# Evaluation of security challenges in cloud computing

Prinka Thapar, Dr. Sanjay Sareen and Anil Kumar Guru Nanak Dev University, Amritsar, Punjab, India
May 9, 2019

## *Abstract*

Cloud computing is a new business model that have generated revolution in information technology (IT) industry. It provides scalable infinite storage space, Virtualized IT resource on demand over the Internet with pay only for service or resource utilized.In the last few years, cloud computing has grown a promising business concept for the IT companies and data concerning to large number of individuals and companies are placed in the cloud which is under the direct control of cloud service provider,with this so many security issues have raised. Despite of so many advantages of cloud computing, companies and customers are still hesitating for deploying their business and sensitive data in the cloud. Data security is one of the major issues that reduces the growth of cloud computing. It is concerned with confidentiality, integrity and availability of data.In this paper, a review of the different data security issues and their existing remedies and technology like Blockchain is used to provide process integrity by ensuring any block or even any modification that adds to chain cannot be edited and provides a very high security and addressing the interoperability, transparency, redundancy etc.Data Security is maintained so that unauthorized user may not access the secure data for misuse with the help of blockchain technology which doesn’t need any involvement of third party.

***KEYWORDS:*** Data confidentiality; data integrity; data fragmentation; encryption; blockchain

## 1 INTRODUCTION

Cloud computing is a new emerging technology which offers easy to use software and data through internet that can be shared among different clients on pay per use demand. Cloud computing has gained popularity due to its compelling features and benefits that it offers like less up-front investment, lowering operating cost, fast deployment, dynamic scalability and automated self-provisioning of resources, architecture abstraction, pay-as-you-go model, low-cost disaster recovery, massive data storage solutions, easy access and less maintenance expenses, ubiquity (i.e., device and location independent) and the operational expense model. The important feature is the storage of massive data of different business organizations that can be shared among them. Cloud computing offers different services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Data Storage as a Service (DaaS) and Database as a Service (DBaaS).

There are many security issues and associated legal and regulatory concerns that have arisen as cloud computing emerges as a primary distributed computing platform and needs to be addressed. Cloud computing is different from traditional computing model in which users have full control of data storage and computation. Data security is one of the biggest challenge to the growth of cloud computing which needs to be addressed. This paper is concentrated towards issues related to security and privacy of data during storage of data in the cloud. Cloud computing is a distributed computing, which delivers highly scalable information technology (IT) services over the internet. Unlike traditional IT services, it delivers IT resources on demand without the need of any capital investment with pay-as-you-go pricing model. Some of the primal benefits of cloud computing are resource utilization, dynamic scalability of resources, virtualization of physical resources and automated self-provisioning of resources (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009; Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011; Hayes, 2008 [1]. In Recent years, database outsourcing or database as a service has developed as a new paradigm of cloud computing in which the organizations deploy their data on the cloud. They can access their data remotely via a web based interface through the internet regardless of their current locations. It offers tremendous opportunities to solve large-scale data storage problems. Companies like Amazon, Google, Microsoft and Rackspace are unleashing more vistas to host their databases, freeing clients from dedicating their own dedicated hardware and software to these databases while enhancing the ability to scale the databases into larger capacities (big data). The database service provider (DSP) takes the responsibility of procuring hardware and software, provisioning, performance tuning, backup and recovery, security and access control for clients. It lends reliable, and scalable data storage and management at a very low price (Curino et al., 2011; Hacigumus, Iyer & Mehrotra, 2002[2].

Nowadays, remote detection and monitoring of infectious and chronic diseases outbreaks in real time and it is needed to be controlled. Patients with various infectious diseases need regular monitoring , it is not possible for the patient to visit hospital for regular check-up and cannot monitor each patient regularly by doctor. So, a remote monitoring system is required to provide Healthcare support service for storing and processing health data. In the emerging cloud computing paradigm, electronic Healthcare system becomes increasingly motivated to cloud services like data management, data storage, data confidentiality, data privacy etc. Today , e-health care systems are so popular, a large amount of personal sensitive data for medical purpose are involved and people are understanding that the data should be authenticated and should not lose control in cyberspace. There are various reasons for keeping health data private and with limiting access. The Company may decide not to hire someone with particular diseases, may not provide life insurance knowing the disease history of a particular patient and discriminate socially. In this paper we have proposed work for sharing the health records and accessing them by the patients and physicians as authorized by the key control cryptography Blockchain scheme. The proposed system enables users to process the patient data without exposing patient privacy for example, if the patient is suffering from a chronic disease, the system create a private Blockchain cloud which used to store the data thus enabling the medical data should not be exposed without the permission of the patient.

