Survey of Challenges in Encrypted Data Storage in Cloud Computing and Big Data

Manibharathi R
Senior Developer, Shiro Software Solutions, Nagercoil.

Dr.K.Selva kumar
Assistant Professor, Department of Mathematics, University College of Engineering, Nagercoil

Dinesh R
Project Manager, Shiro Software Solutions, Nagercoil.

Abstract - Cloud Computing and Big Data is an ever evolving field of technology. In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The rise of big data cloud computing and cloud data stores have been a precursor and facilitator to the emergence of big data. Cloud computing is the commodification of computing time and data storage by means of standardized technologies. Big data applications are a great benefit to organizations, business, companies and many large scale and small scale industries. Cloud computing plays a very vital role in protecting data. The cloud offers a variety of services. It reduces the complexity of the networks, makes provision for customization, scalability, efficiency etc. Besides, the information stored on cloud is generally not easily lost. Data stored on cloud is easily susceptible to leak by hackers. In order to prevent this, data is encrypted using Symmetric Searchable Encryption. In such a case, search over the encrypted data becomes difficult and can be executed using various keyword searches as Single Keyword Search, Multi-keyword Search, Fuzzy Keyword Search, Conjunctive Keyword Search, Similarity Search and Synonym Search. In this survey, we study, what are the challenges occurred in encrypted data storage in cloud computing and big data.

Index Terms – Cloud Computing, Data Retrieval, Big Data.

1. INTRODUCTION

Cloud computing is a large-scale distributed computing paradigm driven by reconfigurable computing resources can be rapidly provisioned and released with minimal management effort in the data centers. Increasing the outsourcing data user continuously presented sensitive information like government records, personal health records and photos etc., So data privacy and data loss will be increase. When users outsource their private onto cloud, the cloud service provider able to monitor the communication between the users and cloud at will trust or untrusted[1]. The cloud server leaks the data information to unauthorized users or even be hacked. To assure the secrecy, users usually encrypting the data before Outsourcing it onto cloud; it brings the adult challenges to effective data utilization. Even day by day stored data density is grown automatically. Big data is currently a major topic across a number of fields, including management and marketing, scientific research, national security, government sector and open data. Both public and private sectors are making increasing use of big data analytics. The word big data refers to the large amounts of digital information companies and governments collect about us and our surrounding environments. Every day, we create 2.5 quintillion bytes of data so much that 90% of the data in the world today has been created in the last two years alone. And remaining 10% of the data has been created when those data storage systems is generated. In present world there are many data generalization factors or data resources those are sensors, CCTV cameras, social networks like Facebook, what's app, Gmail and many more. Online shopping's, airlines, hospitalists data from all these resources huge amount of data is being generated day by day, to handle these huge amount of data the big data is introduced.

Data encryption has been widely used for data privacy preservation in data sharing scenarios, it refers to mathematical calculation and algorithmic scheme that transform plaintext into cyphertext, which is a non-readable form to unauthorized parties. A variety of data encryption models have been proposed and they are used to encrypt the data before outsourcing to the cloud servers. However, applying these approaches for data encryption usually cause tremendous cost in terms of data utility, which makes traditional data processing methods that are designed for plaintext data no longer work well over encrypted data.

Driven by the abundant benefits brought by the cloud computing such as cost saving, quick deployment, flexible resource configuration, etc., more and more enterprises and individual users are taking into account migrating their private data and native applications to the cloud server. A matter of

public concern is how to guarantee the security of data that is outsourced to a remote cloud server and breaks away from the direct control of data owners. Encryption on private data before outsourcing is an effective measure to protect data confidentiality. However, encrypted data make effective data retrieval a very challenging task.

2. IMPORTANCE OF CLOUD COMPUTING

Cloud Computing is transforming the way organizations consume computer services. Where in the past you had to have local systems and servers to run various applications, in the cloud they are managed by an external provider that charges you for the use.

With cloud computing, you pay for your usage just like you pay for electricity. Power is something you just plug into the wall; you turn a switch on and off and you get charged for the amount you use. You don't have to worry about where the power station is, or maintaining the power station or anything like that. All you care about is consuming the service. The concept is the same with cloud computing[2]. It takes the focus away from having to manage, maintain and support all of the local servers and whatnot. The cloud moves all of that into a hosted environment whereby you have someone else managing it. Now all you do is consume the service via a web browser, and someone else handles all the backend process, and all the servers, configuration and maintenance.

