluster of nodes. Hadoop includes various components such as Hadoop Distributed File System (HDFS), MapReduce, Hbase, HCatalog, Pig, Hive, Oozie, ZooKeeper, Kafka, and Mahout [5]. HDFS has become a key tool for managing pools of huge data and supports big data analytics application.

2.1 Hadoop Distributed File System

The Hadoop Distributed File System (HDFS) is designed for storing very large files with streaming data access patterns running on clusters of commodity hardware. Hadoop Distributed File System stores data to provide high aggregate I/O bandwidth [8]. HDFS stores filesystem metadata and application data separately where metadata is stored on a dedicated server called Namenode and application data are stored on other servers called DataNodes.

RnSIR:A New model of Information Spread in Online Social Networks

Sumith N
Dept. of CSE
NITK, Surathkal, India.
s.nireshwalya@gmail.com

Annappa B
Dept. of CSE
NITK, Surathkal, India.
annappa@ieee.org

Swapan Bhattacharya
Dept. of CSE
Jadavpur University, Kolkata, India.
bswapan2000@yahoo.co.in.

***Abstract*—There is a close resemblance between the dynamism of epidemic spread and information spread. For this reason, the *Susceptible-Infected-Recovered(SIR)* model, rooted in epidemiology, is been used to understand the information spread in online social networks. This model is based on homogeneous mixing of population, where an individual is equally likely to be infected by others. However, the degree of sparsity in interactions among the users will invalidate the homogeneous mixing concept. For this reason, SIR model fails to map the complete scenario of information spread among the users. In this paper, to fill in the gap seen in SIR, a new model R_nSIR is developed. The proposed model is able to make a clear distinction between the restrained and susceptible. To this end, the new model is applied to viral marketing to understand its authenticity. The contribution is shown by the increase in spread of information reaching as far as 50% of the susceptible population in the R_nSIR model, when compared to the SIR model. Although the paper discusses the dynamism of information spread in online social networks, the proposed model can be used to understand the spread of epidemics, spread of computer virus, rumors and also analyze the role of users.**

I. Introduction

The constant threat of new epidemic infections, make it important to understand and predict the dynamics of the spread of an infection. For obtaining such understanding, mathematical models and their analysis play an important role. One of the simplest model used to capture the dynamics of epidemic spread is the SIR[5] model. This model describes how eventually entire population is infected[1] by the virus. Due to close resemblance of epidemic spread with information spread in online social networks, the SIR model is readily adopted to understand the information spread process. The spread of information helps in spread of trends, adoption of innovation, product promotion and is used in applications such as recommendation systems and viral marketing.

This paper discusses the benefit of effective spread of information in the context of viral marketing application. Viral marketing is a popular application that is weaved to take utmost benefit the online social network is offering. Specifically, it involves fetching few initiators in the online social networks such that, they cause a vast and rapid product sale by word-of-mouth approach. To this end, the SIR model is used to understand how a user gets influenced by an information and propagates it. The SIR model is based on the assumption of *homogeneous mixing*, i.e.,the entire population eventually gets influenced by the information. However, in the real world users maintain contacts with few of the friends, thus invalidating the *homogeneous mixing* assumption. To this end, the *SIR* fails to model the real world dynamics of information spread.

A. Contributions

In this paper, Restrained-Susceptible-Infected-Recovered (R_nSIR) model is proposed to close the gap between the real world and theoretical assumption of SIR model. Thus, the proposed model will help in better understanding of the information spread process and the role of users.The contributions are:

1) The proposed R_nSIR model includes the restrained phase of users in information spread process
2) The proposed model better represents the role of users in the online social network.
3) Improve in percentage of spread of information.

II. Related work

The seminal work on spread of epidemic diseases is formalized by Mc Kendrick and Kenmrack[5] through the SIR. Since then, various contributions to SIR are seen in epidemiology[3],[7],[9],[10]. Also, the Susceptible -Infected-Susceptible(SIS)[8],[12] model is an alternative representation of epidemic spread which deals with persistence of infection in scale free networks[1] such as online social networks. The *SIS* model takes into consideration that a recovered person is susceptible to the same type of infections in future. However, the direct applicability of this model is inappropriate in online social networks. A person is not interested in an information that he/she had received in the past. For example in context of marketing a product, an enterprise mails sale campaigns to user. A user will receive this information and also act on it, by either purchasing or promoting the sale. However, the second time when the same sale campaign is received, the user may not respond. As such, *SIS* model fails in this context in modeling the online social network information

[1]The words infected and influenced is used in the same sense; first in the context of spread of infection and later in the context of information

978-1-5090-2597-8/16/$31.00 ©2016 IEEE

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 6 – No.1, October 2016 – www.caeaccess.org

Security and Privacy Preservation on Cloud-based Big Data Analysis (CBDA): A Review

Hemanth Kumar N. P.
Assistant Professor
Department of CS&E
AIET, Moodbidri, India

Prabhudeva S.
HOD,
Dept. of ISE, JNNCE, Shivamogga, India

ABSTRACT
The term Big Data is nothing but large voluminous data, more complex data and relationship analysis of these data sets. The today's organizations, business units, government sectors, etc. are adopting the big data technique to store the enormous data generated by them. With all the significances of the big data as per economic and social benefits, lacks with many issues related to the security and privacy of the data. The modern ethnology like cloud computing will offer a scalable service for the big data with optimized cost. But the concern of privacy and security is still unsolved. This paper reflects the survey over the cloud-based big data security and privacy preservation. The survey discusses the recent work carried for privacy preservation and also existing research gap. The survey states a significant section for the future research line-up.

