J. Basic. Appl. Sci. Res., 4(1)54-59, 2014

© 2014, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied
Scientific Research
www.textroad.com

Insight into Security Challenges for Cloud Databases and Data Protection Techniques for Building Trust in Cloud Computing

Muhammad Yousaf Saeed, Adnan Tahir, Sheeraz Mughal, M.N.A. Khan

Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan

Received: July 23 2013
Accepted: August 26 2013

ABSTRACT

Data security has always remained a major issue in IT, but in cloud it is particularly of serious concern since data is scattered at different places all over the globe. The security concerns of users' needs to be rectified to make cloud environment trustworthy. In cloud computing, a trustworthy environment is the basic prerequisite to win confidence of a user to adopt such technology. Data protection and security are the two main foremost factors for gaining user trust and making the cloud successful. A number of data protections and data security techniques have been proposed in the contemporary studies in the field of cloud computing; nonetheless, there are still new avenues to further enhance data protection related techniques. The purpose of this study is to review different security techniques and challenges for securing and protecting data in the cloud and constitutes trust to make the cloud trustworthy. This paper presents a comparative research analysis of the existing research work done regarding the techniques used in cloud computing and brings out certain gaps. Finally, we bring some vital guidelines for gaining trust by securing data in the cloud.

KEY WORDS: Cloud Computing, Cloud Database Security, Database Encryption, Trusted Cloud Services, Data Privacy Policy, Data Protection.

1. INTRODUCTION

Cloud computing is generally known as on demand service. Cloud computing is an Internet based service which provides a new technique to use huge amount of shared resources. It is a flexible and potent service spreading its wings on IT industry at a very fast pace. It enables services to be consumed easily as and when needed. This archetype has developed substantial interest in the corporate sector and the academic world, and is changing the way to do business. The services of cloud computing are provided across the entire computing spectrum. Organizations with big infrastructures are moving and extending their business towards cloud computing to lower their cost and to free their best technology managers to focus on creating strategic differentiation. In this cloud, the ultimate consumers who use the services of cloud do not need anything to connect or equip themselves and their hardware with anything and they can have access to their data just through the Internet connectivity. There is a cloud service provider who facilitates services and manages those services in the cloud. The cloud provider facilitates all the services over the Internet and as a return the end users use services according to their business needs and pay the service provider accordingly. The concept of cloud includes a number of implementations, based on the services they provide. For instance, Google Apps Engine, Microsoft Azure, Eucalyptus, Amazon, Rackspace and Open Stack are some popular implementations of cloud computing by the world renowned companies. In addition, ACME Enterprise implemented VMware based v Cloud for permitting multiple organizations to share computing resources. Applied Materials developed a desktop cloud for CAD to get rid of the expense of changing out desktop PCs too often. "Apps.gov" is a website that provides cloud-based computing services to U.S. government agencies.

Cloud computing is the next generation paradigm in computation, which is continuously growing and emerging. Cloud computing is a new era of computing which refers to both the applications and resources delivered on demand over the Internet as services. The hardware and software resources in the data centers that provide diverse services over the network or the Internet to address the user requirements are called "cloud" [20]. According to National Institute of Standards and Technology (NIST), cloud computing provides *a convenient on demand network access to a shared pool of configurable computing resources* [19]. Here, resources refer to computing applications, network resources, platforms, software services, virtual servers and computing infrastructure. The cloud computing can be conceived as a new computing archetype with an implication for greater elasticity and availability at a minimal cost. The three well-known and commonly used service models in the cloud paradigm are IaaS, PaaS and SaaS.

The cloud is growing day by day as it provides high performance computational services to the users at cheaper rates. The Microsoft, Amazon, Google and Rakespace® are clouds giants. There are other types of different clouds.

[*] **Corresponding Author:** Muhammad Yousaf Saeed, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan. Email: yousafsaeed13@live.com,

Public cloud is the property of service provider and is used publically, private cloud refers to a property of any company, and hybrid cloud is the blends of public and private cloud. Most of the cloud services are being provided by large cloud service companies such as Google, Amazon, and IBM.

