ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 10, October 2013

A User Centric Cryptographic Framework for Data Security in Public Cloud Storage

Reetika Singh
M.E. (CTA) Scholar
Dept. Of CSE, SSGI, Bhilai, C.G., India

Rajesh Tiwari
Associate Professor
Dept. Of CSE, SSGI, Bhilai, C.G., India

***Abstract*— Cloud computing is a set of technologies that allows computing applications and data to be exposed as a set of services from a pool of underlying resources. It provides development environment, allocation and reallocation of resources when needed, storage and networking facility virtually. Cloud Computing is access to massive computing power and storage resources on demand to customers. This paper highlights the problem of ensuring confidentiality and integrity of data stored in public cloud. A user can access cloud service as a utility service. Cloud Computing involves storage of user data in cloud which enables user to throw data in cloud without worrying about how it is stored or backing it up. This paper focuses on achieving user control data storage framework by providing a cryptographic security service and storage service in document centric public cloud applications. In particular, we proposing a framework in which user have full control over its data by implementing an AES symmetric encryption technique for achieving data confidentiality and HMAC technique for checking integrity of stored data in cloud.**

***Index Terms*— Cloud Computing, User Centric, Data Storage Security, Data Confidentiality, Data Integrity, AES Encryption, Public Cloud, and HMAC.**

I. INTRODUCTION

Cloud computing is an innovative technology that facilitates the networked nodes to share the pooled resources on demand in pay per use model. To meet ever changing business needs in computing resources and advances in networking technologies, organisation needs to invest time and money to scale up their infrastructure to outsource their storage and computing needs. On – premise IT infrastructure results in low scaling. Cloud computing is a paradigm in which resources in the computing infrastructure are provided as a service over the Internet. Organization simply connect to the cloud and can use computing resource on pay-per-use method which reduces organization's capital expenditure and can scale up or down the IT infrastructure as per the business need. Cloud computing is a paradigm shift that allows the end user to access computation resources through the Internet and it is gaining popularity because of its scalability, instant access and can save money. End user data is an important asset for any organization and in order to avail the benefits of cloud, it has to outsource data from its computing center to the provider's computing center and then no longer possess the data locally. The fundamental security challenges related to cloud computing are data storage security, data transmission security, application security and security related to third party resources. All the data security technique is built on confidentiality, integrity and availability of these three basic principles of information security [1]. Common methods for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission [5]. For achieving user data storage security in public cloud, a combined cryptographic implementation is proposed. The novel method of selecting the encryption algorithm is to have an algorithm that has speed and computational efficiency for handling encryption of large volumes of data which is in this paper is symmetric encryption AES – 128 algorithm is implemented. For checking data integrity Hashed Message Authentication Code (SHA-256) algorithm is implemented. The paper covers some aspects of major challenging problems for implementing security policies for networked storage from the user's perspective in multi-tenant public cloud environment.

II. LITERATURE REVIEW

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and the system software in the data centers that provide those services [6]. A computing Cloud is a set of network, enabled services, providing scalable, QoS guaranteed, normally personalized inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way [7]. As per NIST, Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud is composed of five essential characteristics (Rapid Elasticity, Measured Service, On-Demand Self-Service, Ubiquitous Network Access, Location-Independent Resource Pooling), three delivery

models (Software as a Service, Platform as a Service, and Infrastructure as a Service), and four deployment models (Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud)." Figure 1 shows a cloud computing framework with 3-4-5 principle.

