International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Trusted Secured Architecture for Storage-as-a-Service (STaaS) Cloud

Sanneboina Nagaraju[1], K. B. V. Rama Narasimham[2]

[1, 2] Computer Science Engineering, Guntur Engineering College, Guntur, India

Abstract: ***Cloud Computing is mainly a service based technology, which involves Cloud Service Provider (CSP) and the User or Customer. The CSP provides types of cloud services, one of them is Data Storage as a Services (STaaS) where user stores his data over the cloud remotely via internet this calls for a serious security issue, as the user is no where the controller of the data security, this is a strict work of the CSP to create a trusted Environment for the user and create a trustworthiness. As per [1] "The data-protection as a service cloud platform architecture dramatically reduces per application development effort required to offer data protection while still allowing rapid development and maintenance". in these paper we presented an secured architecture for STaaS cloud in order to create an trustworthiness for users storage systems over cloud.***

Keywords: cloud computing; Data Storage-as-a-Service (StaaS); Cloud Service Provider (CSP); data- protection; secured architecture.

1. Introduction

Along Cloud Computing providing low costs, rapid deployment and scaling, easy maintenance and anywhere any time access a great challenge it imposes is securing data stored into the cloud. According to Song, Elaine and Ian "currently user rely primarily on legal agreements and implied economics and reputation harm as a proxy for application trustworthiness". Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature.

Researchers have proposed distributed protocols [3]–[5] for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited. In a cloud computing environment, the service content offered by service providers can be adjusted according to the needs of the user. For example, the applicant can request different amounts of storage, transmission speeds, and levels of data encryption and other services. In addition to defining the service items, the agreement normally also notes the time, quality and performance requirements provided with the service. Generally, these service agreements are referred to as Service Level Agreements (SLA) [6]. By signing an SLA, the user shows that he has understood and agreed to the contents of the application service, and agree with the provider's data privacy and protection policies.

A common approach to protect user data is that user data is encrypted before it is stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure.

Creating user trust through the protection of user's data content is the key to the widespread acceptance of the cloud computing. This study proposes a business model for cloud computing based on the concept of using a separate encryption and decryption service. In the model, data storage and decryption of user data are provided separately by two distinct providers. In addition, those working with the data storage system will have no access to decrypted user data, and those working with user data encryption and decryption will delete all encrypted and decrypted user data after transferring the encrypted data to the system of the data storage service provider.

Under the business model proposed in this study, the data storage cloud system provider is authorized to store the user's encrypted data, but does not have access to the Decryption Key. Thus, the storage system can only retrieve encrypted user data, but is unable to decrypt it. The cloud computing system responsible for encrypting user data has authority over all encryption keys required for data encryption but, given that the encryption provider does not store the user's data, internal mismanagement of the decryption keys still poses no risk of unauthorized disclosure of the user's data.

Given that encryption is an independent cloud computing service, a unique feature of the business model is that different services are provided by multiple operators. For example, the

Encryption as a Service provider and the "Storage as a Service" provider cooperate to provide a Cloud Storage System with effective data protection. This study provides a draft SLA for this type of business model of combining multiple providers in a single service, which can establish the cooperation model between operators and the division of responsibility for the services they jointly provide to the user.

2. Previous Work

2.1 Defining cloud

A more detailed review of the evolution of the Cloud Computing concept reveals that it is not a disruptive or totally new concept. It can be traced back to ideas from the 1960s and there are predecessors and related concepts like Application Service Provision, Utility Computing and Grid Computing that appeared in the last decades. The Internet began to grow rapidly in the 1990s and the increasingly sophisticated network infrastructure and increased bandwidth developed in recent years has dramatically enhanced the stability of various application services available to users through the Internet, thus marking the beginning of cloud computing network services. Cloud computing services use the Internet as a transmission medium and transform information technology resources into services for end-users, including software services, computing platform services, development platform services, and basic infrastructure leasing.

As a concept, cloud computing primary significance lies in allowing the end user to access computation resources through the Internet, as shown in Fig. 1. Some scholars find cloud computing similar to grid computing [8], but some also find similarities to utilities such as water and electrical power and refer to it as utility computing [7]. Because the use of resources can be independently adjusted, it is also sometimes referred to as autonomic computing [10].