There can be three main types of cloud computing services which the provider facilitates with. These are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In SaaS, also known as software on demand, the software and its related data is spread on the cloud by the service provider and the user can access and use it through any web browser he/she works with. In platform as a service, the service provider facilitates the user with set of software. PaaS is also known as solution stack as a platform. In infrastructure as a service the cloud service provider facilitates the users with virtual machines, servers and storage to enhance their business capabilities. Like types of cloud services there are cloud types also which are private, public and a hybrid cloud. A private cloud is a cloud in which only the authorized users can use and access the services provided by the provider. In pubic cloud anybody can use the cloud services whereas the hybrid cloud contains the concept of both public and private clouds. Though cloud computing can save an organization's time and money but trusting the system is very much important because the real asset of any organization is the data which they share in the cloud to use the needed services either by putting it directly in the relational database, or eventually in a relational database through an application. Cloud computing brings a number of attributes that require special attention when it comes to trusting the system. The trust of the entire system depends on the data protection and prevention techniques used in it. Numerous different tools and techniques have been tested and introducedby the researchers for data protection and prevention to gain and remove the hurdle of trust but there are still gaps which needs attention and are required to be lined up by making these techniques much better and effective.

Data retrieval and data security protection is the major issue in cloud computing. The security of database is very important for both local machine and cloud-based environment. There are certain drawbacks linked to cloud computing. The major issues include security, resource management and resource monitoring. Additionally, there are no standard rules and regulations to deploy the cloud, and there is a lack of standardization in the cloud. From the security point of view, a number of novel techniques had been designed and implemented in cloud, but due to dynamicity of cloud environment these techniques fall short of ensuring total security. Though cloud cannot be made 100% secure, but security risks can be minimized to certain extent so that users can freely adopt it. This paper is based on reviewing and analyzing different available tools and techniques for data protection and prevention in the environment of cloud computing. Besides, this paper also critically analyzes and summarizes the emphasized techniques proposed in the prior published research work in the contemporary literature.

1. LITERATURE REVIEW

Cloud environment is being adopted at a large scale by many organizations. However, data security and data privacy are of prime concerns in cloud. For more flexibility and enhanced security, a hybrid technique which combines multiple encryption algorithms such as RSA, Triple DES (3DES) and Random Number Generator has been proposed in [1].Triple DES is particularly useful for encryption of block data and RSA is useful for establishing secure communication connection through digital signature based authentication. Pagano *et al.*[2] proposed an In-Memory Database encryption technique for privacy and security of sensitive data over un-trusted cloud environment. For this purpose, there should be a synchronizer between the owner and the client seeking access to the data. Client would require a key from the synchronizer to decrypt the encrypted shared data it receives from the owner. The purpose of the synchronizer will be to store the correlated shared data and the keys separately. A caveat with this technique is that the delay can occur due to the additional communication with the central synchronizer. However, this limitation can be mitigated by adopting group encryption and through minimizing communication between nodes and synchronizer.

Huang *et al.* [3] proposed a new asymmetric encryption mechanism which is applied to the databases in the cloud. The proposed technique follows the concept of commutative encryption and ElGamal encryption. The commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter. Re-encryption mechanism also takes place in the proposed scheme which shows that the cipher-text data is encrypted once again for duality. Such schemes are very useful in cloud applications where privacy is a key concern.

Alzain *et al*. [4] emphasize that most of the security issues related to data privacy in cloud computing have not been addressed yet. Integrity of data, intrusion and availability of service in cloud are of prime concern. To ensure data integrity, one option could be to store data in multiple clouds or cloud databases. For this purpose, Shamir's Secret Algorithm can be used. The data to be protected from internal or external unauthorized access is divided into chunks and Shamir's Secret Algorithm generates a polynomial function against each chunk. The processed data is then stored into different CSPs. Another alternative is to use a hybrid technique which uses both key sharing and authentication techniques [5] for data confidentiality and integrity. The connectivity between user and the CSP can be made more secure by utilizing powerful key sharing and authentication processes. RSA public key algorithm can be used for secure distribution of the keys between the user and CSPs. A three layered data security technique is proposed by Eman *et al.*[6]. The first layer is used for authenticity of the cloud user either by one factor or by two factor authentication. The second layer encrypts the user's data for ensuring protection and privacy. The third layer does fast recovery of data through a speedy decryption process.

