International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Efficient and Secure Data Storage in Cloud Computing

Manish M Saunshi[1], Manoj N[2], M Ramesh[3], Nithyashree B.T[4], Vaidehi M[5]

[1,2,3,4]8th Semester Students, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India
[2]Asst.Professor, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

Abstract - *Cloud computing is the way of providing computing resources in the form of services over internet. The cloud computing allows storing the user's data and to measure the applications and services provided by cloud server. There is an ample data stored at cloud storage server. Security is one of the major issues which reduce the growth of cloud computing so Cloud computing entails encyclopedic security solutions. This is presented on secure file exchanging on Cloud using SHA-256 algorithm which is capable of solving data security, authentication, and integrity problems of files on the cloud. Data security is improved by cryptography algorithms. The rightness of data is verified by introducing techniques. In our proposed system we integrate symmetric and asymmetric algorithms. Results show improved security and less storage space.*

Key Words: **Cloud Computing, Privacy, Security, Encryption, Storage**

1. INTRODUCTION

Cloud computing is the most demanded technologies used all over the world. It provides all kinds of services to the user. One of the most prominent service offered by cloud computing is cloud storage. Cloud storage is simply a term that refers to online space that you can use to store your data. It refers to delivering services over the internet or based on cloud infrastructure. The cloud computing will bring several advantages to the market and the three most important are: cost effectiveness, security and scalability. Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network. The biggest concern about cloud storage is cloud security. Security is considered as a key requirement for cloud computing consolidation as a robust and a feasible multipurpose solution.

Recently, most of the organizations are analyzing the cloud technology in term of cost saving tool used regardless of the level of the security provided by the Cloud Service Provider (CSP), but it is difficult to measure the benefits in term of one category, as discussed by Richard Mayo and Charles Perng in[2] where the saving represent based on the cloud computing Rate of Interest (RoI) a research conducted by IBM group. The RoI can be based on five categories as in Table1.

Table 1: Cost saving in cloud

Hardware	• Number of servers required will be reduced. • Reduce cost of floor space required. • Reduction in the power consumption.	• Negligible cost.
Software	• Number of OS to be purchased per client will be reduced. • Supporting and maintenance cost for different implemented software will be reduced.	• Cost required purchasing the virtualization software. • Cost of the cloud services management Software.
Automated Provisioning	• Reduction in number of hours required to provision each task.	• Cost required for training staff to work on automated provisioning systems. • Cost of deployment. • Maintenance Cost.
Productivity	• Having user friendly support service which will reduce Time required from staffto Wait for IT support.	• Negligible cost.
System	• Enhance	• Negligible cost.

administration	productivity of administration and support staff where there are more systems to support per administrator.	

In Figure 1, shows the result of a case study such as a bank where it requires a huge number of servers to manage their business which results in turning their business into cloud.

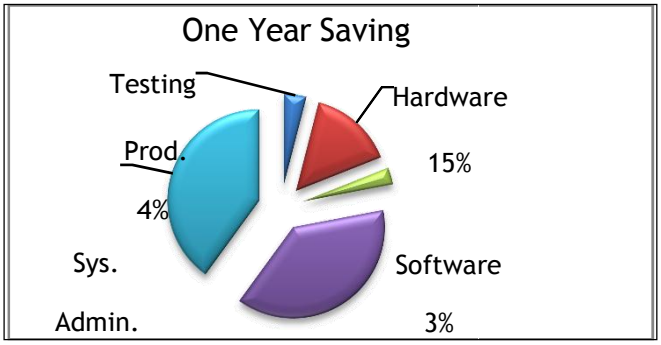


Figure 1. Statics showing savings through cloud services

In the near future, spending on cloud computing will grow rapidly as. "The US government projects between 2019 and 2025 will increase spending on cloud computing by 40% compound annual rate to reach $7 million by 2025". Cost effectiveness is one of the major motivations to use cloud computing. However, we should consider other challenges such as security. Organizations will upload its databases, user related information and in some cases the entire infrastructure will be hosted in the cloud.