Cloud computing is effectively just taking stuff that was traditionally done onsite and moving it to a hosted environment with a structure around it that allows people to consume the servers on a usage basis. The technology behind cloud computing is really just about allowing people to access information on their computers via a remote data centre or from a hosting environment somewhere else.

Why Cloud Computing is Important:

Cost savings. In the past, it's been quite expensive to run, manage and deploy local systems; it has also taken a lot of capital. Most cases involve very technical people that you have to compensate with a lot of money to maintain all the stuff for you. Since you no longer need to run, manage and deploy the systems, there are big cost savings to be had.

Scalability. Cloud computing means you no longer need to worry about having to upgrade systems since it's all hosted elsewhere. You literally just need to make a phone call or click a button to increase your server capacity. If you acquire a company tomorrow and they have 50 staff, the cloud gives you unlimited elastic scale so you can add those 50 users and get them up and running straight away.

Keep up with the latest technology. With cloud computing, you never have to worry about upgrading and updating. The cloud makes sure you are getting the latest servers and are always upgraded with the next version. When a new patch comes out, it is automatically deployed, so you don't have to worry about any of that technical stuff anymore. Cloud computing keeps you on the cutting edge with the most up-to-date technology.

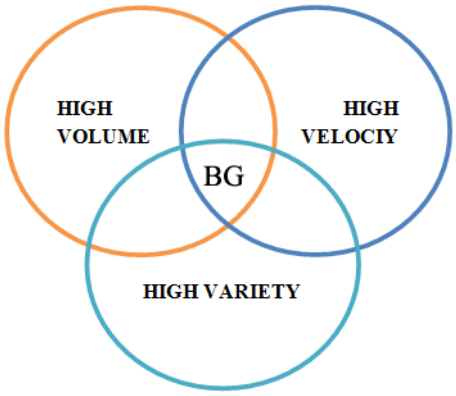
Mobility. Since the cloud is hosted, you are no longer confined to the office. You can take your information mobile and work from tablets and mobile devices. Staff can work from an office computer, from home, or from a client site. The cloud increases the efficiency of an organisation by giving staff more mobility. They can be on site with a client and still enter notes directly into sales reports.

Disaster recovery. Improved up-time is the result of better disaster recovering in the cloud. Your cloud hosting can take advantage of the best enterprise systems; in the event of server failure, it automatically fails over to another server. This is something that you definitely cannot achieve inside a small organisational IT environment, because to implement that sort of disaster recovery would be costly and capital intensive.

3. IMPORTANCE OF BIG DATA

There is no doubt that the industries are going ablaze with the huge eruption of data. None of the sectors have remained untouched of this drastic change in a decade[2]. Technology has crept inside each business arena and hence, it has become an essential part of every processing unit. Talking about IT industry specifically, software and automation are the bare essential terms and are used in each and every phase of a process cycle.

Businesses are focusing more on agility and innovation rather than stability and adopting the big data technologies help the companies achieve that in no time. Big data analytics has not only allowed the firms to stay updated with the changing dynamics but has also let them predict the future trends giving a competitive edge[5]. *Big Data is the combination of these three factors; High-volume, High-Volacity and High-Variety*



Big Data Combination

Volume

Big Data observes and tracks what happens from various sources which include business transactions, social media and information from machine-to-machine or sensor data. This creates large volumes of data.

Velocity

The data streams in high speed and must be dealt with timely. The processing of data that is, analysis of streamed data to produce near or real time results is also fast.

Variety

Data comes in all formats that may be structured, numeric inthe traditional database or the unstructured text documents, video, audio, email, stock ticker data.

Why Big Data is Important

Big Data is Timely – 60% of each workday, knowledge workers spend attempting to find and manage data.

Big Data is Accessible – Half of senior executives report that accessing the right data is difficult.

Big Data is Holistic – Information is currently kept in silos within the organization. Marketing data, for example, might be found in web analytics, mobile analytics, social analytics, CRMs, A/B Testing tools, email marketing systems, and more each with focus on its silo.

Big Data is Trustworthy – 29% of companies measure the monetary cost of poor data quality. Things as simple as monitoring multiple systems for customer contact information updates can save millions of dollars.

