IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Recent Trends in Cloud Computing

O. Jamsheela[1*], Mohd Abdul Hameed[2]

[1] Dept. of Computer Science, EMEA College of Arts and Science, Calicut University, Kerala, India
[2] Dept. of Computer Sciences and Engineering, University College of Engineering, Osmania University, Hyderabad, India

[*]*Corresponding Author ojamshi@gmail.com.com, Tel.: +919495961272*

DOI: https://doi.org/10.26438/ijcse/v7i5.18461851 | Available online at: www.ijcseonline.org

Accepted: 16/May/2019, Published: 31/May/2019

***Abstract*—** Developers with innovative ideas no longer needs the huge amount of capital investment in hardware or supporting software to deploy their service or the human expense to operate it because of the introduction of Cloud Computing. Cloud Computing is the delivery of computing services such as servers, software, databases, storage, networking, intelligence, analytics etc. over the Internet to facilitate faster innovation, economies of scale and flexible resources. While a lot of research is currently going on in the technology itself, this paper is trying to contain the new and emerging technologies in cloud computing. Here we have tried to bring most important new technologies introduced in Cloud Computing such as data sharing and data security. Finally**,** we presented some proposals which have connected other areas with cloud computing.

***Keywords*—**Cloud Computing, Data security, Data sharing, Cloud data sharing, Mobile Cloud Computing

I. INTRODUCTION

Nowadays Cloud Computing has become another most discussed term in all industry. Cloud Computing is not a completely new term, it has a strong connection to the concepts alike Grid Computing paradigm, utility computing, cluster computing, and distributed systems etc. However, there are many different definitions for Cloud Computing and most of them seem to be not a clear idea on what a Cloud is. One of the detailed definitions of cloud computing by NIST is that Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models [1].

Cloud Computing is the delivery of computing services such as servers, software, databases, storage, networking, intelligence , analytics etc. over the Internet to facilitate faster innovation, economies of scale and flexible resources. Users have to typically pay only for cloud services which they have used. The concept helps lower operating costs, run infrastructure more efficiently, increased productivity, speed and efficiency, performance and security. The name was inspired by the cloud symbol that's used to represent the Internet in flowcharts and diagrams. Recently Cloud Computing is connected to almost all fields. In a simple word, cloud computing is a kind of outsourcing of computer services. Using cloud technology, users are able to access applications and software from wherever they are actually stored, the services are being owned by an outside party and reside in the cloud environment. That enables users without worrying about things such as storage and power etc. They can simply enjoy the end result.

The cloud service providers enable users to store files and applications on remote servers and they can access the stored data using the Internet. The user is not required to be in a specific place to access the data, it enables the user to work remotely.

A. Clod Services.

The Cloud services are broadly divided into three different categories such as: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

1. IaaS: The most basic category of cloud computing services. With IaaS, anyone can rent elements of infrastructure such as hardware, software, servers and virtual machines (VMs), storage, networks, operating systems from a cloud provider (third party) and also providing backup, security, and maintenance. IaaS is provided as on demand basis through IP-based connectivity. The users need not purchase software or servers, instead use these resources in an outsourced, on-demand service. Some of the popular

examples of the IaaS system are IBM Cloud and Microsoft Azure.

2. PaaS: PaaS allows and provides the platform for users to develop, run, and manage applications without having the code, storage, infrastructure and so on. Mainly three types of PaaS are there, either public, private or a hybrid mix of the two. Public PaaS is hosted in the cloud, and its infrastructure is managed by the provider. Private PaaS, on the other hand, is housed in onsite servers or private networks, and is maintained by the user. Hybrid PaaS uses elements from both public and private, and is capable of executing applications from multiple cloud infrastructures. PaaS is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online; it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Force.com and Heroku.

3. SaaS: Software as a service is a method for delivering software applications over the Internet, on demand and usually on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser. SaaS provides a complete software solution which we can use as rent basis from a cloud service provider. The underlying middleware, infrastructure, app software and app data are located in the data centre. The service provider manages the hardware and software and with the appropriate service agreement, will ensure the availability and the security of the app and the data as well.

B. Types of cloud deployments: public, private and hybrid

Several different models, types and services have been available and developed to help the uses to select a right choice as their use. There are three different ways to deploy cloud services: on a public cloud, private cloud or hybrid cloud.