2. CLOUD COMPUTING STRUCTURE

A. *Types of Cloud Systems*

There are main three systems categories: Software as a Service, Platform as a Service and Infrastructure as a Service. Let's look at them in more details as follows:

1) *Software as a Services(SaaS):*

Traditionally, users prescribe software and it is license in order to install it on their hard disk and then use it, however, in the cloud users do not required to purchase the software rather the payment will be based on pay-per-use model. It support multi-tenant which means that the physical backend infrastructure is shared among several users which are unique for each user.

2) *Platform as a Service(PaaS):*

In PaaS the development environment provided as service. The developers will use vendor's block of code to create their own applications. The platform will be hosted in the cloud and will be accessed using the browser.

3) *Infrastructue as a Service (IaaS):*

In IaaS, vendors provide the infrastructure as a service where it is delivered in form of technology, datacenters and IT services to the customer which is equivalent to the traditional "outsourcing" in the business world but with much less expenses and effort. The main purpose is to tailor a solution to the customer based on required applications. Table 2 shows cloud computing services that are currently utilized by several providers.

Table 2: Cloud Computing Services

	Services	Providers
SaaS	• Support running multiple instances of it. • Develop software that is capable to run in the cloud.	• Google Docs • Mobile Me • Zoho
PaaS	• Platform which allows developer to create programs that can be run in the cloud. • Includes several applications services which allow easy deployment.	• Microsoft Azure • Force.com • Google App Engine.
IaaS	• Highly scaled and shared computing infrastructure accessible using internet browser. • Consists of Database, servers and storage	• AmazonS3 • Sun's Cloud Service

Security Management (SM)includes functions that control and protect access to organization's resources, information, data, and IT services in order to ensure confidentiality, integrity, and availability. Security management functions are methods for authentication, authorization, encryption, etc. Unfortunately, the expanded definitions and standards around security management do not define a common set of security management areas.

Within the context of Cloud Computing, one of the most important security challenges is to manage and assure a secure usage over multi-provider Inter-Cloud environments with dedicated communication infrastructures, security mechanisms, processes and policies. The aim of Security controls in Cloud computing is, for the most part, no

different than security controls in any IT environment from a functional security management perspective. The adaption and reuse of existing traditional security management areas that have to be enhanced for specific Cloud computing requirements (e.g., dynamic reconfiguration, distributed services, etc.) has been proposed.

Table 3: Examples of cloud providers

Provider	Application	Usage	Description
Amazon (IaaS)	• Elastic Compute Cloud (EC2) • Simple Storage Service (S3)	• Web application hosting • Backup and storage • High performance computing	• Web service provides scalable compute capacity in the cloud [7]. Allows application deployment on the web services interface. • Web services interface which is used for storageand retrieving data.
Google (SaaS, PaaS)	• Gmail • Google Email Security • Google Docs	• Messaging • Securing existing email systems • Collaboration	• Using email services without managing and maintaining message architecture. • Filtering spam and viruses. • Provide collaboration tools without installing software on the machines or servers.
Microsoft Azure (PaaS)	• Windows • .NET services • SQL Services	• Offering application to organization as SaaS • Application Development	• Organization uses Azure Platform to enhance the functionality of existing application without investing in internal infrastructure. • Use Azure platform to develop custom application

3. CLOUD SECURITY AND PRIVACY

In cloud computing, end users' data stored in the service provider's data centers rather than storing it on user's computer. This will make users concerned about their privacy. Moreover, moving to centralized cloud services will result in user's privacy and security breaches. Security threats may occur during the deployment; also new threats are likely to come into view. Cloud environment should preserve data integrity and user privacy along with enhancing the interoperability across multiple cloud service providers. Thus, we would like to discuss data integrity, confidentiality and availability in the cloud. The security related to data distributed on three levels:

- *Network Level:*
  The Cloud Service Provider (CSP) will monitor, maintain and collect information about the firewalls, Intrusion detection or/and prevention systems and data flow within the network.
- *Host Level:*
  It is very important to collect information about system log files. In order to know where and when applications have been logged.
- *Application Level:*
  Auditing application logs, which then can be required for incident response or digital forensics.