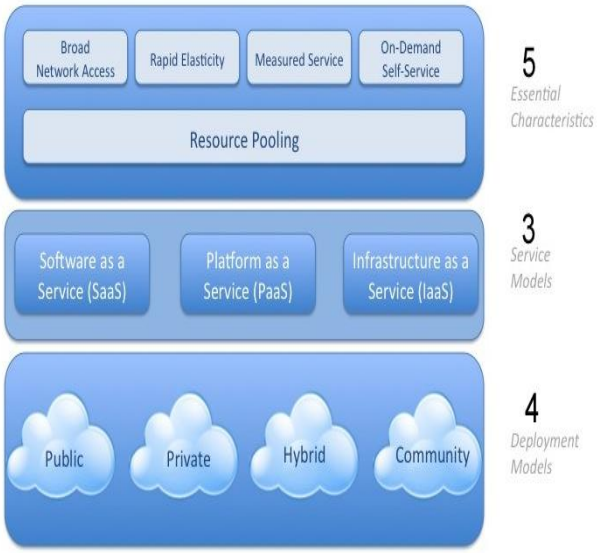

Figure 1 Cloud Computing: 3-4-5 principle

The basic structure of cloud computing model is comprises of users and providers which are divided into five levels from top to bottom – Resource Provider Layer, Cloud Service Provider Layer, Information Transport Layer, Professional Service Provider Layer and End User Layer. The Cloud Service Provider use the resources provided by resources layer and their technology to integrate the cloud services, and through the information transport layer to provide these services to users. Figure 2 shows users and service providers in basic cloud computing architecture.

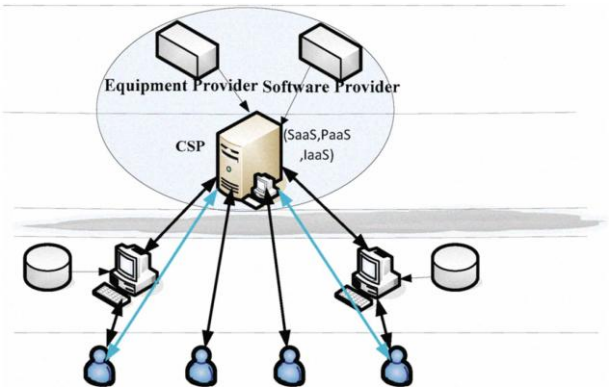

Figure 2 Users and Service Providers in Cloud Computing

Cloud computing collects all the computing resources and manages the automatically through software. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. In [2], [4] top 10 obstacles to and opportunities for the growth of cloud computing are defined. Along with the obstacles, various possible solutions are also discussed. In [3] cloud, protecting and controlling sensitive data is not an easy task. Companies do not have physical ownership of servers and has to rely on cloud provider to ensure security. Users are confused if they are storing their data in cloud, where is the division of responsibility. This problem is addressed in [5], [6] and proposes a distributed verification scheme by relying on cryptographic algorithms and a data protection model based on separating data storage from cryptographic process, thus providing a secure cloud environment for data storage and retrieval. Data protection is the biggest hurdle for companies wanting to move to cloud, since they rely on existing on site data center solutions that provides only preliminary protection access control, but due to multi-tenancy environment, these solutions are not enough that data protection is vulnerable. The security mechanism involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. In [1] they described a level defense system for data security in cloud - first level for user authentication, second level for data encryption and last level for fast recovery of data in cloud storage.

III. PROBLEM IDENTIFICATION & CHALLENGES

Cloud computing is conceptually viewed as a paradigm where software applications, data storage and processing capacity are accessed over the Internet by thin or thick client platforms. Cloud Computing is a software development concept in which services and storage are provided over the Internet. The cloud computing is a virtual environment that requires data transfer throughout the cloud. Cloud computing environments are multi-domain environments in which each domain can use different security, privacy, and trust requirements [3]. Security threats responsibility is equally distributed in cloud over its architectural components- cloud provider, enterprise that uses the cloud and the end users. One of the most significant problems is data security in the field of Cloud Security. In the Cloud Computing environment, important data, files and records are entrusted to a third party, which enables data security to become the main security issue of Cloud Computing. Despite the potential benefits and revenues that could be gained from the cloud computing model, the model still has a lot of open issues (obstacle/opportunity) that impact the model creditability and pervasiveness [2]. Obstacles are listed in Table 1 as under:

Obstacle	Opportunity
Availability/Business Continuity	Use Multiple Cloud Providers
Data Lock-In	Standardize APIs; Compatible SW to enable Hybrid Cloud Computing
Data Confidentiality & Auditability	Deploy Encryption, VLANs, Firewalls
Data Transfer Bottlenecks	FedExing Disks; Higher BW Switches
Performance Unpredictability	Improved VM Support; Flash Memory; Gang Schedule VMs
Scalable Storage	Invent Scalable Store
Scaling Quickly	Invent Auto-Scaler that relies on ML

Table 1 Obstacles to and Opportunities for growth of cloud computing

Cloud users face security threats both from outside and inside world. In cloud framework, responsibility of security is divided among cloud user, cloud service provider and any third party user. Normally it is the cloud user who is responsible for application – level security, since its user data which is being stored in the cloud. The main concerns for cloud user includes –

- Security & Privacy (data communication).
- Performance.
- Reliability (how user data is stored in a shared environment).

Data security (Privacy & Confidentiality) at public deployment of cloud includes security risks lists for:

- Privileged User Access.
- Data in Transit.
- Data at Rest.
- Data in Processing.
- Data Segregation.
- Data Integrity.
- Data Recovery.
- Long term viability.

The cloud computing is a virtual environment that requires data transfer throughout the cloud. To ensure data confidentiality, authentication, integrity, and availability, the provider should include the following: Encryption, Physical Security, Authentication and access control, Separation of duties and Intrusion detection and prevention. Public cloud data storage system requires a transition of responsibility and control to the cloud provider over data as well as software applications; users store their data in the cloud and no longer possess control over both the physical and logical aspects of the data. Thus security imposed on data by encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission [5], [6]. Table 2 shows the proposed data security aspect at each phase of data life cycle from its generation to destruction as under:

Table 2 Proposed Data Security Mechanism for user data in Cloud

Data Attributes	Storage	Processing	Transmission
Confidentiality	Symmetric Encryption	Homomorphic Encryption	SSL
Integrity	Hashed Message Authentication Code	Homomorphic Encryption	SSL

In this paper , we are defining a protection model for data storage in which the storage service provider can't store the data in the plain text, the data is first converted in encrypted format by the cryptographic process and the transferred via secure channel to storage provider for storage. To access data files shared by the data owner, data consumer or users download data files of their interest from cloud severs and then decrypt and can check for the integrity of data.

IV. CRYPTOGRAPHIC IMPLEMENTATION

Cloud computing is a type of computing environment where business owners outsource their computing need including application software services to a third party & when they need to use the computing resources they access the resource via Internet. The proposed framework comprises of 2 entities – Data Owner & Service Provider and 3 services – Data generation and transfer, Cloud Storage and Cryptographic Control.

Cryptographic Secure Framework comprises of following steps:

1. User authentication at service provider's side, if successful, then user can access cloud's broad range of computing activities.
2. For data manipulation service, i.e. for data storage, user transfers the file to cryptographic control (AES – 128 bit) for encryption.
3. Then transmit the encrypted user data for storage in cloud storage. File is hashed using SHA-256 and digest is stored on user side which will be used in checking data integrity.
4. For data retrieval service, first file is downloaded on user's side, then decryption and cryptographic hash is performed locally and retrieved digest and calculated digest is compared for ensuring data integrity.
5. User can also delete their stored data in cloud without modifying database constraints.

In the proposed framework, Data confidentiality and Data integrity are ensured by data encryption (Symmetric Cryptography) and Hashed Message Authentication Code (MAC) respectively. In this, AES Encryption technique is proposed for ensuring data confidentiality and Cryptographic Hash Function (SHA-256) is proposed for data integrity. The proposed security framework provides user centric interface where all operations are performed on the client side, which gives the users more control on the security of their data, and thus the data are not dependent on the security solutions provided by the servers.

Figure 3 & 4 shows the proposed user centric cryptographic framework for data storage in cloud.