Delettre *et al.* [7]introduced a concealment concept for databases security. Data concealment approaches merge real data with the visual fake data to falsify the real data's volume. However, authorized users can easily differentiate and separate the fake data from the real data. Such techniques somehow increase the overall volume of real data, but provide enhanced security for private data. The objective of data concealment is to make the real data safe and secure from malicious users and attackers. Watermarking method can serve as a key for the real data. Only the authorized user s have key of watermarking. Manivannam *et al.* [8] have proposed a lightweight mechanism for database encryption known as Transposition, Substitution, Folding and Shifting (TSFS) algorithm. However, as the numbers of keys are increased, the amount of computations and processing also increases.

Perveen *et al.* [9] has proposed a technique known as security as a service for securing cloud data. Like other services, this service would be available on demand. The proposed technique can achieve maximum security by dividing the user's data into pieces. These data chunks are then encrypted and stored in separate databases which follow the concept of data distribution over cloud. As each sub-piece of data is encrypted and separately distributed in databases over cloud, this provides enhanced security against different types of attacks. Asad *et al.* [10] describe the distribution of resources for cloud computing based on tailored active measurement. The main theme of this technique is based on network design, the specific routes for the incoming and outgoing traffic, and gradually changing the resources as per the needs of the user. Tailored measurement relies on the computing resources and storage resources. Due to the variable nature of networks, the allocation of the resources at a particular time based on tailored active method does not remain optimal. Due to variable nature of cloud, it possible that the resources may increases or decreases, and to counter this, we have to optimize changes in the user requirement either offline or online and the resource connectivity.

The cloud computing facilitates huge amount of shared resources on the Internet. Cloud systems should be capable of averting DoS attacks.Shen *et al.*[11]analyzed requirement of security services in cloud computing and suggest integrating cloud services for trusted computing platform (TCP) and trusted platform support services (TSS). The trusted model should bear characteristics of confidentiality, dynamically building trust domains and dynamic of the services. Normally, the cloud infrastructures require that user transfers their data into cloud merely based on trust.Neisse *et al.*[12]analysindifferent attacks scenarios on Xen cloud platform to evaluate cloud services based on trust. Security of data and trust in cloud computing is the key point for its broader adoption. Yeluri*et al.* [13]focused on cloud services from security point of view and explore security challenges in cloud when deploying the services. Identity management, data recovery and management, security in cloud confidentiality, trust, visibility and application architecture are the key points for ensuring security in cloud computing.

The overall picture of grid computing has been changed by cloud computing and distribution of data is a new way of cloud computing. The security challenges in the cloud include threats, dataloss, service disruption, outside malicious attacks and multi-tenancy issues [14].Chen *et al.* [15] analyse privacy and data security issues in cloud computing by focusing on privacy protection, data segregation and cloud security. Thedata security issues are primarily at SPI (SaaS, PaaS, IaaS) level and the major challenge in cloud computing isdata sharing.Cloud computing [16] provides a podium to use wide range of Internet-based services. But besides its advantages, it also increases the security threat when a trusted third party is involved. By involving a trusted third party, there is a chance of heterogeneity of users which affects security in the cloud. A possible solution to this problem could be to use a trusted third party independent approach for Identity Management to use identity data on untrusted hosts.

Squicciarini [17] has focused on problems of data leakage and loss of privacy in cloud computing. Different levels of protections can be used to prevent data leakage and privacy loss in the cloud. Cloud computing provides new business services that is based on demand. The cloud networks have been built through dynamic virtualization of hardware, software and datasets. Cloud security infrastructure and the trust reputation management play a vital role to upgrading the cloud services [18]. The Internet access security, server access security, program access security and database security are the main security issues in the cloud.