At each level, it is required to satisfy security requirements to preserve data security in the cloud such as confidentiality, integrity and availability as follows:

A. *Confidentiality*

Ensuring that user data which resides in the cloud cannot be accessed by unauthorized party. This can be achieved through proper encryption techniques taking into consideration the type of encryption: symmetric or asymmetric encryption algorithms, also key length and key

management in case of the symmetric cipher. Actually, it is all based on the CSP. For instance, Mozy Enterprise uses encryption techniques to protect customer data whereas Amazon S3 does not. It also depends on the customer awareness where they can encrypt their information prior to uploading it. Also, The CSP should ensure proper deployment of encryption standards using NIST standards in.

B. Integrity:

Cloud users should not only worry about the confidentiality of data stored in the cloud but also the data integrity. Data could be encrypted to provide confidentiality where it will not guarantee that the data has not been altered while it is reside in the cloud. Mainly, there are two approaches which provide integrity, using Message Authentication Code (MAC) and Digital Signature (DS). In MAC, it is based on symmetric key to provide a check sum that will be append to the data. On the other hand, in the DS algorithm it depends on the public key structure (Having public and private pair of keys). As symmetric algorithms are much faster than asymmetric algorithms, in this case, we believe that Message Authentication Code (MAC) will be the best solution to provide the integrity checking mechanism. Studies show that, PaaS and SaaS doesn't provide any integrity protection, in this case assuring the integrity of data isessential.

C. Availability:

Another issue is availability of the data when it is requested via authorized users. The most powerful technique is prevention through avoiding threats affecting the availability of the service or data. It is very difficult to detect threats targeting the availability. Threats targeting availability can be either Network based attacks such as Distributed Denial of Service (DDoS) attacks or CSP availability. For example, Amazon S3 suffered from two and a half hours outage in February 2008 and eight hours outage in July2008.

4. PROBLEM STATEMENT

Since the cloud is a multi tenancy model, Data security is one of the prime issue. In this paper we enhance the cloud performance by implementing appropriate data security techniques. Although cryptographic approaches can achieve the security goals for the cloud system, it might significantly reduce the efficiency of the cloud system and hence makes deployment of traditional data utilization service difficult. For example, the traditional encryption of data in the cloud makes inefficient to exploit the data redundancy when the server performs deduplication to save storage space. Moreover, the encrypted data cannot be searched in the traditional way due to the protection of the data privacy and hence results in additional costs for the user and the server. Therefore, it is desirable to build cryptographic approaches to achieve the security goals without introducing significant overhead for the cloud system. In this project, we mainly focus on efficient and secure data storage and retrieval in cloud computing

A. Challenges:

- The main challenge for any organization in managing the identities resulted from the variety of the user population that an organization consists- customers, employers, partners, etc.
- Managing and maintaining staff turnover within the organization where it varies based on the current trend of the business in the market and itsfunction.
- Handling user's identities in the case of merges and demerges.
- Avoid the duplication of identities, attributes and credentials.

The above mentioned challenges and more, direct companies to look for centralized and automated identity management systems. It is an arrangement made between groups of enterprises (this relationship based on the trust) so that users can use the same identification attributes to obtain services from the trusted group. The core responsibility is to manage the access control for services beyond the organizations internal network.

Thus, we would like to discuss the current practice of identity and access management (IAM) which is considered a great help in providing Authentication, Authorization and Auditing for users who are accessing the cloud computing as follows:

1) Authentication:

Cloud computing authentication involves verifying the identity of users or systems. For instance, service to service authentication involves in verifying the access request to the information which served by another service.

2) Authorization:

Once the authentication process succeeds, then the process of determining the privileges could be given to legitimate users. In this stage, the system will enforce the security policies.

3) Auditing:

It is the process of reviewing and examining the authorization and authentication records in order to check, whether compliances with predefined security standards and policies. Also, it will aid in detecting any system breaches.