Though the cloud data storage has many benefits over the traditional storage system, it has many security issues that put a barrier on the adoption of cloud storage service (Rayan, 2013; Chen & Zhao, 2012; Avram, 2014[3]. Cloud computing is the posterity of information technology provided the security issues and challenges are resolved. The various privacy concerns related to users, sensitive data stored in the cloud and data accesses are addressed in (Vimercati, Foresti & Samarati, 2013[4].

## 2 RELATED WORK

Cloud Security Alliance released a report " Top threats to cloud computing " in march,2010[5]and where they identified seven threats such asAbuse and Nefarious Use of Cloud Computing, Insecure Interfaces and APIs, Malicious Insiders, Shared Technology Issues, Data Loss or Leakage, Account or Service Hijacking and Unknown Risk Profile. The European Network and Information Security Agency published a report in November, 2009 where they identified eight top security risks such as loss of governance, isolation failure, compliance risks, management interface compromise,lock in, data protection, insecure or incomplete data deletion and malicious insider. Gartner in his survey has identified seven security issues that a cloud user should ask to cloud provider before using cloud com- puting services[6]. These are user access, Regulatory compliance, Data location, Data segregation, Recovery, Investigative support and Long-term viability. A group of researchers from the University of California at Berkeley identified 10 obstacles to the growth of cloud computing. These are Availability of Service, Data Lock-In, Data Confidentiality and Auditability, Data Transfer Bottlenecks, Per- formance Unpredictability, Scalable Storage, Bugs in Large-Scale Distributed Systems, Scaling Quickly, Reputation Fate Sharing and Software Licensing. Leavitt identified six challenges that are Performance, latency, reliability, Security and privacy, Related bandwidth
costs and Vendor lock-in and standard .

Borgmann et al. released a document " On the security of cloud storage services " in march, 2012 where they classified top five data storage security challenges[7]. These are Registration and Login, to protect against incrimination, information gathering and to enforce usage of strong passwords. (ii) Transport Security, to secure communication between client and server. Secure Deduplication, to avoid privacy problems when using deduplication. Chen and Jhao identified data security and privacy protection issues that occurred during all stages of data life cycle. Encryption, to disable the provider to examine stored data. Secure File Sharing, to protect documents shared by a closed group, optionally including non-subscribers.

Subashini and Kavitha described security issues existing in cloud service models such as IaaS, PaaS and SaaS[8]. They identified fourteen threats in Software as a Service(SaaS) delivery model such as Data Security, Data locality, Data integrity, Data segregation, Data access, Authentication and authorization, Data confidentiality , Network Security ,Web application security, Vulnerability in virtu- alization, Availability, Backup and Identity management . Khordhed explores the CSA top security threats and identifies the gaps and their existing solutions [10].

Goyal, Pandey, Sahai & Waters, 2006; Bethencourt, Sahai & Waters, 2007; Han, Mu, Susilo & Mu, 2013; Boneh, Boyen & Goh, 2005; Wang, Liu, Wu & Guo, 2011; Tebba, Hajji & Ghazi, 2012) used encryption technique[11]. They used encryption and decryption during the process of storage and retrieval of data. In this framework, a user sends a data to a client that translates the original data on unencrypted relations to a data that execute on encrypted relations to run on the server. The server executes the data and the results is passed to the client. The client anticipates the results and revert the results in plain text form to the user. Although data encryption provides a fine layer of protection against the disclosure of data, retrieving information from the encrypted database is very expensive and puts extra load on the server.

Matthias et al. (2013)[16] have given an idea of using multiple clouds to distribute the resources of a client in order to protect them from internal or external attacks. An idea of a secret sharing scheme was first proposed by Shamir (1979) in which a secret is divided into shares. A new approach based on a secret sharing scheme proposed by (Agrawal, Abbadi, Emekci, & Metwally, 2009); Emekci, Methwally, Agrawal, & Abbadi, 2014) in which sensitive data that needs to be kept confidiential is divided into shares and each share is stored on another DSP. In order to execute the query by a client, it is transformed into sub-queries and the relevant shares are restored from the database service providers and the original data is restructured and send back to the client. The database service providers are unable to deduce anything from the data they store and the user is able to perform queries on its database.