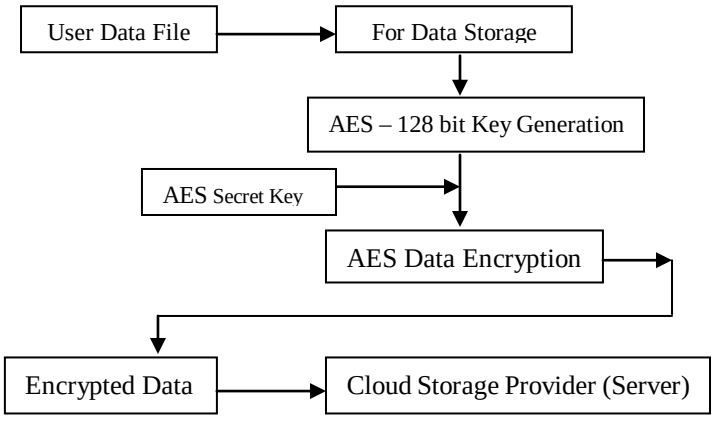

Figure 3 Data Encryption using AES before storage at Client's Side

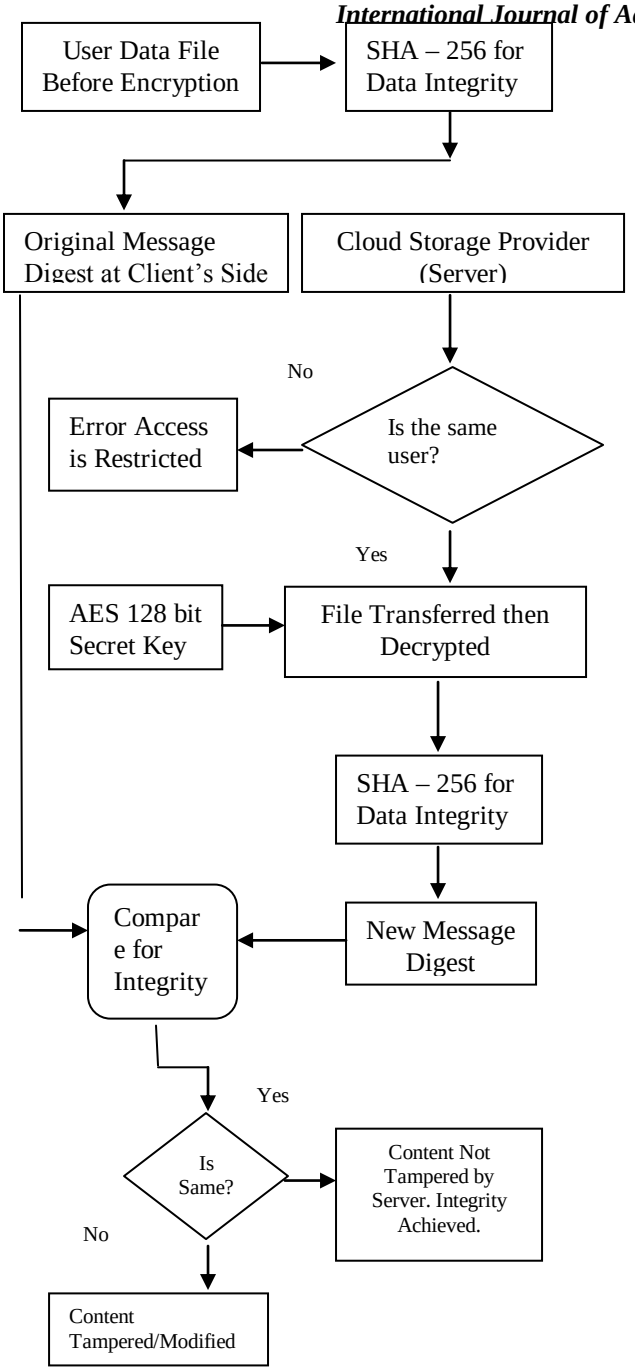

Figure 4 Data Verification at Client's Side Using AES and SHA

Advanced Encryption Standard (AES) is a block cipher with a block size of 128, 192 & 256 bits. AES algorithm begins with Key Expansion which is the round keys derived from the cipher key using 16-byte (128 bits) key. Initialize the 16-byte (128 bits) plain text block, then XOR the text block with expanded key. The algorithm is executed with 9 rounds of four stages namely – SubBytes, ShiftRows, MixColumns and AddRoundKey. A message authentication code (MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