5. PROPOSED SYSTEM

The proposed design allows the user to audit the cloud storage efficiently and in a more secured manner by

encrypting the data and later uploading it. The proposed design further supports secure and efficient dynamic operations on outsourced data including managed control such as,

> Deletion
> Append
> Security

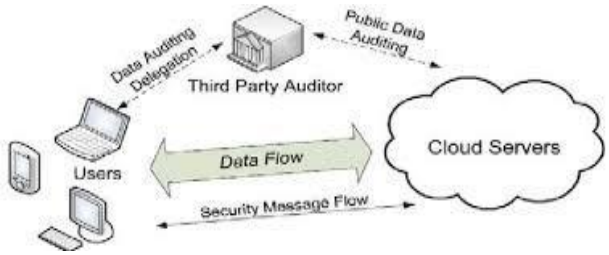


Figure 2.Cloud Data Storage Architecture

The three network entities viz. the client, cloud server and TPA are present in the cloud environment. The client stores data on the storage server provided by the cloud service provider (CSP). TPA keeps a check on client's data by periodically verifying integrity of data on-demand and notifies client if any variation or fault is found in client's data. Figure 2 shows the cloud data storage architecture

6. ARCHITECTURE

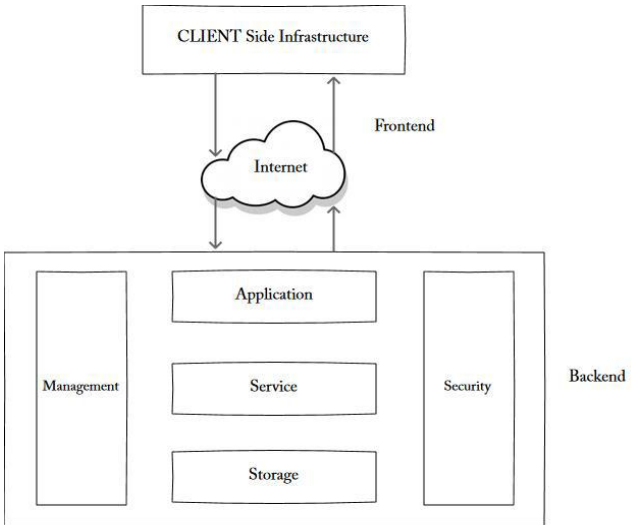


Figure 3. Architecture

At its most basic, cloud architecture can be classified into two sections: front-end and back-end, connected to each other via a virtual network or the internet.

Cloud Computing architecture refers to the various components and sub-components of cloud that constitute the structure of the system.

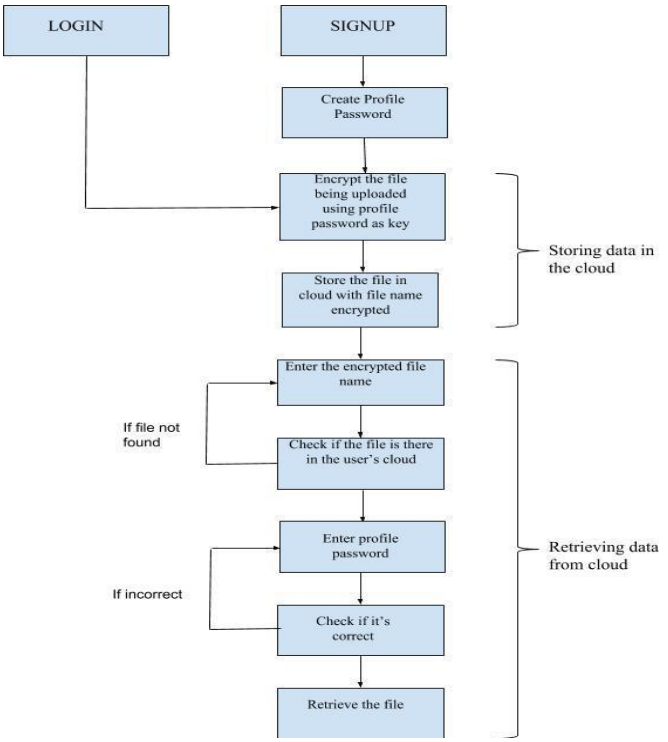
- A front-end platform that can include fat clients, thin clients, and mobile devices
- Back-end platforms, such as servers and storage
- A network (internet, intranet)