Big Data is Relevant – 43% of companies are dissatisfied with their tools ability to filter out irrelevant data. Something as simple as filtering customers from your web analytics can provide a ton of insight into your acquisition efforts.

Big Data is Secure – The average data security breach costs $214 per customer. The secure infrastructures being built by big data hosting and technology partners can save the average company 1.6% of annual revenues.

Big Data is Authoritive – 80% of organizations struggle with multiple versions of the truth depending on the source of their data. By combining multiple, vetted sources, more companies can produce highly accurate intelligence sources.

Big Data is Actionable – Outdated or bad data results in 46% of companies making bad decisions that can cost billions.

4. CHALLENGES IN CLOUD COMPUTING

Concern about security and privacy in the cloud will drive adoption of cloud encryption systems, but cloud providers warn there are six secu
22%. However, security and privacy are still cited by many organisations as the top inhibitors of cloud services adoption, which has led to the introduction of cloud encryption systems in the past 18 months. While encryption is important to the secure adoption of cloud services, it should not be viewed as the "silver bullet", warns Gartner in a recent research note. Analysts recommend that enterprises should first develop a data security plan that addresses six security issues. Failure to do so, they say, could add cost and complexity to the adoption of cloud computing without addressing the fundamental issues of data privacy and long-term security and resiliency. They warn that badly implemented encryption systems may also even interfere with the normal functioning of some cloud-based services.

Breach notification and data residency

Not all data requires equal protection, so businesses should categorise data intended for cloud storage and identify any compliance requirements in relation to data breach notification or if data may not be stored in other jurisdictions.

"Silver bullet", Gartner also[5] recommends that enterprises should put in place an enterprise data security plan that sets out the business process for managing access requests from government law enforcement authorities. The plan should take stakeholders into account, such as legal, contract, business units, security and IT.

Data management at rest

Businesses should ask specific questions to determine the cloud service provider's (CSP's) data storage life cycle and security policy.

Businesses should find out if:

- Multitenant storage is being used, and if it is, find out what separation mechanism is being used between tenants.
- Mechanisms such as tagging are used to prevent data being replicated to specific countries or regions.
- Storage used for archive and backup is encrypted and if the key management strategy includes a strong identity and access management policy to restrict access within certain jurisdictions.

Data protection in motion

As a minimum requirement, Gartner recommends that businesses ensure that the CSP will support secure communication protocols such as SSL/TLS for browser access or VPN-based connections for system access for protected access to their services.

The research note says that businesses always encrypt sensitive data in motion to the cloud, but if data is unencrypted while in use or storage, it will be incumbent on the enterprise to mitigate against data breaches.

In IaaS, Gartner recommends that businesses favour CSPs that provide network separation among tenants, so that one tenant cannot see another's network traffic.

Encryption key management

Enterprises should always aim to manage the encryption keys, but if they are managed by a

cloud encryption provider, Gartner says they must ensure access management controls are in place that will satisfy breach notification requirements and data residency.

If keys are managed by the CSP, then businesses should require hardware-based key management systems within a tightly defined and managed set of key management processes.

When keys are managed or available in the cloud, Gartner says it is imperative that the vendor provides tight control and monitoring of potential snapshots of live workloads to prevent the risk of analyzing the memory contents to obtain the key.

Access controls

"Silver Bullet" Gartner recommends that businesses require the CSP to support IP subnet access restriction policies so that enterprises can restrict end-user access from known ranges of IP addresses and devices.

The enterprise should demand that the encryption provider offer adequate user access and administrative controls, stronger authentication alternatives such as two-factor authentication, management of access permissions, and separation of administrative duties such as security, network and maintenance.

Businesses should also require:

Logging of all user and administrator access to cloud resources, and provide these logs to the enterprise in a format suitable for log management or security information and event management systems.

The CSP to restrict access to sensitive system management tools that might "snapshot" a live workload, perform data migration, or back up and recover data.

That images captured by migration or snapshotting tools are treated with the same security as other sensitive enterprise data.

Longterm resiliency the encryption system

Gartner recommends that businesses understand the impact on applications and database indexing, searching and sorting. They should pay specific attention to advanced searching capabilities, such as substring matching functions and wildcarding such as "contains" or "ends with".