The inherent issues of data security, governance and management with respect to control in the cloud computing are discussed in [21]. The major issues in cloud data security are: data privacy, data protection, data availability, data location and secure transmission. The issue of storing data over the trans-boarder servers is a serious concern of clients as cloud venders are governed by the local laws and, therefore, the cloud clients should be cognizant of those laws. The data availability is also an important concern and service downtime must be according to the predefined SLAs. Moreover, the cloud provider should ensure the data security, particularly data confidentiality and integrity. The cloud provider should share all such concerns with the client and a build trust relationship in this connection. The cloud vender should provide guarantees of data safety and explain jurisdiction of local laws to the clients. The main focus in the paper is on those data issues and challenges which are associated with data storage location and its relocation, cost, availability and security.

The data confidentiality, authentication and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness [22]. A cryptographic algorithm named as Diffie-Hellman is proposed in [23] for secure communication, which is quite dissimilar to the key distribution management mechanism. Such a system normally consists of three modules: administration, authentication and encryption modules. Each module has different but interconnected functions. The administration module is used by the cloud provider for user registration and administration. While the authentication module is used for authentication of users, and encryption module is used for data encryption. The authentication realization is a two-way process. Firstly, the system requires the user to enter normal login and password, and then it generates one-time password and sends it on the user mobile for authentication. Once the one-time password is supplied, the system authenticates the user and grants access to the system. The system eliminates the cloud overload and prevents it from man in the middle attack.

Sun *et al.* [24] highlight the key security, privacy and trust issues in existing environment of cloud computing and help users to recognize the tangible and intangible threats associated with its use. According to the authors, there are three major potential threats in cloud computing, namely the security, privacy and trust. Security plays a vital role in current era of long dreamed vision of computing as utility. It can be divided into four sub-categories: safety mechanisms, cloud server monitoring or tracing, data confidentiality and avoiding malicious insiders' illegal operations and service hijacking. Furthermore, the authors highlight the importance of data privacy in cloud computing. It is a key point from user perspective; therefore, it is vital to understand its allied issues like user control over the data and legal jurisdiction requirements. Moreover, the trust is a complex relationship between cloud client and provider, and it should be planned prior to adopting the cloud milieu. The trust between cloud provider and client should be reliable and measurable to make the trustworthy decisions. The trust can be divided into four sub-categories: trust evaluation, trust relationship, trust degree and trust monitoring.

3. Motivation

The systematic investigation of the data protection techniques and security challenges being faced in the area of cloud computing in order to address these issues as a future work served as a motivation to conduct this research work. The study also helped us to understand the current state of the research in this area and helped establish facts and reach new conclusions.

4. CRITICAL EVALUATION

In this section, we provide summary of the critical review of the proposed techniques discussed in the previous section. The hybrid encryption technique proposed by Kaur [1] provides flexibility to the user by allowing them to use one or more algorithm altogether, however, with increase in the level of computation due to the selection of multiple encryption algorithms, the performance of query processing decreases. To technique proposed in [2] offers data privacy and security at row/column level of cloud database. Such a technique provides flexibility as well as data security by storing clients' data in the In-Memory Database while rest of data in the synchronizer. Likewise, Commutative Encryption which is a double encryption method is proposed by Huang [3] which provides enhanced security but at the computational cost. The concept of multi-cloud databases has been proposed in [4] for better data security purposes, but it is cost-intensive solution. Rao [5] proposed a centralized database security using two factor authentication which bears minimal cost.

Enhanced data security model based on a three layered architecture is proposed by Mohamed [6] which provides best encryption algorithm for data protection. Likewise, data concealment approach proposed in [7] adds fake data to the original data so that even if the data is stolen then still it remains meaningless to the stealer. A lightweight encryption model used in [8] is a good alternative for database security. Security as a service [9] can also be used to achieve maximum security by utilizing existing cloud resources and providing security on demand. To attain trust in cloud computing, Shen *et al.* [11] proposed a mechanism to integrate cloud service. The trust, data architecture, identity management, data protection, software isolation, and availability are the key area of interest discussed in [15]. A system for data encryption, authentication and data integrity is proposed in [19].