1. Public cloud: Third-party cloud service providers are owned and operated the public clouds. They deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. Clients can access these services and manage the account using a web browser.
2. Private cloud: A single business or organisation used cloud computing resources is refered as a private cloud. A private cloud can be physically located on the company's on-site datacenter. Third-party service providers also host someones private cloud on a payment basis. A private cloud is one in which the services and infrastructure are maintained on a private network.
3. Hybrid cloud: Hybrid clouds is a combination of public and private clouds, bound together by technology that allows data and applications to be shared between them. A hybrid cloud gives greater flexibility, more deployment options and helps optimise the existing infrastructure, security and compliance since it allows data and applications to move between private and public clouds.
4. Community cloud: The cloud infrastructure is maintained for the exclusive use of a specific community of consumers from organizations that have shared concerns. It may be operated, owned, and managed by one or more of the organizations in the community or a third party or some combination of them, and it may exist on or off premises[1].

The remainder of the paper is organized as follows: Section II contains the literature review on cloud computing. In Section III, new trends and technologies in cloud computing is discussed. The section is partitioned in to three sub sections. The first part contains new trends in secured data sharing in cloud computing, second part dealt with data security in cloud computing and the third section contains an overall view of the new technologies on cloud computing. The paper is concluded in Section IV.

II. RELATED WORK

Many papers have been published which dealt with cloud computing paradigm. Josep and Anthony D., et al. states that their aim was to reduce that confusion by clarifying terms, providing simple figures to quantify comparisons between of cloud and conventional computing, and identifying the top technical and non-technical obstacles and opportunities of cloud computing [2].

Another paper is trying to compare and contrast Cloud Computing with Grid Computing from various angles and give insights into the essential characteristics of both [3]. Another group of authors have published a paper as View of Cloud Computing [4]. The authors of paper [5] define what is Cloud computing and they also provide the architecture for creating Clouds with market-oriented resource allocation by leveraging technologies such as Virtual Machines (VMs). They also provide insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation. The authors also present some representative Cloud platforms, especially those developed in industries, along with their current work towards realizing market-oriented resource allocation of Clouds as realized in Aneka enterprise Cloud technology [5]. The aim of another paper on cloud computing is to provide a better understanding of the

design challenges of cloud computing and identify important research directions in this increasingly important area [6]. Other paper presents a set of recommendations for the practitioners who will provide and manage this technology. They also outline the different areas of research that need attention. Finally, they have presented some of the key issues facing governmental agencies who, due to the unique nature of the technology, will have to become intimately involved in the regulation of cloud computing[7].

III. NEW TRENDS AND TECHNOLOGIES IN CLOUD COMPUTING .

*A. Secure **data sharing** in cloud computing.*

Data sharing in cloud computing is a very important task. Many secure data sharing technologies have been introduced in this area and became popular too such as fine-grained data sharing, attribute-based encryption etc. However, most of the existing solutions suffer from the disadvantages of high computation overhead and weak data security, which has severely impeded resource-constrained mobile devices to customize the service. The problem of simultaneously achieving efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. With the popularity of cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved. In addition, how to achieve both anonymity and traceability is also a challenge in the cloud for data sharing.

1. A new research paper is introduced to addresses this challenging issue by proposing a new attribute-based data sharing scheme suitable for resource-limited mobile users in cloud computing [8]. The proposed scheme eliminates a majority of the computation task by adding system public parameters besides moving partial encryption computation offline. In addition, a public cipher text test phase is performed before the decryption phase, which eliminates most of computation overhead due to illegitimate cipher texts. For the sake of data security, a Chameleon hash function is used to generate an immediate cipher text, which will be blinded by the offline cipher texts to obtain the final online cipher texts. The proposed scheme is proven secure against adaptively chosen-cipher text attacks, which is widely recognized as a standard security notion. The paper also presents an extensive performance analysis, which indicates that the proposed scheme is secure and efficient.