Front-end is the side that is visible to the client, customer, or user. Front-end pieces include the user interface, and the client's computer system or network that is used for accessing the cloud system. You have probably noticed that different cloud computing systems use different user interfaces—for example, not only can you choose from a variety of web browsers (including Chrome, Safari, Firefox, etc.), but the Google Docs user interface is different than that of Sales force.

On the other hand, the back-end pieces are on the side used by the service provider. These include various servers, computers, data storage systems, virtual machines, and programs that together constitute the cloud of computing services. The back- end side also is responsible for providing security mechanisms, traffic control and protocols that connect networked computers for communication. To briefly summarize: the front-end is the part you see, and the back-end is the computing that happens behind the scenes. Cloud services can be delivered publicly or privately using the internet and can also remain within a company's network when delivered over an intranet. Sometimes, organizations make use of a combination of both. No matter where the actual "cloud" is—a company's own data center or a service provider's data center, cloud computing uses networking to enable convenient, on-demand access to a shared pool of computing resources like networks, storage, servers, services, and applications. By using virtualization, these assets can be provisioned and released quickly and easily as necessary.

An online network storage where data is stored and accessible to multiple clients. Cloud storage is generally deployed in the following configurations: public cloud, private cloud, community cloud, or some combination of the three also known as hybrid cloud.

7. DATA FLOW DIAGRAM



Methodology:

In the proposed method, to ensure security the SHA-256 algorithm has been applied.

SHA-256 Algorithm:

This algorithm handles256 bits known as digest length. This algorithm does not use any keys. SHA-256 or Secure Hash algorithm is commonly used in data security for various applications. The hash function which is a mathematical model, converts the actual data into encrypted form. If the input data changes the output hash also changes.

Sample Results:

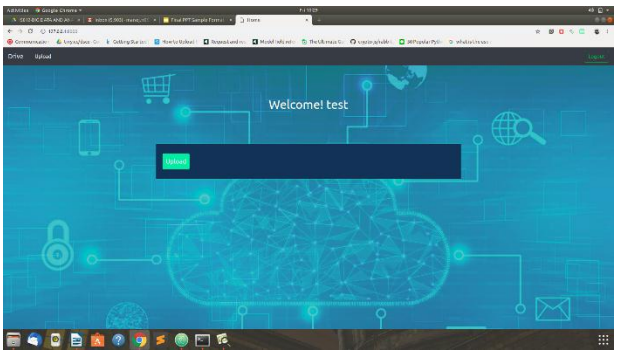
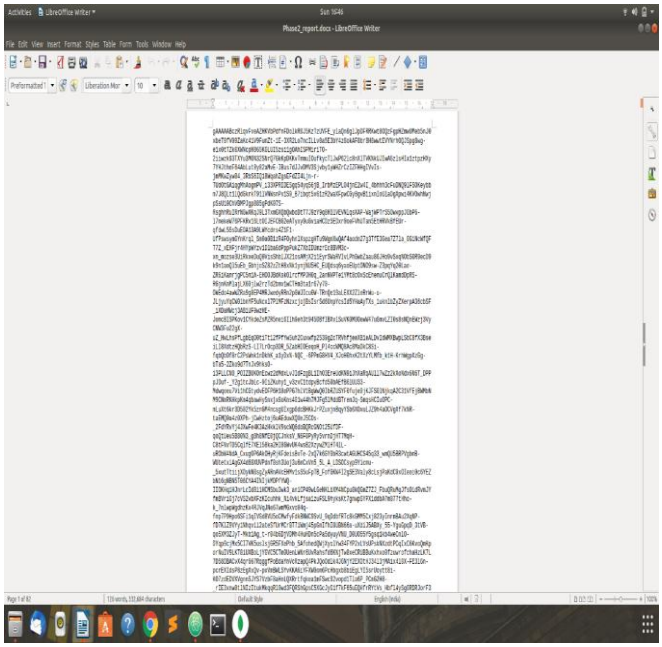


Figure 5 Image for encryption



8. CONCLUSION:

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computingre sources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. Data sharing in cloud computing enables multiple participants to freely share the group data, which improves the efficiency of work in cooperative environments and has widespread potential applications. However, how to ensure the security of data sharing within a group and how to efficiently share the outsourced data in a group manner are formidable challenges.