If the encryption vendor offers options for "function preserving encryption" — for example, to preserve sort — regulations may require the use of standardised and approved algorithms or proof of independent certification for the potentially weakened encryption.

5. CHALLENGES IN BIG DATA

With the proliferation of devices connected to the Internet and connected to each other, the volume of data collected[6], stored, and processed is increasing everyday, which also brings new challenges in terms of the information security. In fact, the currently used security mechanisms such as firewalls and DMZs cannot be used in the Big Data infrastructure because the security mechanisms should be stretched out of the perimeter of the organization's network to fulfill the user/data mobility requirements and the policies of BYOD (Bring Your Own Device). Considering these new scenarios, the pertinent question is what security and privacy policies and technologies are more adequate to fulfill the current top Big Data privacy and security demands (Cloud Security Alliance, 2013). These challenges may be organized into four Big Data aspects such as infrastructure security (e.g. secure distributed computations using MapReduce), data privacy (e.g. data mining that preserves privacy/granular access), data management (e.g. secure data provenance and storage) and, integrity and reactive security (e.g. real time monitoring of anomalies and attacks).

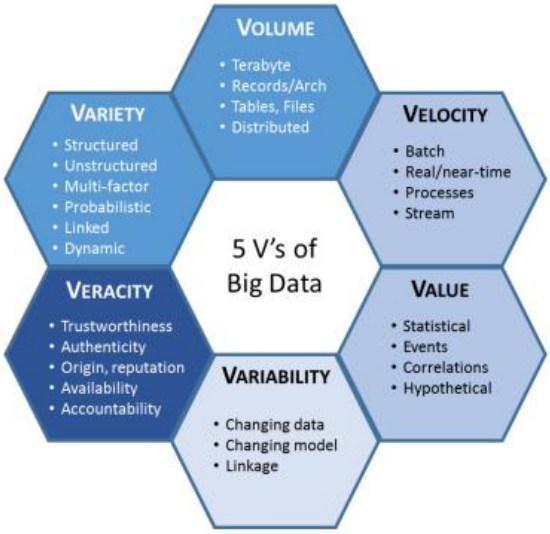


Figure 2 The Five V's of Big Data

Considering Big Data there is a set of risk areas that need to be considered. These include the information lifecycle (provenance, ownership and classification of data), the data creation and collection process, and the lack of security procedures. Ultimately, the Big Data security objectives are

no different from any other data types – to preserve its confidentiality, integrity and availability.

Being Big Data such an important and complex topic, it is almost natural that immense security and privacy challenges will arise (Michael & Miller, 2013; Tankard, 2012). Big Data has specific characteristics that affect information security: variety, volume, velocity, value, variability, and veracity (Figure 2). These challenges have a direct impact on the design of security solutions that are required to tackle all these characteristics and requirements (Demchenko, Ngo, Laat, Membrey, & Gordijenko, 2014). Currently, such out of the box security solution does not exist.

Cloud Secure Alliance (CSA), a non-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, has created a Big Data Working Group that has focused on the major challenges to implement secure Big Data services (Cloud Security Alliance, 2013). CSA has categorized the different security and privacy challenges into four different aspects of the Big Data ecosystem. These aspects are Infrastructure Security, Data Privacy, Data Management and, Integrity and Reactive Security. Each of these aspects faces the following security challenges, according to CSA:

Infrastructure Security

- Secure Distributed Processing of Data
- Security Best Actions for Non-Relational Data-Bases

Data Privacy

- Data Analysis through Data Mining Preserving Data Privacy
- Cryptographic Solutions for Data Security
- Granular Access Control

Data Management and Integrity

- Secure Data Storage and Transaction Logs
- Granular Audits
- Data Provenance

Reactive Security

- End-to-End Filtering & Validation
- Supervising the Security Level in Real-Time

6. BIG DATA AND CLOUD

Big data architecture supports high velocity data capture, storage and analysis. Big data requires huge amount of storage. Data in Big data may be in unstructured format, without standard formatting, and data sources can be beyond the traditional corporate database. Storing small and medium sized business organization's data in cloud as Big Data is a better option for data analysis work. An in-house storage model used to store Big Data in Network-Attached Storage (NAS). The architecture of NAS constitutes several computers attached to each other. Clustered storage is not feasible for small and medium size business.