Keywords
Big data, Cloud Computing, Privacy and security issues

1. INTRODUCTION
The term big data is nothing but large voluminous data, more complex data and relationship analysis of these data sets. The main advantage of big data is that it performs the better analysis of huge data than conventional analysis methods. Due to this reason the big data has gained very much interest in the present generation, which has advancement in the data collection, data storage and performs the data interpretation. From last few decades, the use of digital media is been increased in many areas which generating the tremendous amount of data, for example, hospital data, bank data, social networking data, etc. The data storage cost is decreasing day by day by which we can store the entire data rather than discarding it. In addition to this, many of the data analyzing techniques are developed and have not succeeded for efficient data analysis. The cloud computing is the recent technique which offers many significant advancements in the research work of the big data analysis. In this way, cloud arranges enormous data that contain sensitive information and are required to send particular measures and various leveled shields to keep up a key separation from data confirmation breakdowns that may achieve tremendous and extravagant damages. Critical information as to disseminate figuring incorporates data from a broad assortment of different locales and requests. Over the time, affiliations have assembled noteworthy information about the general population in our social requests that contain tricky information, e.g. therapeutic data. Researchers need to get to and analyze such data using huge data propels as a piece of circulated processing, while affiliations are required to actualize data security consistence. There has been huge progression on privacy protection for fragile data in both industry and the informed group, e.g., plans that make traditions and mechanical assemblies for anonymization or encryption of data for security purposes. This portion sorts business identified with this area according to assorted security protection necessities. Regardless, these courses of action have not yet been for the most part gotten by cloud organization suppliers or affiliations. Like this, with the extension of these new cloud headways recently, security and data protection requirements have been creating to guarantee individuals against surveillance and database exposure.

Cloud computing has raised several security threats such as, malicious insiders, data loss, data breaches, and denial of service that have been extensively studied. These threats mainly originate from issues such as multi-tenancy, loss of control over data and trust. This means that there are important concerns about security and privacy need to be focused on cloud computing by all parties involved in the cloud computing arena.

This paper discusses some significant aspects of the big data over cloud computing with the privacy and security issues. The most significant and latest existing work towards the privacy and security solution in cloud-based big data analysis (CBDA) is discussed and finalized with the future level of the work required in the CBDA privacy and security solution. The section wise representation of this survey paper is provided as Section 2 followed with the big data concepts and security and privacy issues; Section 3 represents the cloud computing concepts and privacy & security issues in it, methods used for cloud-based big data analysis. Section 4 talks about the existing research work are CBDA and privacy & security preservation. Section 5 figure out the research gap in existing research gap. Section 6 suggests the future research lineup and the conclusion are given in section 7.

2. BIG DATA
The term big data is nothing but large voluminous data, more complex data and relationship analysis of these data sets. The main advantage of big data is that it performs the better analysis of huge data than conventional analysis methods. Due to this reason the big data has gained very much interest in the present generation, which has advancement in the data collection, data storage and performs the data interpretation. From last few decades, the use of digital media is being increased in many areas which generating the tremendous amount of data, for example, hospital data, bank data, social networking data, etc. The data storage cost is decreasing day by day by which we can store the entire data rather than discarding it. In addition to this, many of the data analyzing techniques are developed and have not succeeded in efficient data analysis.

The big data in the real world is like the collection of huge resources which can be used regularly. The big data provides the vast application advantages, but the conventional data analysis methods fail to provide the proper privacy mechanism. The privacy concern of the big data includes the private data disclosure to the world.

International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244
Impact Factor: 6.111

Novel Authorized Accessible Privacy Model in Distributed m-Healthcare Cloud Computing System

Geetha S, PG Student, Dept of Computer Science and Engg, Alvas Institute of Engineering and Technology, Moodbidri

Manjunath Kotari, Senior Associate Professor & Head of Department CSE, Alvas Institute of Engineering and Technology, Moodbidri

Abstract: ***Distributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem, in this paper, a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Finally, the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.***

Keywords: ***Authentication, access control, security and privacy, distributed cloud computing, m-healthcare system***

I. INTRODUCTION

DISTRIBUTED m-healthcare cloud computing systems have been increasingly adopted worldwide including the European Commission activities, the US Health Insurance Portability and Accountability Act (HIPAA) and many other governments for efficient and high-quality medical treatment. In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering. As to the security facet, one of the main issues is access control of patients' personal health information, namely it is only the authorized physicians or institutions that can recover the patients' personal health information during the data sharing in the distributed m-healthcare cloud computing system. In practice, most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. Therefore, in distributed m-healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physicians their personal health information should be shared with have become two intractable problems demanding urgent solutions. There have emerged various research results focusing on them. A fine-grained distributed data access control scheme is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control method provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient-centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing. However, it mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system. Moreover, it is not enough for to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients' data confidentiality and identity privacy in the distributed m-healthcare cloud computing scenario under the malicious model was left untouched.

In this paper, we consider simultaneously achieving data confidentiality and identity privacy with high efficiency. As is described in Fig. 1, in distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's