V. RESULT & ANALYSIS

Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network. In public cloud infrastructure, storage services provides customer with scalable and dynamic storage. Cloud Computing is renting of resources like networks, servers, storage, applications & services in pay as you go model. In proposed framework, there are 2 main modules – client/cloud user authentication & data manipulation service. Data manipulation service includes – data storage at server's side and data retrieval at client's side. Cryptographic Implementation includes following steps:

1. After user authentication, AES-128 bit Secret key is generated using Key Generator class. Then using secret key, first file is encrypted at client/user's side. Prior to encryption, Hash digest (SHA-256) of original user data file is calculated and stored. Both the encryption and hash function operation is performed simultaneously. Figure 5 below shows the sequence of events at client's side.

```
F:\JAVA>javac cclient.java
Note: cclient.java uses or overrides a deprecated API.
Note: Recompile with -Xlint:deprecation for details.

F:\JAVA>java  cclient
Enter username :
Reetika
Enter Password :
Authorised User
Timestamp for Authentication in Miliseconds : 7032
Enter the file name :
SC.txt
Record Inserted
File is hashed for verification..
File -  SC.txt is encrypted and transferred to cloud..
Timestamp for Data Transfer in Miliseconds : 494
```

Figure 5 Data Encryption and Hash Calculation at User's Side

2. For data retrieval at client's side, firstly the intended file is downloaded then decryption is performed locally. Since in this framework, AES Symmetric Technique is implementing, in which a single secret key is used for encryption and decryption. So, in multi-tenant environment like cloud, only the user (probably the same user who encrypted the desired file), who have access authority can able to decrypt the file. After decryption, user can check the integrity of stored file by calculating the digest of decrypted file and then comparing it with the stored digest of original file. If both the digest are same, then there is no modification/tampering done at server side. Figure 6 below shows sequence of data retrieval/access

```
F:\JAVA\Server>javac cftserver.java

F:\JAVA\Server>java  cftserver
Cloud Server's Started
Waiting 4 Connection
Cloud User Connected
Checking for user authentication...
Successful User Authentication
Content Transfered..
Reetika's Data : SC.txt is stored.

F:\JAVA\Server>_
```

operation.

Figure 6 Data Access & Integrity Check from Server's Side

Secure framework includes mechanism for AES encryption/decryption for data storage in public cloud, HMAC-SHA (256) for data verification and integrity, and also a Service level agreement in compliance with data regulatory system stating that data stored in the cloud should not be tampered, modified and readable by the server be defined prior to use cloud services between cloud user and cloud service provider.

In this paper, AES is implemented in CTR (Counter) mode in which for encryption, the counter is encrypted and then XORed with the plain text block to get the cipher text. In previous studies, for encryption process, asymmetric algorithm – RSA was implemented. But for more security of data at rest and in transit, symmetric cryptography is preferred. We have analyzed following symmetric algorithms – DES and Blowfish with AES encryption and found that AES with 128 bit and 256 bit key size is comparatively faster in terms of encryption and decryption time, CPU execution time and Memory utilization [11], [12]. Moreover, we have also analyzed AES with RSA, and found that RSA is slow in execution of encryption and decryption process when tested using Java Cryptography Extension. Table 3 shows the performance analysis of DES & Blowfish (in CBC mode), AES (in CTR mode) and RSA using JCE in client server architecture for transfer of data of size 5-30 KB.