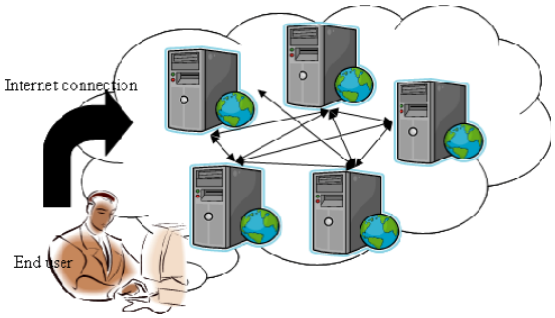


Figure 1: Cloud computing concept map

The literature contains many explanations of cloud computing [11]. After compiling scholarly definitions of cloud computing, Vaquero, Rodero-Merino, Caceres, and Lindner suggested that cloud computing could be defined as the integration of virtual resources according to user requirements, flexibly combining resources including hardware, development platforms and various applications to create services [12]. The special features of cloud computing include the storage of user data in the cloud and the lack of any need for software installation on the client side. As long as the user is able to connect to the Internet, all of the hardware resources in the cloud can be used as client-side infrastructure. Generally speaking, cloud computing applications are demand-driven, providing various services according to user requirements, and service providers charge by metered time, instances of use, or defined period.

2.2 Do Data in Cloud is secured?

In a cloud computing environment, the equipment used for business operations can be leased from a single service provider along with the application, and the related business data can be stored on equipment provided by the same service provider. This type of arrangement can help a company save on hardware and software infrastructure costs, but storing the company's data on the service provider's equipment raises the possibility that important business information may be improperly disclosed to others [13].

Some researchers have suggested that user data stored on a service-provider's equipment must be encrypted [9]. Encrypting data prior to storage is a common method of data protection, and service providers may be able to build firewalls to ensure that the decryption keys associated with encrypted user data are not disclosed to outsiders. However, if the decryption key and the encrypted data are held by the same service provider, it raises the possibility that high-level administrators within the service provider would have access to both the decryption key and the encrypted data, thus presenting a risk for the unauthorized disclosure of the user data.

2.3 Previous methods in protection of clod data

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. These protection methods normally require cryptography algorithms and digital signature techniques, as explained below:

Common data encryption methods include symmetric and asymmetric cryptography algorithms. Symmetric cryptography is used in the U.S. Federal Information Processing Standard's

(FIPS) 46-3 Triple Data Encryption Algorithm (TDEA, also known as Triple-DES or 3DES) or 197 Advanced Encryption Standard (AES) and others. This type of encryption and decryption process uses a secret key. Asymmetric cryptography, on the other hand, uses two different keys, a "public key" for encryption, and a "private key" for decryption. Examples include RSA cryptography [6] and Elliptic Curve Cryptography (ECC) [7]. Generally speaking, symmetric cryptography is more efficient, and is suitable for encrypting large volumes of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography.

The use of passwords as an authentication process is more familiar to general users, but messages sent by the user are vulnerable to surreptitious recording by hackers who can then use the data in the message to log into the service as the user. In more advanced authentication systems, the system side will generate a random number to send the user a challenge message, requesting the user to transmit an encrypted response message in reply to the challenge message, thus authenticating that the user has the correct encryption key. Without this key, the user will not be allowed access. In the process of challenge and response the

client's encrypted key uses the client's password to convert a derived value and. In this program, each communication between the client and server is unique, and a hacker using an old message would fail to access the system. In addition, the One-Time Password (OTP) authentication system differs from most peoples' conception of a password [8]. Most people understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP however is the single-use nature of the password.

After receiving authentication from the user, the system side must create a secure transmission channel to exchange information with the user. The Secure Sockets Layer (SSL) is a common method of building secure channels [9], primarily using RSA encryption to transmit the secret keys needed for the both sides to encrypt and decrypt data transmitted between them.