2. Group data sharing in cloud environments is also another challenge and has become a hot topic in recent decades. Another research paper proposed by Shen, Jian, et al on the data sharing in cloud environment, they have given special attention on group data sharing. The paper focuses on secure and efficient data sharing and storage for the same group in the cloud in an anonymous manner. A novel traceable group data sharing scheme is proposed by leveraging the key agreement and the group signature to support anonymous multiple users in public clouds. However, the group members can communicate anonymously with respect to the group signature, and the real identities of members can be traced if necessary. Based on the key agreement a common conference key is derived to enable group members to share and store their data securely. Here the important thing is that for key generation, a symmetric balanced incomplete block design is utilized which substantially reduces the burden on members to derive a common conference key. Both theoretical and experimental analyses demonstrate that the proposed scheme is secure and efficient for group data sharing in cloud computing [9].

3. Mobile devices can store/retrieve personal data from anywhere at any time. With the popularity of cloud computing, the data security problem in mobile cloud becomes more and more dangerous and it discourages further development of mobile cloud. Consequently, there are lots of research studies have been conducted to improve the cloud security. However, most of the new approaches are not applicable for mobile cloud because mobile devices only have limited computing resources and power. Solutions for this problem are in great need for mobile cloud applications. In a new research paper the authors propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments [10].

4. In the cloud environment the sharing of data with multiple users from different domains has been benefited considerably. To ensure the sharing file should not be exposed to the unauthorized users or cloud providers, it is highly desirable to make the sharing in a highly secure way. Unfortunately, issues are still remaining challenging. To deal with these challenges, a novel anonymous attribute-based broadcast encryption (A ^{2} B ^{2} E) is proposed which features the property of hidden access policy and enables the data owner to share his/her data with multiple participants who are inside a predefined receiver set and fulfil the access policy. The authors first suggest a concrete A ^{2} B ^{2} E scheme together with the rigorous and formal security proof without the support of the random oracle model. Then, design an efficient and secure data sharing system by incorporating the A ^{2} B ^{2} E scheme, verifiable outsourcing decryption technique for attribute-based encryption, and the idea of online/offline attribute-based encryption. Extensive security analysis and

performance evaluation demonstrate that the proposed data sharing system is secure and practical [11].

5. It is convenient to share large-scale data among various kinds of users in cloud computing. As a kind of attribute-based encryption, ciphertext-policy attribute-based encryption (CP-ABE) is an efficient technique for realizing fine-grained access control on shared data. However, traditional CP-ABE is not suitable for mobile cloud computing, where mobile users are resource-limited and privacy is fragile. In a new research paper, the authors have proposed an efficient and privacy-aware attribute-based data sharing system supporting offline key generation and offline encryption. In the proposed system, sensitive attribute values specified in an access structure are not explicitly sent along with a ciphertext. The online/offline encryption mechanism alleviates the computational burden of mobile users by performing most of encryption tasks without draining the battery charge. In addition, the online/offline key generation mechanism allows the attribute authority to finish most of operations in the key generation process in advance, which enables efficient mobile user registration. The proposed system is proved as a fully secured and efficient system in the standard model and performance analysis also shows its effectiveness in mobile cloud computing [12].

B. **Data Security** in cloud computing.

In fact, security problem is one of the major obstacles in cloud computing adoption. Many efficient technologies are proposed to secure the data in cloud. However, the data protection is still remains significant challenges in cloud storage for data sharing. Here we have suggested some new proposals from various authors in this regard.

1. The cryptographic techniques are usually applied to protect the confidentiality of the shared sensitive data in cloud computing. Among them, how to protect and revoke the cryptographic key is the fundamental challenge. To handle this issue a new data protection mechanism is proposed by Zuo, Cong, et al[13] for cloud storage. They have mentioned the following properties. 1) The cryptographic key is protected by the two factors. Only if one of the two factors works, the secrecy of the cryptographic key is held. 2) The cryptographic key can be revoked efficiently by integrating the proxy re-encryption and key separation techniques. 3) The data is protected in a fine-grained way by adopting the attribute based encryption technique. They have done a security analysis and performance evaluation which shows that the proposal is secure and efficient. This paper proposed a fine-grained two-factor data protection for cloud storage. They have separated the secret key into two parts (the two-factor) one can be stored in a potential-insecure place, and the other is stored in a tamper resistant device. Only if one of them is kept secret, the proposal remains secure.

2. Jouini et.al proposed a new system to deal with security problems in cloud computing systems and show how to solve these problems using a quantitative security risk assessment model named Multi-dimensional Mean Failure Cost (M2FC). In fact, they summarize first security issues related to cloud computing environments and then propose a generic framework that analysis and evaluate cloud security problems and then propose appropriate countermeasures to solve these problems[14].