Encryption based techniques are very useful for hiding the sensitive data, but it bears a computation cost and carries the load of managing the keys. Moreover, it faces the performance of queries and encrypted data escalates the burden of computation on the . Another framework that completely different from encryption is based on fragmentation to shelter the confidentiality of data was first proposed in Ciriani et al., 2009[15]. The sensitive attributes are stored locally on the owner's side (trusted environment), while the sensitive associations are protected by splitting the attributes in such a way that at least one of the attribute is stored at owner side. The limitation of this technique is that the data owners have to manage the data on their side, hence put extra load on the data owner. However, to minimize the load of managing the data on the owner side, by downsizing the data stored at the owner site and proposed an algorithm that removes the storage at the data owner site (Ciriani et al., 2009).

Aggarwal et al., 2005)[14] instructed about the idea of partitioning the data into two fragments residing at two non-communicating independent servers. The idea behind this is to encode sensitive attributes to hide their contents and the sensitive associations are decomposed by using vertical fragmentation. However, the proposal is based upon the assumption that the two servers cannot interact with each other. A combination of encryption and fragmentation are used to satiate the confidentiality constraints. An improved approach based on multiple fragments without imposing any restrictions on the number of fragments was proposed in (Ciriani et al., 2010).

### Survey on data security threats to cloud computing

Data security is the most important issue to be addressed in order to promote the use of cloud computing. Data security is concerned with confidentiality, integrity and availability. Traditional data of each organization resides within the organization boundary and the organization itself is responsible for security and authentication of data. However, in the cloud computing service model, the sensitive data of an organization is stored outside the organization boundary and the control of the data is transferred to the hands of cloud providers. As a result, the data owner loose direct control to their data and is protected from certain attacks and accidents. Consequently, several data storage issues can arise. Typically, cloud users never know the exact location of their data nor other sources of data collectively stored with their data.

- Data Confidentiality refers to the ability to keep the data secret from cloud service provider (CSP) as well as from unauthorized users[26].Many organizations consider their sensitive data more precious than physical assets, so maintaining confidentiality of data in the cloud is a critical issue that needs to be resolved. In order to protect the data from CSP various approaches have been proposed, the outsourced data are either encrypted before outsourcing them so that only authorized users can view them or the data can be fragmented across several servers and stored in different locations.

- Data Encryption The privacy of data stored in the cloud which is under the control of CSP is a very vital issue and needs to be addressed. Ryan identified most serious threat to data confidentiality that comes from cloud provider because the data in the cloud can be accessed by the cloud provider. Therefore, to protect the data against internal or external attacks, all data needs to be stored on the servers in encrypted form so that the data remain confidential even in the event of a successful attack. When the data is encrypted and stored on remote servers using a private key which is known only to cloud provider. This may prevent data theft from external attackers but does not protect against malicious CSP. In order to prevent internal attacks, the data can be encrypted on the client machine before data is transmitted into the cloud and the key is only known to data owner (client). But this canlead to extra overheads and data can never be decrypted in the event of key is lost.

- Availability The SaaS application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture supported by a load-balanced farm of application instances, running on a variable number of servers , resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies in order to ensure the safety of the enterprise data and minimal downtime for enterprises. With Amazon for instance, the AWS API endpoints are hosted on the same Internet-scale, world-class infrastructure that supports the Amazon.com retail site and to mitigate DDoS attacks, Amazon maintains internal bandwidth that exceeds its provider-supplied Internet bandwidth. Standard Distributed Denial of Service (DDoS) mitigation techniques such as synchronous cookies and connection limiting are used. These assessments test and validate the availability of the SaaS vendor.

- Data access issue is mainly related to security policies provided to the users while accessing the data. These policies are set for a small business organization for using a cloud provided by some other provider for carrying out its business processes. Based on these security policies each employee can have access to a particular set of data, wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users (Blaze et al., 1999; Kormann and Rubin, 2000; Bowers et al., 2008). The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization.