When using cryptographic technology to protect user data, the keys used for encryption and decryption of that data must be securely stored. In particular, cloud computing service providers must have specific methods for constraining internal system management personnel to prevent them from obtaining both encrypted data and their decryption keys – this is critical to protecting user data. Operator policies for protecting user data must be clearly laid out in the Service Level Agreement (SLA) and must explain how special privilege users are prevented from improperly accessing user data.

Kandukuri, Paturi and Rakshit offer six recommendations for SLA content [6], including (1) special privilege user data access must be controlled to prevent unauthorized storage or retrieval, (2) cloud computing services must comply with relevant laws, (3) user data must be properly stored and encrypted, (4) a reset mechanism must be provided in case of service disruption or system crash, (5) service must be sustainable and guaranteed against service discontinuation due to change or dissolution of the provider and (6) if cloud computing services are used for illegal purposes, the provider must be able to provide records to assist with investigations.

3. A Trusted Secured architecture for Storage-as-a-Service(STaaS) Cloud

Cloud service provider (CSP) Lends his Infrastructure in the Model of IAAS And the Third party Lends Encryption and Decryption Software in the Model of SAAS, here the Entire Crypto system Keys Are distributed among the Customer and the Third party keeping the CSP away And Both the Third party and Customer can interconnect In accessing the data Which was preserved by the Customer in CSP, which answers the data security problem in an robust approach.

3.1 Core Concepts

This study proposes An Adopted Secured Business Framework in the Cloud Environment. The concept is based on separating the storage and encryption/decryption of user data, as shown in Fig. 2. In this business model, Encryption/Decryption as a Service and Storage as a Service (SaaS) are not provided by a single operator. In addition, the SaaS provider may not store unencrypted user data and, once the provider of Encryption/Decryption as a Service has finished encrypting the user data and handed it off to an application (e.g. a SAAS system), the encryption/decryption system must delete all encrypted and decrypted user data.

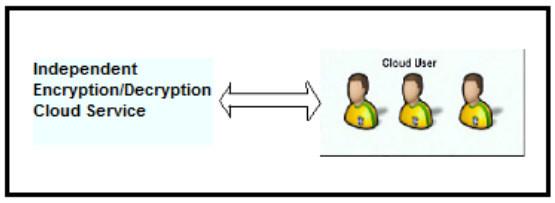


Figure 2: Encryption/Decryption as an independent service

The concept of dividing authority is often applied in business management. For example, responsibility for a company's finances is divided between the accountant and cashier. In business operations, the accountant is responsible for keeping accounts, while the cashier is responsible for making payments. By keeping these two functions separate, the company can prevent the accountant from falsifying accounts and embezzling corporate funds. Official documents frequently need to be stamped with two seals (i.e., the corporate seal and the legal representative's seal), thus preventing a staff member from abusing his position to issue fake documents, and these seals are normally entrusted to two different people. These examples of the division of authority are designed to avoid a concentration of power which could raise operational risks.

In a cloud computing environment, the user normally uses cloud services with specific functions, e.g., Salesforce.com's SAAS service [10], SAP's ERP services [11], etc. Data generated while using these services is then stored on storage facilities on the cloud service. This study emphasizes the addition of an independent encryption/decryption cloud service to this type of business model, with the result that two service providers split responsibility for data storage and data encryption/decryption.

To illustrate the concept of our proposed business model, Fig. 3 presents an example in which the user uses separate cloud services for SAAS, storage and encryption/decryption. According to the user's needs, SAAS Cloud Services could be swapped for other function-specific application services (e.g., ERP Cloud Services, Account Software Cloud Services, Investment Portfolio Selection and Financial Operations Cloud Services).

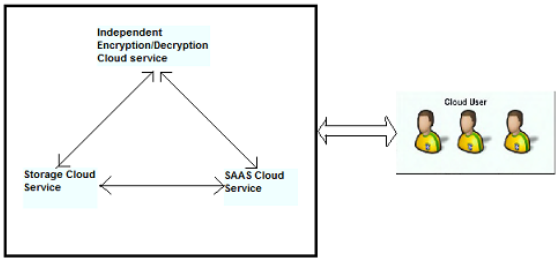


Figure 3: Security Agreement framework integrating separate cloud services for data encryption/decryption, SAAS and storage

Prior to the emergence of an emphasis on the independence of encryption/decryption services, SAAS, ERP and other cloud services would simultaneously provide their users with storage services. This study emphasizes that Encryption/Decryption Cloud Services must be provided independently by a separate provider.