3. The file sharing ability between mobile terminals and public clouds is limited because of the storage and computing capacity limitations of a mobile terminal. Moreover, the security issues of public clouds increases the risks again. Private clouds can be regarded as a very effective trusted platform and have more security when a user uses a file from public clouds. Yang, Li, et al[15] propose a new scheme called FREDP (File Remotely keyed Encryption and Data Protection). The new scheme involves three-party interaction among a mobile terminal, private clouds and public clouds. The private clouds share the cipher text file to the public clouds until the mobile terminal and the trusted third party, the private clouds, finish the encryption of the plaintext file using a remotely keyed encryption algorithm. The private clouds as the third party regularly verify the integrity of the data in the public clouds to ensure security when a mobile terminal uses data. Finally, to use the data the mobile terminal and private clouds decrypt the ciphertext file. The authors have analysed the security of FREDP using BAN. The FREDP satisfies the security standard.

4.

C. Other Recent Technologies.

An interesting proposal is introduced by Langmead, Ben, and Abhinav Nellore[16]. In their paper they have explained how cloud computing is used for large-scale genomics collaborations and research. They also explain how cloud computing will likely be a basic underpinning for future large-scale genomics collaborations and for efforts to re-analyze archived data, including privacy-protected data.

Another approach is introduced as an implementation of biometric system. The proposed method presents a new Cloud platform designed to support basic web applications shared by small and medium companies. The platform guarantees secure access of multiple users and complete logical separation of computational and data resources related to different companies. They have ensured a high-level of protection of the data stored in the Cloud by using a peculiar data fragmentation approach. The OpenStack architecture is used to build the platform. The user authentication is based on an original biometric approach that easily integrates finger and face modalities [17].

Another two papers [18] [19] have introduced another kind of approaches which connects cloud computing with healthcare. In this paper, the authors propose a new scheme

that provides a combined approach of fine-grained access control over cloud-based multiserver data along with a provably secure mobile user authentication mechanism for the Healthcare Industry 4.0. The proposed scheme is the first to pursue fine-grained data access control over multiple cloud servers in a Mobile Cloud Computing environment [18].

In cloud computing different devices can be used to monitor residents' health and upload collected health data to cloud servers for sharing, which facilitates the development of e-healthcare record (EHR) systems. EHR systems have been faced privacy and efficiency challenges. One of most important issues concerned by patients is the confidentiality of EHRs. A new scheme is proposed for removing these kinds of issues [19]. The proposed system introduced a fine-grained EHR access control scheme which is proven secure in the standard model. In the proposed scheme, an EHR owner can generate offline ciphertexts before knowing EHR data and access policies, which performs a majority of computation tasks. Furthermore, the online phase can rapidly assemble the final ciphertexts when EHR data and access policies become known [19].

Ning, Zhaolong, et al.[20] have introduced "Green and sustainable cloud of things". The article first discusses some distinct research directions to provide a comprehensive understanding of edge computing supported by the integration of IoTs and cloud computing. The authors proposed a green and sustainable virtual network embedding framework for cooperative edge computing in wireless-optical broadband access networks [20].

An opensource software framework for cloud computing is presented as EUCALYPTUS in [21]. EUCALYPTUS implements as Infrastructure as a Service (IaaS) systems that give users the ability to run and control entire virtual machine instances. The paper gives an outline of the basic principles of the EUCALYPTUS design, detail important operational aspects of the system, and discuss architectural trade-offs. Finally, the authors provide evidence that EUCALYPTUS enables users familiar with existing Grid and HPC systems to explore new cloud computing functionality while maintaining access to existing, familiar application development software and Grid middle-ware[21].

Many research papers have been published based on cloud computing. Each day researchers are introducing different new technologies to improve the cloud computing security, trust, data sharing speed and so on. Some authors have contributed as survey papers on cloud computing. A survey paper is presented by Sakshi kathuria [22] by saying that the security will be more on multi cloud than a single cloud. In another survey paper, the authors briefly analyzed the factors and working aspects of cloud-based Trust models and the they also compares the factors of different types of Trust models, which are calculating trust values using different types of parameters such as data integrity, service availability and data turnaround efficiency[23]. Now a days in each and every field is using cloud based technologies. Even the people without any awareness about clouds are using cloud technologies. Cloud Computing has become an integral part of our life. Its use make our life easy and avoids wasting of our valuable time.

