IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

Hybrid crypto system for cloud storage security using MECC and Native bayes classifer A Review

P Munichandra Reddy

Department of Computer Science, S.V. University, Tirupathi, India

Corresponding Author: pmunichandrareddy@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si6.8790 | Available online at: www.ijcseonline.org

Abstract - The global ubiquity of cloud computing may expose consumer's sensing personal data to significant privacy and security threats. A critical challenge for the cloud computing industry is to earn consumers' trust by entering adequate privacy and security for sensitive consumer data. Regulating consumer privacy and security also challenges government enforcement of data protection laws that were designed with national borders in mind. In this paper, we present a hybrid cloud architecture which combines public cloud, private cloud computing and cryptography to minimize the bank's operational costs, maximizing the flexibility, scalability, availability and reliability of the services provided by the bank and guarantees the privacy, confidentiality and safety of the client's record. A smart card which contains a secret key is produced for each client upon creating a new account. A smart card which contains a pair of public/private keys is produced for each bank. A smart card which contains a secret key is produced for the auditor to decrypt the database of the banks' public/private keys for auditing purposes. The secret key is used to encrypt and decrypt the client's account data. The bank uses its public key to double encrypt the client's data that are temporarily stored in the bank's private cloud before being transmitted to be stored permanently in the public cloud. In order to perform any transaction on a client's account, the client's record must be retrieved from the public cloud and stored temporarily in the bank's private cloud in order to be decrypted with the bank's private key and then decrypted using the client's secret key in order to perform the required transaction in the private cloud.

***Keywords*—** Online banking, Hybrid cloud, Cryptography, Security

I. Introduction

Cloud computing emerges as a new computing paradigm that aims to provide reliable, customized and quality of service guaranteed computation environments for cloud users. 26 Applications and databases are moved to the large centralized data centres, called cloud 6. It requires customers to share, store, and process critical business data in the cloud, where they have little control today. Indeed, the ability to manage customer data in service provider environments in compliance with regulatory and corporate policies and in a transparent manner to service customers is identified as one of the main problems in SaaS adoption. Cloud computing is as important "to this decade PCs were to the 1970's, a technological and social leap that will change how businesses function, how cities are planned, how people carry out their work and what citizens expect from online services. Cloud computing is described in the popular press as the next big thing and a major technology disruption. It is likened and equated to the Industrial Revolution in terms of implications for technological innovations and economic growth. At the same time, the transformational nature of the cloud is associated with significant security and privacy risks. Cloud computing systems have recently emerged as a viable low-cost alternative to traditional computing platforms. This has sparked widespread interest, adoption, and/or research initiatives from all institutions alike.

Cloud computing is a new way of managing its infrastructure, applications and computer data over the Internet (VPN) by delegating administrative tasks of maintenance and supply of material resources to a third party (Cloud Computing provider), the only way to interact with data is an interface from their smartphone or computer, Cloud providers are essentially concerned by delivering services. Cloud computing has evolved as a popular and universal paradigm for service-oriented computing where computing infrastructure and solutions are delivered as a service1. The cloud has revolutionized the way computing infrastructure is abstracted and used. Cloud computing has captured significant portion of the competitive market today. Many organizations make use of cloud services. Although cloud computing services is growing and gaining popularity, the fear about the usage of cloud services is still an open issue. Various issues deterring adoption are identified in the literature; one of the major issues is security. Cloud Computing (CC) is one of the newest developments of the Internet. CC allows information technology and systems to be delivered and used externally over the Internet. This technology includes servers, personal computers, laptops, tablets, applications, telephones, smart phones, email and file storage.

Cloud computing is a model for enabling 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. Cloud computing refers to expandable and on demand services that are served via the Internet from specialized data centres. These services have a potential to enable and facilitate both formal and informal learning by allowing students and academics share learning resources, interact and brainstorm solutions, elaborate reports, and create conceptual designs. Cloud computing is clearly one of today's most enticing technologies, atleast inpart due to its cost-efficiency and flexibility. Several security issues in the cloud are impeding the vision of cloud computing asanew IT procurement model . IaaS cloud providers use different cloud solutions such as Openstack, Cloudstack or Amazon EC2 to provide a scalable environment. These solutions use hypervisors (such as Xen, KVMor VMWare) to offer virtualization and schedule access of guest Operating Systems (OSs) to physical resources such as CPU, memory or disk I/O. User Virtual Machines (VMs)instances are booted from OS images which are typically customized to be deployed in the cloud .