- Authentication and authorization Most companies store their employee information in some type of Lightweight Directory Access Protocol servers. In the case of SMB companies, a segment that has the highest SaaS adoption rate, Active Directory seems to be the most popular tool for managing users.With SaaS, the software is hosted outside of the corporate firewall.Many a times user credentials are stored in the SaaS provider's databases this means SaaS customers must remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple SaaS products will increase IT management overhead. For example, SaaS providers can provide delegate the authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users.

Table 1: Significance and overview of existing research related to various security issues in cloud computing

| SSN | Tittle | Year | Published By | Type of security issue |
|---|---|---|---|---|
| 1 | Cloud computing and emerging IT platforms | 2009 | IEEE | Database outsourcing and Cloud computing offering different services |
| 2 | Top threats to cloud computing | 2010 | IEEE | Identified seven threats |
| 3 | IT Spending and Staffing Survey | 2005 | CIDR | Provided Distributed Architecture for Secure Database Services |
| 4 | A Distributed Architecture for Secure Database Services | 2005 | CIDR | Primary benefits of cloud computing |
| 5 | Relational cloud: A database-as-a-service for the Cloud | 2011 | CIDR | Reliable, and scalable data storage and management at a very low price |
| 6 | Cloud computing security: The scientific challenge | 2013 | IEEE | Described about the barrier in the adoption of cloud storage service |
| 7 | Managing and accessing data in the cloud | 2013 | CRISIS | Privacy, risks and approaches |
| 8 | Report on the security of cloud storage services | 2013 | IEEE | Classified top five data storage security challenges |
| 9 | A survey on security issues in service delivery models of cloud computing | 2011 | Journal of NCA | Identified fourteen threats in Software as a Service(SaaS) delivery model |
| 10 | A survey proactive attack detection in cloud computing | 2013 | Google Scholar | Gaps, Threat remediation challenges |
| 11 | Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data | 2006 | CCS | Use of encryption and decryption during the process of storage and retrieval of data |
| 12 | Cloud security issues | 2009 | IEEE | Identified data security and privacy protection issues that occurred during all stages of data life cycle |
| 13 | Secure and efficient access to outsourced data | 2009 | ACM | Instructed about the idea of partitioning the data into two fragments residing at two non-communicating independent servers |
| 14 | Combining Fragmentation and Encryption to protect Privacy in Data Storage | 2010 | ACM | Encoding sensitive attributes to hide their contents and the sensitive associations |
| 15 | Security and privacy-enhancing multicloud architectures | 2013 | IEEE | Distribute the resources of a client in order to protect them from attacks |
| 16 | The role of trust management in distributed systems security | 1999 | Springer | Secret Sharing |
| 17 | Ciphertext-policy attribute-based encryption | 2007 | IEEE | Use of multiple private keys for better security |
| 18 | Hierarchical attribute-based encryption | 2011 | Elsevier | Combining(HIBE)system and the CP-ABE system supporting "full delegation" |
| 19 | Privacy enhanced data outsourcing in the cloud | 2011 | Elsevier | Data Outsourcing |
| 20 | Secure overlay cloud storage with access control | 2012 | IEEE | Tree-based cryptographic key management scheme |
| 21 | Identity-based data storage in cloud Computing | 2013 | Elsevier | Characteristics of the user in the form of access policy |
| 22 | Security of information on a network using Blockchain | 2017 | IEEE | Overview of the Blockchain technology and its implementation |
| 23 | Blockchain technology in healthcare | 2016 | IEEE | e-Health Networking, Applications and Services |
| 24 | Privacy-Preserving Smart Contracts | 2016 | IEEE | Blockchain integrated cloud that incorporates a proof-of-stake |
| 25 | The blockchain-based digital content distribution system | 2015 | IEEE | Big Data and Cloud Computing |

Various encryption techniques are used most commonly is Attribute-based encryption which was firstly introduced by Sahai and Waters[19], in which they suggested that one's identity can be viewed as a combination of several attributes expressing the characteristics of the user in the form of access policy. They proposed attribute-based encryption that allows the specification of a decryption policy to