The Encrypted Big Data stored in cloud can be analyzed using a programming methodology called MapReduce in which query is passed and data are fetched. The extracted query results are then reduced to the data set relevant to query. This query processing is simultaneously done using NAS devices. Though MapReduce algorithm usage in Big Data is well appreciated by many researchers as it is schema free and index free, it requires parsing of each record at reading point. This is the biggest disadvantage of MapReduce algorithm usage for query processing in cloud computing.

Business regard big data as a valuable business opportunity. As such, several new companies such as Cloudera, Hortonworks, Teradata and many others, have started to focus on delivering Big Data as a Service (BDaaS) or DataBase as a Service (DBaaS). Companies such as Google, IBM, Amazon and Microsoft also provide ways for consumers to consume big data on demand. Next, we present two examples, Nokia and RedBus, which discuss the successful use of big data within cloud environments.

Nokia

Nokia was one of the first companies to understand the advantage of big data in cloud environments (Cloudera, 2012). Several years ago, the company used individual DBMSs to accommodate each application requirement. However, realizing the advantages of integrating data into one application, the company decided to migrate to Hadoop-based systems, integrating data within the same domain, leveraging the use of analytics algorithms to get proper insights over its clients. As Hadoop uses commodity hardware, the cost per terabyte of storage was cheaper than a traditional RDBMS (Cloudera, 2012).

Since Cloudera Distributed Hadoop (CDH) bundles the most popular open source projects in the Apache Hadoop stack into a single, integrated package, with stable and reliable releases, it embodies a great opportunity for implementing Hadoop infrastructures and transferring IT and technical concerns onto the vendors' specialized teams. Nokia regarded Big Data as a Service (BDaaS) as an advantage and trusted Cloudera to deploy a Hadoop environment that copes with its requirements in a short time frame. Hadoop, and in particular CDH, strongly helped Nokia to fulfil their needs (Cloudera,2012).

Redbus

RedBus is the largest company in India specialized in online bus ticket and hotel booking. This company wanted to

implement a powerful data analysis tool to gain insights over its bus booking service (Kumar, 2006). Its datasets could easily stretch up to 2 terabytes in size. The application would have to be able to analyse booking and inventory data across hundreds of bus operators serving more than 10.000 routes. Furthermore, the company needed to avoid setting up and maintaining a complex in-house infrastructure.

At first, RedBus considered implementing inhouse clusters of Hadoop servers to process data. However they soon realized it would take too much time to set up such a solution and that it would require specialized IT teams to maintain such infrastructure. The company then regarded Google bigQuery as the perfect match for their needs, allowing them to:

- Know how many times consumers tried to find an available seat but were unable to do it due bus overload;
- Examine decreases in bookings;
- Quickly identify server problems by analysing data related to server activity;

Moving towards big data brought RedBus business advantages. Google bigQuery armed RedBus with real-time data analysis capabilities at 20% of the cost of maintaining a complex Hadoop infrastructure (Kumar, 2006).

As supported by Nokia and RedBus examples, switching towards big data enables organizations to gain competitive advantage. Additionally, BDaaS provided by big data vendors allows companies to leave the technical details for big data vendors and focus on their core business needs

7. ENCRYPTED BIG DATA MANAGEMENT IN CLOUD

The cost and scalability of the database server is high and hence it cannot be used for Big Data processing. One option is to use classic multi-tier database application architecture for processing Big Data. In general, different business models are used for different applications of Big Data[7]. Distributed File System architecture that supports fault tolerance by data partitioning and replications. Google's cloud computing platform and Hadoop are utilizing this distributed file system. Web data sets are generally semi structured and it cannot satisfy big service providers. Big table is used as distributed storage system that can scale to very large amount of data. Bit table provides clients a data model that supports dynamic control over data layout and format.

Challenges in Encrypted Big Data Management:

There are many challenges in managing Encrypted Big Data in cloud. We need to provide mechanisms to handle every increasing volume of data, data that are unstructured. These varieties of data need to be extracted quickly along with the provisions of aggregating and correlating data if they are from multiple sources.

How to organize, store and extract unstructured data is a biggest challenge in cloud environments. Since we have large volumes of data, timely retrieval of data is expected. Protocols and interfaces are needed for integrating data of different nature viz. structured, semi-structured and unstructured from different sources.

To manage resources and efficient data processing, new programming methodologies and paradigms are needed with improved backend engines to manage optimized file system architecture.