A summary of critical review of data protection techniques is provided in Table I below.

Table I. Critical Review of Data Protection Techniques

Ref #	Focused Area	Tools/Techniques	Merits	Demerits
[1]	Cloud Database Security	Hybrid Encryption Technique using RSA algorithm, 3-DES &Random Number Generation.	A user can use any combination of the algorithms.	Computation extensive.
[2]	Cloud Database Security	Row-level encryption for In-Memory DataBase. Uses synchronizer to store correlated shared data and keys separately.	Provides enhanced security by storing client's data in In-Memory DataBase while other appended data in Synchronizer	Delay occurs due to communication with the Synchronizer.
[3]	Database Security	Commutative Encryption based on ElGamal Encryption	Ensure integrity of cloud-database.	Requires more processing due to dual encryption.
[4]	Cloud Security	Concatenation of Shamir's Algorithm & Polynomial Function.	Ensure data integrity. Avoids intrusion.	Cost per unit time increases as number of shares increase.
[5]	Centralised Cloud Computing Security	Centralized Database security using RSA, Two Factor Authentication and TORDES algorithm.	Enhanced data protection. Minimal cost requirement.	This technique is only beneficial for small messages.
[6]	Security of Cloud Data	Enhanced Data Security Model for cloud that entails "Three Layer System Architecture".	Fast Encryption algorithm.	The user can only select the specific encryption techniques even if more powerful encryption techniques are available.
[7]	Security and Privacy of Cloud Data	Data Concealment in Cloud Database.	The proposed method can also be used for traditional databases.	The method lacks proper marking to the concealed data and fake data can be concatenated with the original data.
[8]	Database Encryption	TSFS algorithm with Only 3 Keys	Enhanced database security.	Proposed algorithm lacks handling special characters such as "@".
[9]	Cloud Security	Coprocessor and Data Distribution Technique in Cloud	Technique provides flexibility by providing Security as service model.	Technique does not support parallel processing.
[11]	Trusted Cloud Computing Platform	Trusted Module Platform, Trusted Services	Trusted cloud services help build trust in cloud computing.	There is short of mechanism for hardware to support trusted computing in cloud.
[13]	Cloud Computing	Amazon`s Cloud Platform, XML Signature, Browser Security	Highlights security issue at browser level.	Complex procedure is used for solutions.
[14]	Cloud Services	Trusted Chain for Computing	Proposed solution can help improve hardware security.	Proposed solution is limited to hardware protection.
[17]	Identity of Data Protection in Cloud	Management of Identity Systems	Identity Management system help secure data without using TTP services.	Solution implementation is challenging in the real world cloud data.

5. CONCLUSION ANDFUTURE WORK

The barrier and hurdles towards the rapid growth of cloud computing are the security and privacy issues associated with it. Reducing data processing cost is a mandatory requirement of any organization, but the data and information is always the asset and the backbone of any organization. No organization can transfer its data or information to a third party system until and unless a bridge of trust is build. A number of techniques have been proposed by the researchers for data protection and to attain highest level of data security, but there are still many gaps that need to be filled by making these techniques more effective. Lot more work is required in the area of cloud computing to make it acceptable by the clients. This paper highlighted different techniques for data protection in the cloud computing environments to build trust. Besides, this study also critically analyzed and summarized the highlighted techniques proposed in the prior published research. As a future dimension to this work, the research will be conducted for the improved, efficient and secured framework for data protection and prevention to gain trust in cloud computing by providing maximum data security.

Acknowledgment

The authors declare that they have no conflicts of interest in this research.

6. REFERENCES

[1] A. Kaur, and M. Bhardwaj, “Hybrid Encryption for Cloud Database Security,” International Journal of Engineering Science & Technology [IJESAT], *Cloud Database Security*, vol.2, pp.737-741, 2012.