Table 3 Performance Analysis of Various Encryption Techniques

Algorithm	Key Size in Bits	Block Size in Bits	Execution Time in (Secs)
DES	64	64	.85
AES	128	128	.55
Blowfish	128	64	.45
RSA	-	-	1.7

VI. CONCLUSION

Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing deliver to organizations on-demand service wherever they need. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing deliver to organizations on-demand service wherever they need. These deliveries are software, infrastructure and storage over the internet. According to service delivery models, deployment models and essential features of the cloud computing, data security is the prime aspect of cloud computing. There are three types of main problems in Cloud Computing, including Data Security, Data Storage Security and Hostile Attack. In this paper, we focused on data security in cloud storage which is essentially a distributed data storage system. The main goal is to securely store and manage data that is not controlled by the owner of the data. The proposed framework aims at providing a separated mechanism for data storage and cryptographic security in public deployment of cloud by implementing symmetric encryption technique for confidentiality of data at rest and cryptographic hashing for integrity of data in transit in achieving user data security. The proposed model provides an integrated user centric cryptographic framework of Data, Storage and Security as service for the user data in the network based cloud applications.

REFERENCES

[1] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, *"Data Security Model for Cloud Computing"*, 2009 International Workshop on Information Security and Application (IWISA 2009) – Nov 2009.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, David Patterson, and Matei Zaharia "*A View of Cloud Computing*", Communications of the ACM, April 2010, Vol.53, Issue. 4.

[3] Hassan Takabi and James B.D. Joshi, "*Security and Privacy Challenges in Computing Environment*", IEEE Computer and Reliability Societies, Nov-Dec, 2010.

[4] S. Subashini n, V.Kavitha**, "***A survey on security issues in service delivery models of cloud computing*", Journal of Network and Computer Applications, Elsevier, 2010.

[5] Joshi Ashay Mukundaro, Galande Prakash Verma, *"Enhancing Security in Cloud Computing"*, Information and Knowledge management, IISTE, Vol.1 No.1, 2011.

[6] Gargee Sharma and Prakriti Trivedi. *"A Model for Data Protection Based on the Concept of Cloud Computing"***.** International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012.

[7] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, JieTao, "*Cloud computing: A Perspective study"*.

[8] Dyen Chen, Hong Zhao, *"Data Security and Privacy Protection Issues in Cloud Computing"*, 2012, International Conference on Computer Science and Electronics Engineering.

[9] N. Saravanan, A. Mahendrian, N.Sairam and N. Venkata Subramaniam, *"An Implementation of RSA algorithm in Google Cloud using Cloud SQL"*, Research Journal of Applied Sciences, Engineering and Technology, Oct-2012.

[10] Atul Kahate, *"Cryptography & Network Security"*, 2E, McGraw Hill.

[11] Dhawan, Priya, *"Performance Comparison: Security Design Choices,"* Microsoft Developer Network October 2002. http://msdn2.microsoft.com/en-us/library/ms978415.aspx.

[12] Aamer Nadeem et al, *"A Performance Comparison of Data Encryption Algorithms",* IEEE 2005 .

[13] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing.

[14] Bhaskar Prasad Rimal, Admela Jukan, Dimitrios Katsaros, Yves Goeleven, *"Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach"*, 2011 J Grid Computing, Springer.

Reetika Singh completed B.E. (Computer Science & Engg.) from Shri Shankaracharya College of Engineering & Technology, Bhilai under Chhattisgarh Swami Vivekanand Technical University, Bhilai. And is pursuing her M.E. in Computer Technology & Application from FET (CSE), Shri Shnakaracharya Group of Institutions - SSTC, Junwani, Bhilai under Chhattisgarh Swami Vivekanand Technical University, Bhilai. Her research area includes Cloud Computing, Analysis and Design of Algorithms, Computer Network, Network Programming & Internet Multimedia Technologies.

Rajesh Tiwari, A.M.I.E, M.E. (CTA), PhD Pursuing is working as Sr. Associate Professor in FET (CSE), Shri Shnakaracharya Group of Institutions - SSTC, Junwani, Bhilai under Chhattisgarh Swami Vivekanand Technical University, Bhilai. His research area includes Cloud Computing, Parallel Computing, Computer System Architecture, and Parallel Processing.