Encrypted Big Data Issues in Cloud

Although big data solves many current problems regarding high volumes of data, it is a constantly changing area that is always in development and that still poses some issues. In this section we present some of the issues not yet addressed by big data and cloud computing.

As the amount of data grows at a rapid rate, keeping all data is physically cost-ineffective. Therefore, corporations must be able to create policies to define the life cycle and the expiration date of data (data governance). Moreover, they should define who accesses and with what purpose clients' data is accessed. As data moves to the cloud, security and privacy become a concern that is the subject of broad research.

Big data DBMSs typically deal with lots of data from several sources (variety), and as such heterogeneity is also a problem that is currently under study. Other issues currently being investigated are disaster recovery, how to easily upload data onto the cloud, and Exaflop computing.

Within this section we provide an overview over these problems.

Security

Cloud computing and encrypted big data security is a current and critical research topic (Popović & Hocenski,2015). This problem becomes an issue to corporations when considering uploading data onto the cloud. Questions such as who is the real owner of the data, where is the data, who has access to it and what kind of permissions they have are hard to describe. Corporations that are planning to do business with a cloud provider should be aware and ask the following questions:

Who is the real owner of the data and who has access to it? The cloud provider's clients pay for a service and upload their data onto the cloud. However, to which one of the two stakeholders does data really belong? Moreover, can the provider use the client's data? What level of access has to it and with what purposes can use it? Can the cloud provider benefit from that data?

In fact, IT teams responsible for maintaining the client's data must have access to data clusters. Therefore, it is in the client's best interest to grant restricted access to data to minimize data access and guarantee that only authorized personal access its data for a valid reason.

Where is the encrypted data? Sensitive data that is considered legal in one country may be illegal in another country, therefore, for the sake of the client, there should be an agreement upon the location of data, as its data may be considered illegal in some countries and lead to prosecution

Privacy

The harvesting of encrypted data and the use of analytical tools to mine information raises several privacy concerns. Ensuring data security and protecting privacy has become extremely difficult as information is spread and replicated around the globe. Analytics often mine users' sensitive information such as their medical records, energy consumption, online activity, supermarket records etc. This information is exposed to scrutiny, raising concerns about profiling, discrimination, exclusion and loss of control (Tene & Polonetsky, 2012). Traditionally, organizations used various methods of deidentification (anonymization or encryption of data) to distance data from real identities. Although, in recent years it was proved that even when data is anonymized, it can still be re-identified and attributed to specific individuals (Tene & Polonetsky, 2012). A way to solve this problem was to treat all data as personally identifiable and subject to a regulatory framework. Although, doing so might discourage organizations from using de-identification methods and, therefore, increase privacy and security risks of accessing data

Privacy and data protection laws are premised on individual control over information and on principles such as data and purpose minimization and limitation. Nevertheless, it is not clear that minimizing information collection is always a practical approach to privacy. Nowadays, the privacy approaches when processing activities seem to be based on user consent and on the data that individuals deliberately provide. Privacy is undoubtedly an issue that needs further improvement as systems store huge quantities of personal information every day.

Data Governance

The belief that storage is cheap, and its cost is likely to decline further, is true regarding hardware prices. However, a big data DBMS does also concern other expenses such as infrastructure maintenance, energy, and software licenses (Tallon, 2013). All these expenses combined comprise the total cost of ownership (TCO), which is estimated to be seven times higher than the hardware acquisition costs.

Regarding that the TCO increases in direct proportion to the growth of big data, this growth must be strictly controlled. Recall that the "Value" (one of big data Vs) stands to ensure that only valuable data is stored, since huge amounts of data are useless if they comprise no value.

Data Governance is a general term that applies to organizations with huge datasets, which defines policies to retain valuable data as well as to manage data accesses throughout its life cycle. It is an issue to address carefully. If governance policies are not enforced, it is most likely that they are not followed. Although, there are limits to how much value data governance can bring, as beyond a certain point stricter data governance can have counterproductive effects.

Disaster Recovery

Encrypted Data is a very valuable business and losing data will certainly result in losing value. In case of emergency or hazardous accidents such as earthquakes, floods and fires, data losses need to be minimal. To fulfil this requirement, in case of any incident, data must be quickly available with minimal downtime and loss. However, although this is a very important issue, the research in this particular area is relatively low.