3.2 Operating examples of the Encryption/Decryption as a Separate Cloud Service Business Model

This section presents a SAAS application service as an example of the new business model.

After the user logs into the SAAS system, if the SAAS Service System requires any client information, it will execute a Data Retrieval Program. When this data needs to be saved, it will execute a Data Storage Program. The Data Retrieval Program is illustrated in Fig. 4 and is explained below.

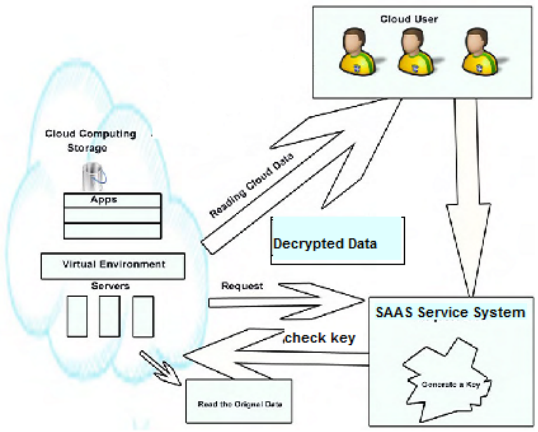


Figure 4: Data retrieval diagram

When a user wants to access the SAAS Cloud Service, he must first execute the Login Program as shown in Step 1. This step can use current e-commerce or other services which have already securely verified the user's registration, such as symmetric key-based challenge and reply login verification, or through a One-Time Password.

After the user's login has been successfully verified, if the SAAS Service System requires client information from the user, it sends a request for information to the Storage Service System, as shown in Step 2. In this step, the SAAS Service System transmits the user ID to the Storage Service System where it searches for the user's data. This data is encrypted so, once found, a request must be sent to the Encryption/Decryption Service System along with the user ID Step 3 shows the Storage Service System executing the transmission of encrypted client data and the user ID to the Encryption/Decryption Service System.

Since the Encryption/Decryption Service System can serve multiple users and the encryption/decryption for each user's data requires a different key, therefore each user's unique ID and keys are stored together. Therefore, in Step 4, the Encryption/Decryption Service System uses the received user ID to index the user's data decryption key, which is then used to decrypt the received data. Using the correct decryption key to decrypt the data is critical to restoring the data to its original state.

After the Encryption/Decryption Service System has decrypted the client's data, in Step 5 the decrypted client data is provided to the SAAS Service System which then displays the client data to the user in Step 6, completing the Data Retrieval Program. Prior to sending the decrypted client data, the Encryption/Decryption Service System and the SAAS Service System can establish a secure data transmission channel (e.g., a Secure Sockets Layer connection) to securely transmit the decrypted client data. After the decrypted client data is sent, the Encryption/Decryption Service System is not allowed to retain the decrypted data and any unencrypted data must be deleted to prevent the encrypted data and the decryption key from being stored in the same system. This is a critical factor in ensuring the privacy of user data.

The above-mentioned Data Retrieval Program requires the collaboration of three different cloud service systems. Different methods of system collaboration are already supported by mature technologies, including two systems based on Universal Description Discovery and Integration (UDDI), Web Service Description Language (WSDL), and Simple Object Access Protocol (SOAP) to use Web Services or transmit Extensible Markup Language (XML) formatted data [13].

Next, we describe the Data Storage Program, as shown in Fig. 5. This program also involves the collaboration of three cloud service systems: SAAS Service System, Encryption/Decryption Service System, and Storage Service System.