[2] F. Pagano, and D. Pagano, “Using In-Memory Databases on the cloud, ”*Cloud Database Security,*vol.3, pp.30-37, 2011.

[3] K. Huang, and R. Tso, “A Commutative Encryption Scheme based on ElGamal Encryption,” Database Encryption*, vol.4,* pp.156-159, 2012.

[4] M. A. AlZain, B. Soh, and E. Pardede, “MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing”, *Cloud Security*, pp.784-791, 2011.

[5] A. K. Rao, “Centralized Database Security in Cloud,” International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol.1, pp.544-549, 2012.

[6] E. M.Mohamed, H. S. Abdelkader& S. EI-Etriby “Enhanced Data Security Model for Cloud Computing” 8th International Conference on INFOrmatics and Systems (INFOS2012), pp.12-17, 2012.

[7] C. Delettre, K. Boudaoud,& M. Riveill, “Cloud Computing, Security and Data Concealment,” IEEE Symposium on Computers and Communications (ISCC), pp.424-431, 2011.

[8] D.Manivannan,&R.Sujarani, “Light Weight and Secure Database Encryption Using TSFS Algorithm,” International Conference on Computing Communication and Networking Technologies (ICCCNT), pp.1-7, 2010.

[9] P. Ram, &Sivaasan, “Security as a Service (SaaS) as Securing User Data by Coprocessor and Distributing the Data,” IEEE Trendz in Information Sciences & Computing (TISC), pp.152-155, 2010.

[10] M. Asad, “A Framework for Resource Allocation Strategies in Cloud Computing Environment”*2011 35th IEEE Annual Computer Software and Applications Conference Workshops*, pp 261-266, 2011.

[11] Z. Shen, Li Li, Fei Yan, Xiaoping Wu, “Cloud Computing System based on Trusted Computing Platform”, International Conference on Intelligent Computation Technology and Automation (ICICTA), 2010.

[12] Ricardo Neisse, DominikHolling, Alexander Pretschner, “Implementing Trust in Cloud Infrastructures”, In: 11th IEEE/ACM International Symposium on Cloud and Grid Computing (CCGrid) 2011.

[13] Raghu Yeluri, Enrique Castro-Leon, Robert R. Harmon, James Greene, "Building Trust and Compliance in the Cloud for Services", In: Annual SRII Global Conference (SRII), 2012.

[14] AkhilBehl “Emerging Security Challenges in Cloud Computing", In: World Congress on Information and Communication Technologies (WICT), 2011.

[15] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012.

[16] RohitRanchal, Bharat Bhargava, Lotfi Ben Othmane, LeszekLilien, Anya Kim, Myong Kang, Mark Linderman, "Protection of Identity Information in Cloud Computing without Trusted Third Party", 29th IEEE Symposium on Reliable Distributed Systems, 2010.

[17] Anna Squicciarini, SmithaSundareswaran, Dan Lin "Preventing Information Leakage from Indexing in the Cloud ", IEEE 3rd International Conference on Cloud Computing (Cloud), 2010.

[18] Kai Hwang, Deyi Li, “Trusted Cloud Computing with Secure Resources and Data Coloring", IEEE Internet Computing, 2010.

[19] P. Mell and T. Grance, “The NIST Definition of Cloud Computing”, version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, www.csrc.nist.gov, 7 Oct 2009.

[20] N. Leavitt, “Is Cloud Computing Really Ready for PrimeTime?”, IEEE Computer, January 2009.

[21] Z. Mehmood, “Data Location and Security Issues in Cloud Computing”, International Conference on Emerging Intelligent Data and Web technologies, 2011, IEEE.

[22] D. H. Patil, R. R. Bhavsar, A. S. Thorve, “Data Security over Cloud”, International Journal of Computer Applications® (IJCA), 2012.

[23] RSA Laboratories, “The Diffie-Hellman key agreement protocol”, http://www.rsa.com/rsalabs/node.asp?id=2248.

[24] D. Sun, G. Chang, L. Sun and X. Wang, “Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environment”, Procedia Engineering, vol. 15, 2011, pp. 2852-2856.