9. REFERENCES

1. Maithilee Joshi, Karuna P. Joshi and Tim Finin-"Attribute Based Encryption for Secure Access to Cloud Based EHR Systems" 2018 IEEE 11th International Conference on Cloud Computing

2. Sukhpal Singh, Gill and RajkumarBuyya -"Failure Management for Reliable Cloud Computing: A Taxonomy, Model and Future Directions "IEEE Cloud Computing 5, no. 1 (2018): 60-72.

3. Nelson Gonzalez-" A quantitative analysis of current security concerns and solutions for cloud computing" Journal of Cloud Computing: Advances, Systems and Applications 2012.

4. SameeraAbdulrahmanAlmulla-"Cloud Computing Security Management" , ISBN: 978-0-4596-802769, 2009

5. Michael Kretzschmar- "Cloud Computing Security Management Areas in the Inter Cloud", 2011 IEEE 4th International Conference on Cloud Computing.

6. V. Yamuna, AnushaPriya, "Efficient and Secure Data Storage in Cloud Computing RSA and DSE function", vol. 25, no. 6, June 2009, pp 599–616.

7. P.Geetha, "A Comparative-Study of Load-Cloud Balancing Algorithms in Cloud Environments", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)

8. V. Guzhov, K. Bazhenov, S. Ilinykh, A. Vagizov: "Cloud computing security *issues",* The 2-nd Indo-Russian Joint Workshop on Computational Intelligence and Modern Heuristics in Automation and Robotic*s*,pp. 128-133, 2011.

9. Partha Dutta, Tridib Mukherjee, Vinay G. Hegde and SujitGujar†: 2014 IEEE International Conference on "Cloud Computing-C-Cloud: A Cost-Efficient Reliable Cloud of Surplus Computing Resources"

10. Cong Wang, Qian Wang, and Kui: "Preserving Public Auditing for Data Storage Security in Cloud Computing" IEEE INFOCOM 2010.

11. T. Mather, S. Kumarasuwamy and S. Latif, "Cloud Security andPrivacy", O'Rielly, ISBN: 978-0-4596-802769, 2009.

12. J. W. Rittinghouse,J. F. Ransome, "Cloud Computing: Implementation,Management and Security" CRC Press, ISBN: 978-1-4398-0680-7,2009.

13. Paul McDougall, "The Four Trends Driving Enterprise CloudComputing",http://www.informationweek.com/cloudcomputing/blog/archives/2008/06/the-four -trends.html, 10 June 2008, retrieved 26 Feb 2009

14. M. Dikaiakos, G. Pallis, D. Katsaros, P. Mehra and A. Vakali, "CloudComputing: Distributed Internet Computing for IT and ScientificResearch", IEEE Internet Conputing, vol. 13, no. 5, 2009.

15.*"Architectural Strategies for Cloud Computing",* Oracle Corporation,August 2009.

16. H. Cademartori, "*Green Computing Beyond the Data Center*", ©TechTarget, 2007.

17. L. M. Kaufman, "Data Security in the World of Cloud Computing",IEEE Security & Privacy, vol. 7, no. 4, 2009.

BIOGRAPHIES:

1. **Author 1: Manish M Saunshi**
Description: 8th semester student, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

2. **Author 2: Manoj N**
Description: 8th semester student, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

3. **Author 3: M.Ramesh**
Description: 8th semester student, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

4. **Author 4: Nithyashree B T**
Description: 8th semester student, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

5. **Author 5: Vaidehi M**
Description:
Asst.Professor, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.