II. RELATED WORK

Salim Bitam *et al.* have proposed a Cloud computing is a network access model that aims to transparently and ubiquitously share a large number of computing resources. These are leased by a service provider to digital customers, usually through the Internet. Due to the increasing number of traffic accidents and dissatisfaction of road users in vehicular networks, the major focus of current solutions provided by intelligent transportation systems is on improving road safety and ensuring passenger comfort. Cloud computing technologies have the potential to improve road safety and traveling experience in ITSs by providing flexible solutions (i.e., alternative routes, synchronization of traffic lights, etc.) needed by various road safety actors such as police, and disaster and emergency services. In order to improve traffic safety and provide computational services to road users, a new cloud computing model called VANET-Cloud applied to vehicular ad hoc networks is proposed. Various transportation services provided by VANET-Cloud are reviewed, and some future research directions are highlighted, including security and privacy, data aggregation, energy efficiency, interoperability, and resource management.

R. Velumadhava Raoa *et al.*, have proposed a Cloud Computing trend is rapidly increasing that has an technology connection with Grid Computing, Utility Computing, Distributed Computing. Cloud service providers such as Amazon IBM, Google’s Application, Microsoft Azure etc., provide the users in developing applications in cloud environment and to access them from anywhere. Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. Providing security is a major concern as the data is transmitted to the remote server over a channel (internet). Before implementing Cloud Computing in an organization, security challenges needs to be addressed first. In this paper, we highlight data related security challenges in cloud-based environment and solutions to overcome.

To increase the profit, a semi-trusted cloud service provider may outsource the files of its client to some low expensive cloud service providers, which may violate the wishes of cloud users and impair their legitimate rights and interests. In this paper Tao Jiang, Xiaofeng Chena *et al.* , have proposed a probabilistic challenge–response scheme is proposed to prove that users’ files are available and stored in a specified cloud server. In our scheme, common cloud infrastructure with some reasonable limits, such as rational economic security model, semi-collusion security model and response time bound, are exploited to resist the collusion of cloud servers. Those limits guarantee that a malicious cloud service provider could not conduct a t-round communication in a limited time. The security and performance analysis demonstrate that our scheme provides strong incentives against an economically rational cloud service provider from re-outsourcing its clients’ data to some other cloud providers.

Cloud computing has emerged as a new computing paradigm that offers great potential for storing data remotely. Presently, many organizations have reduced the burden of local data storage and maintenance by outsourcing data storage to the cloud. However, integrity and security of the outsourced data continues to be a matter of major concern for data owners due to the lack of control and physical possession over the data. To deal with this problem, Mehdi Sookhaka, Abdullah Gania *et al.* , have proposed remote data auditing (RDA) techniques. However, the majority of existing RDA techniques was only applicable for static archived data and is not applicable for auditing or dynamically updating the outsourced data. They were also not applicable to big data storage because of the high computational overhead on the auditor. In this paper, we propose an efficient RDA technique based on algebraic signature properties for a cloud storage system that incurs minimum computational and communication costs. We also present the design of a new data structure-Divide and Conquer Table (DCT)—that can efficiently support dynamic data operations such as append, insert, modify, and delete.

Cloud computing is becoming increasingly important for provision of services and storage of data in the Internet. However there are several significant challenges in securing cloud infrastructures from different types of attacks. The focus of this paper Vijay Varadharajan *et al.* [20], have proposed a security services that a cloud provider could offer as part of its infrastructure to its customers (tenants) to counteract these attacks. Our main contribution is a security architecture that provided a flexible security as a service model that a cloud provider could offer to its tenants and customers of its tenants. Our security as a service model while offering a baseline security to the provider to protect its own cloud infrastructure also provides flexibility to tenants to have additional security functionalities that suit their security requirements. The paper describes the design of the security architecture and discusses how different types of attacks are counteracted by the proposed architecture. We have implemented the security architecture and the paper discusses analysis and performance evaluation results.

With the advent of cloud computing, individuals and organizations have become interested in moving their databases from local to remote cloud servers. However, data owners and cloud service providers are not in the same trusted domain in practice. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective database utilization a very challenging task. To address this challenge, in this paper, Jin Li, Zheli Liu *et al.* , have proposed L-EncDB, a novel lightweight encryption mechanism for database, which (i) keeps the database structure and (ii) supports efficient SQL-based queries. To achieve thoses goal, a new format-preserving encryption (FPE) scheme was constructed in this paper, which could be used to encrypt all types of character strings stored in database. Extensive analysis demonstrates that the proposed L-EncDB scheme is highly efficient and provably secure under existing security model.