Table 2: Security and performance comparision between proposed model and related framework

| Type of security isues | Gartner | Borgmann | Kavitha | Bethencourt | Wang | Aggarwal | K.Lauter | Ryan | M.Zhou | Madhusudan |
|---|---|---|---|---|---|---|---|---|---|---|
| Data Confidentiality | Yes | No | Yes | Yes | Yes | No | Yes | Yes | No | Yes |
| Data Encryption | No | No | No | Yes | No | Yes | Yes | Yes | Yes | Yes |
| Data integrity | No | Yes | Yes | No | Yes | Yes | No | Yes | No | Yes |
| Data access | No | Yes | Yes | Yes | No | No | No | No | No | Yes |
| Authentication | Yes | Yes | Yes | Yes | Yes | No | No | Yes | No | Yes |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Authorization | Yes | Yes | Yes | Yes | Yes | No | No | Yes | No | Yes |
| Availability | Yes | Yes | Yes | Yes | No | No | No | Yes | No | Yes |
| Cryptography | No | No | No | No | Yes | No | Yes | Yes | No | Yes |
| Data Security | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Data Privacy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Fragmentation | N0 | No | No | No | No | Yes | No | No | No | No |
| Data Management | Yes | Yes | Yes | No | No | No | No | No | Yes | Yes |

be associated with a cipher-text. Each user in the system is provided with a decryption key that is associated with a tree-access structure that has a set of attributes associated with it. A user can then encrypt a message under a public key and a policy. Decryption will only work if the attributes associated with the decryption key match the policy used to encrypt the message.

J. Bethencourtet al.[19] introduced a system for Ciphertext-Policy Attribute Based Encryption. This system offers a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. This model allows policies to be expressed as any monotonic tree access structure and provide protection against collusion attacks in which an attacker might obtain multiple private keys.

S. Kamara and K. Lauter[20] proposed cryptographic storage service that provides data confidentiality and integrity protection. In this client process the data and decryption policy associated with it and generate decryption master key. The encrypted data is thensent to the cloud and decryption key resides with the client custody and is used to decrypt the data at the time of retrieval. It provides access only to authorized users for retrieving the data from the cloud. One limitation of this system is that the encrypted data can be shared among trusted clients only by sending the credentials (private key) to other clients. Moreover, major concern is the security of master secret key with the data owner.

Wang et al [21] proposed a tree-based cryptographic key management scheme ”owner- write-users-read” for data storages in the cloud. In this scheme, a single root node holds the master key that can be used to derive other node keys. Each node key can be usedto derive the keys of its children in the hierarchy. With their scheme, a data block stored in the cloud can be updated by a party who holds either the specific decryption key or a node key corresponding to one of its parents.

G.Wang et al [22] described a hierarchical attribute-based encryption (HABE) model, by combining the hierarchical identity based encryption (HIBE) system and the CP-ABE system supporting “full delegation” and “fine-grained access control over attributes”, respectively.

M.Zhou et al [23] proposed a practical application for private data management, name it as OWUR/W (owner-write-users-read/write) applications, where a data source protected with a node key in a key management tree can be shared with or managed by another party without compromising the security of the data encrypted with its child node's keys.

J. Han et al [25] discussed an identity-based data storage, where a proxy server re-encrypts ciphertexts for a requester based on his/her identity. In this model, the data owner encrypts his files and outsources them to the proxy server. He validates the requesters and issues access permissions to the proxy server. The proxy server stores the ciphertexts and can transfer them to ciphertexts for the requester when he obtains corresponding re-encryption keys from the owner. The requester can decrypt the re-encrypted ciphertext.

Y. Tang et al [24] proposed a secure cloud storage system that provides policy based access control to active data files are associated with a set of user-defined file access policies (e.g., time expiration, read/write permissions of authorized users), such that data files are accessible only to users who satisfy the file access policies. In addition, it generalizes time-based file assured deletion (i.e., data files are assuredly deleted upon time expiration, in which data files are assuredly deleted when the associated file access policies are revoked and become obsolete.

Sood [26] created an encryption model that uses SSL based 128-bit encryption to encrypt the data at the client end before transmitting them in the cloud. In this model, the data is classified according to three cryptographic parameters viz: confidentiality, integrity and availability. A message authentication code (MAC) is also generated and is transmitted along with encrypted data to the cloud. This model provides extra level of protection by allowing only those users to access the encrypted data stored in the cloud, who have valid user name and password. Since the data is encrypted at the client side and the encryption key resides with the data owner, the data is also protected from cloud provider.