As the loss of data will potentially result in the loss of money, it is important to be able to respond efficiently to hazardous incidents. Successfully deploying big data DBMSs in the cloud and keeping it always available and fault-tolerant may strongly depend on disaster recovery mechanisms.

8. CONCLUSION

With encrypted data increasing on a daily base, big data systems and in particular, analytic tools, have become a major force of innovation that provides a way to store, process and get information over petabyte datasets. Cloud environments strongly leverage big data solutions by providing fault-tolerant, scalable and available environments to big data systems.

Although big data systems are powerful systems that enable both enterprises and science to get insights over data, there are some concerns that need further investigation. Additional effort must be employed in developing security mechanisms and standardizing data types. Another crucial element of Big Data is scalability, which in commercial techniques are mostly manual, instead of automatic. Further research must be employed to tackle this problem. Regarding this particular area, we are planning to use adaptable mechanisms in order to develop a solution for implementing elasticity at several dimensions of big data systems running on cloud environments. The goal is to investigate the mechanisms that adaptable software can use to trigger scalability at different

levels in the cloud stack. Thus, accommodating data peaks in an automatic and reactive way.

Within this paper we provide an overview of big data in cloud environments, highlighting its advantages and showing that both technologies work very well together but also presenting the challenges faced by the two technologies.

REFERENCES

[1] N.Nandhini, P.G Kathiravan "An Efficient Retrieval of Encrypted Data In Cloud Computing", Vol.2 Special Issue 1, 2014, IJIRCCE
[2] Vivekanand, Dr.B.M Vidhyavathi, "Security Challenges in Big Data: Review", Volume 6, No.6 2015,IJARC
[3] Xiaofeng Ding, Member, IEEE, Peng Liu and Hai Jin, Senior Member, IEEE,"Privacy-Preserving Multi-Keyword Top-k Similarity Search Over Encrypted Data", Volume:PP, Issue 99, 2017, IEEE Transactions on Dependable and Secure Computing
[4] Hui Yin, Zheng Qin, Jixin Zhang, Lu Ou, and Keqin Li, Fellow, IEEE, "Achieving secure, universal, and fine-grained query results verification for secure search scheme over encrytped cloud data", Volume PP, Issue 89, 2017, IEEE Transactions on Cloud Computing
[5] http://rgtechnologies.com.au/resources/cloud-computing/
[6] https://www.computerweekly.com/news/2240180087/Six-security-issues-to-tackle-before-encrypting-cloud-data
[7] Jose Moura, Carlos Serrao,"Security and Privacy Issues of Big Data", https://arxiv.org/ftp/arxiv/papers/1601/1601.06206.pdf
[8] J.Raja, M.Ramakrishnan, "A Comprehenisve Stuidy on Big Data Security and Integrity Over Cloud Storage",Vol 9(40), 2016, IJST
[9] Pedro Caldeira Neves, Bradley Schmer, Jorge Bernardino, Javier Camara, "Big Data in Cloud Computing: features and issues", http://acme.able.cs.cmu.edu/pubs/uploads/pdf/IoTBD_2016_10.pdf

Authors

Mr. R. Manibharathi completed MCA from Institute Of Road and Transport Technology, Erode, Anna University, Chennai. He graduated BSc Information Technlogy from Manonmaniam Sundaranar University. He is currently working as Senior Developer at Shiro Software Solutions. His research interest in Cloud Computing, networking and Big Data.

Dr. K. Selva kumar started my research and teaching works from April 1987 at Bharathidasan University, Trichy, Tamilnadu, India. Received Ph.D. from Bharathidasan University in 1992. At present working as Assistant Professor in Mathematics at University College of Engineering, Anna University, Nagercoil Campus, Tamilnadu, India. Developing software for Networking , cloud computing. Image Processing, Singular perturbation problems in control design, aircraft optimal control guidance, Numerical methods for engineering related research problems.

Mr. Dinesh R has obtained his Bachelor Degree in Physics from Manonmaniam Sundaranar University. The obtained his Masters Degree from Anna University. Currently He is working as Project Manager in Shiro Software Solutions. He has 6 years experience in Software industries. He also has 4 years experience in teaching as Assistant Professor. His Specializations include Cloud Computing, Big data and Networking.