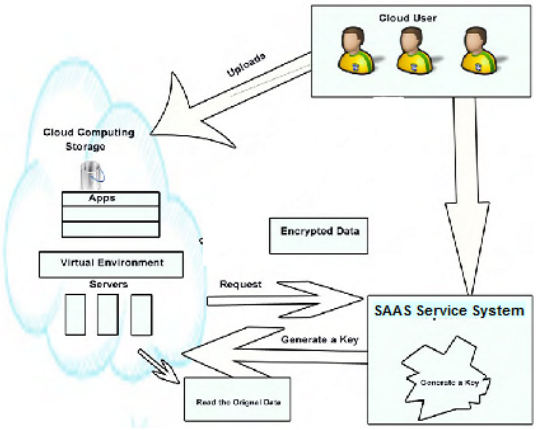


Figure 5: Data storage diagram

Step 1 of Fig. 5 shows the client sending a Data Storage Request to the saas Service System which then initiates the Data Storage Program, requesting data encryption from the Encryption/Decryption Service System as shown in Step 2. In Step 2, the Saas Service System and the Encryption/Decryption Service System establish a secure data transfer channel to transmit the user ID and the data requiring storage from the Saas Service System to the Encryption/Decryption Service System.

As the encryption of data from different users requires different keys, in Step 3 the Encryption/Decryption Service System initiates data encryption, which involves using the

received user ID to index the user's encryption key which is then used to encrypt the received data.

Following this study's emphasis on the principle of divided authority, once the client data is encrypted by the Encryption/Decryption Service System it must be transferred to the Storage Service System where the user ID and encrypted data are stored together. Therefore, when the Encryption/Decryption Service System executes Step 4, it must transfer the user ID and encrypted client data to the Storage Service System. Step 5 shows the Storage Service System receiving the user ID paired with the data for storage. In this business model, the following the completion of Step 4 at the Encryption/Decryption Service System, all unencrypted and decrypted user data must be deleted.

Step 6, the final step of the Data Storage Program, transmits a Data Storage Complete message from the Storage Service System to the SAAS Service System, at which point the Saas Service System may confirm that the client data has been stored. If it doesn't receive a Data Storage Complete message, it can re-initiate the Data Storage Program or, after a given period of time, proceed with exceptional situation handling.

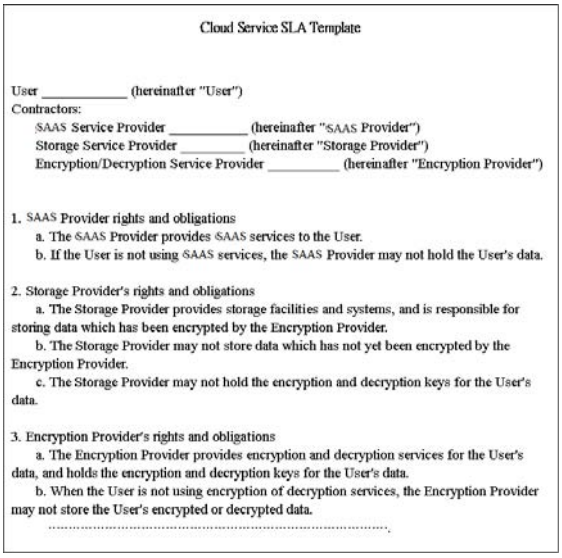
In the above example, the user's goal in logging into the Saas Service System is possibly to maintain part of the client data, thus the system design must take data maintenance into consideration. Feasible design methods include matching the encrypted client data with the corresponding user ID and client ID, thus allowing for the indexing of the user ID to obtain the corresponding client data. Then the client ID can be used to index the client data the user wishes to maintain. Considering the massive amount of client data, search efficiency could be improved by combining the user ID and client ID to form a combined ID used for searching for a specific client's data.

In the new business model, multiple cloud service operators jointly serve their clients through existing information technologies including various application systems such as ERP, accounting software, portfolio selection and financial operations which may require the user ID to be combined with other IDs for indexing stored or retrieved data. In addition, the foregoing description of the two systems can use Web Service related technology to achieve operational synergies and data exchange goals. These technologies can consider open international standards including the World Wide Web Consortium's (W3C) published Web Service, UDDI, WSDL and SOAP standard documentation.

4. Recommended Service Level Agreement Content

The above-mentioned example has multiple service operators coordinating to provide a Saas Cloud Service. The data handling flow and cooperation among operators will affect the effectiveness with which users use the service. Unlike conventional Service Level Agreements (SLA), any SLA between the user and the service provider must consider the rights and obligations of the collaborating operators, and operators should sign contracts between themselves to establish the division of responsibilities and cooperation model for providing common services to clients.