IV. CONCLUSION AND FUTURE SCOPE

The paper covers only some recent proposals in cloud computing. Security and data sharing are two of the most important issues in Cloud computing. So we have included more papers on those topics. We also have included some interesting approaches in Cloud Computing field. Many researchers have proposed lots of methods in these areas. We have selected only few papers in this survey. Finally, various cloud related schemes have been discussed on a comparative framework. On a whole, the paper aims at constructing a proper snapshot of the recent trends in Cloud Computing.

REFERENCES

[1] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[2] JoSEP, Anthony D., et al. "A view of cloud computing." *Communications of the ACM* 53.4 (2010).

[3] Foster, Ian, et al. "Cloud computing and grid computing 360-degree compared." *arXiv preprint arXiv:0901.0131* (2008).

[4] Fox, Armando, et al. "Above the clouds: A berkeley view of cloud computing." *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*28.13 (2009): 2009.

[5] Buyya, Rajkumar, et al. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." *Future Generation computer systems* 25.6 (2009): 599-616.

[6] Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." *Journal of internet services and applications* 1.1 (2010): 7-18.

[7] Marston, Sean, et al. "Cloud computing—The business perspective." *Decision support systems* 51.1 (2011): 176-189.

[8] Li, Jin, et al. "Secure attribute-based data sharing for resource-limited users in cloud computing." *Computers & Security* 72 (2018): 1-12.

[9] Shen, Jian, et al. "Anonymous and traceable group data sharing in cloud computing." *IEEE Transactions on Information Forensics and Security* 13.4 (2018): 912-925.

[10] Li, Ruixuan, et al. "A lightweight secure data sharing scheme for mobile cloud computing." *IEEE Transactions on Cloud Computing* 6.2 (2018): 344-357.

[11] Xiong, Hu, Hao Zhang, and Jianfei Sun. "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing." *IEEE Systems Journal* 99 (2018): 1-22.

[12] Zhang, Yinghui, Axin Wu, and Dong Zheng. "Efficient and privacy-aware attribute-based data sharing in mobile cloud computing." *Journal of Ambient Intelligence and Humanized Computing* 9.4 (2018): 1039-1048.

[13] Zuo, Cong, et al. "Fine-grained two-factor protection mechanism for data sharing in cloud storage." *IEEE Transactions on Information Forensics and Security* 13.1 (2018): 186-196.
[14] Jouini, Mouna, and Latifa Ben Arfa Rabai. "A security framework for secure cloud computing environments." *Cloud Security: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2019. 249-263.
[15] Yang, Li, et al. "A remotely keyed file encryption scheme under mobile cloud computing." *Journal of Network and Computer Applications* 106 (2018): 90-99.
[16] Langmead, Ben, and Abhinav Nellore. "Cloud computing for genomic data analysis and collaboration." *Nature Reviews Genetics* 19.4 (2018): 208.
[17] Masala, Giovanni L., Pietro Ruiu, and Enrico Grosso. "Biometric authentication and data security in cloud computing." *Computer and Network Security Essentials*. Springer, Cham, 2018. 337-353.
[18] Roy, Sandip, et al. "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications." *IEEE Transactions on Industrial Informatics* 15.1 (2019): 457-468.
[19] Liu, Yi, et al. "Secure and fine-grained access control on e-healthcare records in mobile cloud computing." *Future Generation Computer Systems* 78 (2018): 1020-1026.
[20] Ning, Zhaolong, et al. "Green and sustainable cloud of things: Enabling collaborative edge computing." *IEEE Communications Magazine* 57.1 (2019): 72-78.
[21] Nurmi, Daniel, et al. "The eucalyptus open-source cloud-computing system." *Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*. IEEE Computer Society, 2009.
[22] Sakshi kathuria,"A Survey on Security Provided by Multi-Clouds in Cloud Computing",International Journal of Scientific Research in Network Security and Communication,Vol.6,Issue.1,pp 23-28
[23] Kaur, U., M. Mahajan, and D. Singh. "A Comparative Analysis of Trust Models in Cloud Computing." *International Journal of Scientific Research in Network Security and Communication*6.2 (2018): 19-23.