The author Madhusudan Singh, Abhiraj Singh and Shiho Kim included various areas of cyberattacks and proposed the overview of the Blockchain technology and its implementation; then discussed the infrastructure of IoT which is based on Blockchain network and model has been provided for security of information on a network using Blockchain [33].

In this paper the author U. Mukhopadhyay, A. Skjellum “ Cloud computing for big data for monitoring, storage and analyze” presents importance of using cloud computing technology for big data processing collected from sensors [31].

M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in e-Health Networking [30] reviewed the blockchain related applications emerging nowadays, proposed the development of a secure framework and evaluation method for Blockchain. Security and Privacy of the personal health information have been identified by using Blockchain.

The author Rahul Shende, Shailesh Kamble , Sandeep Kakde suggested various details about cloud security , methods of encryp- tion and decryption techniques, and basic implementation of the blockchain [29]. It includes privacy protection for e-health data and protection of the personal information of the patients.

Deepak K. Tosh , Sachin Shetty , L aurent Njilla discussed design for Blockchain integrated cloud that incorporates a proof-of-stake based consensus protocol for securely recording the data operations occurring in cloud computing [28].

The author Madhusudan Singh, Abhiraj Singh and Shiho Kim included various areas of cyberattacks and proposed the overview of the Blockchain technology and its implementation; then discussed the infrastructure of IoT which is based on Blockchain network and model has been provided for security of information on a network using Blockchain [33]

## 3 CONCLUSION AND FUTURE WORK

As described in the paper, though there are several advantages in using a cloud-based system, there are yet many security and privacy issues that need to be resolved. Cloud computing is a disruptive technology in which the users access services based on their requirements without regard to where the services are hosted or how they are delivered. This survey report is based on the conceptualization of the cloud security based on real world security system where in security depends on the requirement and asset value of an individual or organization. For example, a normal human does not require personal security but a well known personality needs a body guard, an organization needs a set of security persons and a state or country have their mass military to safe guard their assets.Blockchain is a universal solution for all problems such as financial transactions, economic risks, security issues, big data platform, energy internet, smart city infrastructure, e- health, e- voting, food security and so on. It aim at the problems such as poor security of internet of things, difficulty in upgrading the equipment, high cost building and operating big data, poor flexibility in anti-attack ,the user privacy leakage and trading market mode. It not only reduces cost but reduce government workload, improves service efficiency, promotes urban health and sustainable development.

**References**

[1] Buyya, Yeo, Venugopal, Broberg & Brandic, 2009; Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011; Hayes, 2008

[2] Gomolski B., U.S. IT Spending and Staffing Survey, 2005, Gartner Research, 2005. Aggarwal, G., Bawa, M., Ganesan, P., Garcia-Molina, H., Kenthapadi, K., Motwani, R., Srivastava, U., Thomas, D. & Xu, Y. (2005). Two Can Keep a Secret: a Distributed Architecture for Secure Database Services. In Proceedings of the CIDR 2005, Asilomar, CA, 2005.

[3] Curino, C., Jones, E. P. C., Popa, R. A., Malviya, N., Wu, E., Madden, S.................. Zeldovich, N. (2011). Relational cloud: A database-as-a-service for the Cloud. In Proceedings of the CIDR, pp. 235–241, Asilomar, CA.

[4] Rayan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software, 86(9), 2263–2268. doi:10.1016/j.jss.2012.12.025

[5] Vimercati, S. D. C. D., Foresti, S., & Samarati, P. (2013). Managing and accessing data in the cloud: Privacy, risks and approaches. In Proceedings of CRISIS 2012, pp. 1 –9, Cork.

[6] Cloud Security Alliance. Top Threats to Cloud Computing http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[7] J. Brodkin. (2008). "Gartner: Seven cloud-computing security risks." Infoworld, Available: ¡http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1¿ .

[8] Borgmann M., Hahn T., Herfert M., Kunz T., Richter M., Viebeg U. & Vowe S. Fraunhofer SIT technical report on the security of cloud storage services, March 2012.

[9] Subashini S., & Kavitha V.(2011). Review: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1),1-11.

[10] Khordhed M.T., Ali A.B.M.S, Saleh A.Wasimi. Review: A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing . Future Generation Computer Systems , 28(1),833-851.