The proposed example of a SAAS Cloud Service includes a template for a multi-party SLA for the user, SAAS operator, encryption/decryption service operator, storage service operator. The content is based on policies for ensuring data privacy, as shown in Fig. 6.



Cloud Service SLA Template

User _____ (hereinafter "User")
Contractors:
SAAS Service Provider _____ (hereinafter "SAAS Provider")
Storage Service Provider _____ (hereinafter "Storage Provider")
Encryption/Decryption Service Provider _____ (hereinafter "Encryption Provider")

1. SAAS Provider rights and obligations
a. The SAAS Provider provides SAAS services to the User.
b. If the User is not using SAAS services, the SAAS Provider may not hold the User's data.

2. Storage Provider's rights and obligations
a. The Storage Provider provides storage facilities and systems, and is responsible for storing data which has been encrypted by the Encryption Provider.
b. The Storage Provider may not store data which has not yet been encrypted by the Encryption Provider.
c. The Storage Provider may not hold the encryption and decryption keys for the User's data.

3. Encryption Provider's rights and obligations
a. The Encryption Provider provides encryption and decryption services for the User's data, and holds the encryption and decryption keys for the User's data.
b. When the User is not using encryption of decryption services, the Encryption Provider may not store the User's encrypted or decrypted data.

Figure 6: Cloud services SLA template (Based on policies to ensure data privacy)

5. Conclusion

Protection of cloud user data is a critical phase to be handled in STaaS cloud environments, in these paper, we surveyed and proposed an enhanced security framework which uses separate Encryption and Decryption system as Trusted Third Party (TTP) which provides an SAAS Service which will be responsible for delivering security and integrity in Storage Service Environment between CSP and the user or CSP customer.

References

[1] Dawn song,Elaine shi,Ian Fischer "Cloud Data Protection for the Masses ," IEEE, 2012.
[2] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory Computing (STOC 09), ACM, 2009, pp. 169-178.
[3] L. Whitney, "Microsoft Urges Laws to Boost Trust in the Cloud," CNET News, 20 Jan. 2010; http://news.cnet.com/8301-1009_3-10437844-83.html.
[4] Tien-Ho Chen, Hsiu-lien Yeh, Wei-Kuan Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Schemefor Cloud Computing", Fifth FTRA International Conference on Multimedia and Ubiquitous Engineering, 2011
[5] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, May 2011

[6] Cong Wang, Qian Wang, and Kui Ren "Ensuring Data Storage Security in Cloud Computing," in Proceedings of the 2009 iacr.org.
[7] Chakraborty, T. K, Dhami, A.; Bansal, P.; Singh, T."Enhanced public auditability & secure data storage in cloud computing" Advance Computing Conference (IACC), 2013 IEEE 3rd International.
[8] Fred Cheng, "Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm," ACM: Mobile Networks and Applications, Pages 304-336, Volume 16 Issue 3, June 2011.
[9] Urien, P.; Marie, E.; Kiennert; Christophe "An Innovative Solution for Cloud Computing Authentication: Grids of EAP-TLS Smart Cards," IEEE, Digital Telecommunications (ICDT), 2010 Fifth International Conference, pp. 22-27, June 2010.
[10] R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.
[11] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.
[12] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.
[13] D. Benslimane, S. Dustdar, and A. Sheth, "Services mashups: the new generation of web applications". IEEE Internet Computing, vol. 12, no.5, pp. 13–15, 2008.

Author Profile

Sanneboina Nagaraju Obtained B.Tech in Computer Science Engineering from Vidya Vikas Institute Technologies, Chevella. At present pursuing the M.Tech in Computer Science and Engineering (CSE) at Guntur Engineering College, Guntur.

K. B. V. Rama Narasimham obtained the M.C.A Degree from Madras University in 1999 and M.Tech (CSE) from JNTU, Kakinada in 2013. At present pursuing Ph. D (CSE) in K. L. University. He has 8 years of teaching experience and working in Computer Science and Engineering (CSE) Department at Guntur Engineering College, Guntur.