[11] Goyal, V., Pandey, O. , Sahai, A. & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In proceedings of the CCS 2006, pp. 89-98, NY, USA, 2006.

[12] Kandukuri BR, Paturi VR, Rakshit A. Cloud security issues. In: IEEE international conference on services computing, 2009, p. 517–20.

[13] Wang W, Li Z, Owens R, Bhargava B,"Secure and efficient access to outsourced data," In Proceedings of the 2009 ACM workshop on cloud Computing security, pp. 55–66,NY, USA, 2009.

[14] Aggarwal, G., Bawa, M., Ganesan, P., Garcia-Molina, H., Kenthapadi, K., Motwani, R.................... Xu, Y. (2005). Two can keep a secret:
A distributed architecture for secure database services. In Proceedings of the CIDR 2005, Asilomar, CA.

[15] Ciriani, V., Vimercati, S., De Capitani di, Foresti, S., Jajodia, S., Paraboschi, S. & Samarati, P.(2010). Combining Fragmentation and Encryption to protect Privacy in Data Storage. ACM Transactions on Information and System Security, 13(3), 1-30.

[16] Matthias Bohli, J., Gruschka, N., Jensen, M., Lacono, L. L., & Marnau, N. (2013). Security and privacy-enhancing multicloud architectures. IEEE Transactions on Dependable and SecureComputing,10(4),212–224.doi:10.1109/TDSC.2013.6

[17] Blaze M, Feigenbaum J, loannidis J, Keromytis AD. The role of trust management in distributed systems security, secure Internet programming, issues for mobile and distributed objects. Berlin: Springer-Verlag; 1999. p. 185–210.

[18] V. Goyal, O. Pandey,A. Sahai, and B. Waters,"Attribute-based encryption for fine-grained access control of encrypted data," In ACM conference on Computer and communications security, pp. 89-98, NY, USA, 2006.

[19] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute-based encryption," In IEEE Symposium on Security and Privacy, pp. 321-334.IEEE Computer Society, 2007.

[20] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, 2010

[21] Wang W, Li Z, Owens R, Bhargava B,"Secure and efficient access to outsourced data," In Proceedings of the 2009 ACM workshop on cloud Computing security, pp. 55–66,NY, USA, 2009.

[22] G.Wang, Q.Liu, J.Wu,M.Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," In Elsevier Journal of Computers and Security, vol. 30, pp. 320-331, 2011.

[23] M.Zhou, Y.Mu, W.Susilo, J.Yan, L. Dong,” Privacy enhanced data outsourcing in the cloud,” In Elsevier Journal of Network and Computer Applications, vol. 35, pp.1367-1373,2012.

[24] Y. Tang, P.P.C Lee, J.C.S Lui, ‘Secure overlay cloud storage with access control and assured deletion’, In IEEE transactions on dependable and secure Computing, vol 9(6), 2012.

[25] J.Han, Y.Mu, W.Susilo,Y.Mu, “Identity-based data storage in cloud Computing,” In Elsevier Journal of Future Generation Com- puter Systems, vol. 29, pp.673-681,2013

[26] Sood SK.(2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(1),1831-1838.

[27] Wang, G., Liu, Q., Wu, J. & Guo, M. (2011). Hierarchical Attribute-Based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers. Computers and Security, 30(5), 320-331.

[28] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua and L. Njilla, ”Consensus protocols for blockchain-based data provenance: Chal- lenges and opportunities,” 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York City, NY, 2017, pp. 469-474. A. E. Kosba, A. J. Miller, E. Shi, Z. Wen, and C. Papamanthou. “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” IEEE symposium on security and privacy, pp 839-858, 2016.

[29] J. Zhang, N. Xue, and X. Huang, “A secure system for pervasive social network-based healthcare,” IEEE Access, 2016..

[30] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on. IEEE, 2016, pp. 1–3.

[31] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, “A brief survey of cryptocurrency systems,” in 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2016, pp. 745–752.

[32] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, “The blockchain-based digital content distribution system,” in Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on. IEEE, 2015, pp. 187–190.

[33] Madhusudan Singh, “Perspective, Challenges, and Future of Automotive Security Enriched with Blockchain Technology”, IEEE Transportation Electrification Community WebinarAbstract,06 Dec, 2017.