For many companies the remaining barriers to adopting cloud computing services are related to security.One of these significant security issues is the lack of auditability for various aspects of security in thecloud computing environment. In this paper Hassan Rasheed *et al.* 22, have proposed look at the issue of cloud computing security auditing from three perspectives: user auditing requirements, technical approaches for (data) security auditingand current cloud service provider capabilities for meeting audit requirements. We have also divide specific auditing issues into two categories: infrastructure security auditing and data security auditing. We find ultimately that despite a number of techniques available to address user auditing concerns in the data auditing area, cloud providers have thus far only focused on infrastructure security auditing concerns.

III. METHODOLOGY

Security and privacy issues still pose significant challenges. In this chapter, we describe various service and deployment models of cloud computing and identify major challenges. In particular, we discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the proposed method in cloud computing deployment.

- Two main issues exist with security and privacy aspects of Cloud Computing loss of control over data and dependence on the Cloud Computing provider.
- These two issues can lead to a number of legal and security concerns related to infrastructure, identity management, access control, risk management, regulatory and legislative compliance, auditing and logging, integrity control as well as Cloud Computing provider dependent risks.
- A major concern regarding dependence on a specific Cloud Computing provider is availability. If the Cloud Computing provider were to go bankrupt and stopped providing services, the customer could experience problems in accessing data and therefore potentially in business continuity.
- Some widely used Cloud Computing services (e.g. GoogleDocs) do not include any contract between the customer and Cloud Computing provider. Therefore a customer does not have anything to refer to if incidents occur or any problems arise.

These are the main drawbacks of various existing works, which motivate us to do this research on Cloud Security.

IV. RESULTS AND DISCUSSION

In this research, we have intended to propose an efficient approach for providing very high secure storage data to the cloud system. At first the user is register their details in cloud and create their own user name and password and then gets the public and private key. If the user has already registered in cloud server he/she enter their user name and password and then login to the cloud server. For the purpose of accessing data from the cloud server, we will need a secure authentication. In authentication, the cloud server verifies the authentication of the user if the authentication is success the user will be connected to the server otherwise the server will negate the user request. Next process of our proposed method is to encrypt the file by using cryptography method. The goal of cryptography is to make data unreadable by a third party. In our proposed method Modified Elliptic Curve Cryptography (MECC) is used for the encryption. To improve the storage security of the proposed method, we use the steganography techniques after the encryption method. The goal of steganography is to hide the data from a third party. In our method we use linguistic steganography method is used to hide the data from the TPA. Here binary cuckoo search is used along with stenographic algorithm. Here we are combining both cryptography and steganography, in order to overcome the issues of cloud storage security. Then we split the data randomly and stored the data into cloud. To evaluate the secure data storage in cloud, we employ the intrusion detection system.

V. CONCLUSION AND FUTURE SCOPE

The aim of the intrusion detection system is to alert or notify the system that some malicious activities have taken place and try to eliminate it. In this work, I have planned to detect an instruction using Naïve bayes classifier along with Artificial bee colony optimization algorithm over cloud data. Here the input values will be taken for training. Subsequently, test data will be given to the trained network, which outputs if the data is intruded or not. Our method will be implemented in Cloud simulator in the working platform Java.

REFERENCES

[1] Jun Li, Bryan Stephenson, "*GEODAC: A Data Assurance Policy Specification and Enforcement Framework for Outsourced Services*", In Proceedings of IEEE Transaction in Services Compuitng, Vol. **4**, No. **4**, Oct 2011.

[2] Tristan Groleat and Helia Pouyllau, "Distributed Learning Algorithms for Inter-NSP SLA Negotiation Management", In Proceedings of IEEE Transaction on Network and Service management, Vol. 9, No. 4, Dec 2012.

[3] Nancy J. King, V.T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud", ELSEVIER Journal of Computer law & security RE, Vol. 28, No. 3, pp.308-319, June 2012.

[4] Nir Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution", ELSEVIER journal of Telecommunication policy, Vol. 37, No. 4–5, pp. 372-386, May–June 2013.

[5] Justin L. Rice, Vir V. Phoha, "Using Mussel-Inspired Self-Organization and Account Proxies to Obfuscate Workload Ownership and Placement in Clouds", In Proceeding of IEEE Transactions on Information Forensics and Security, Vol. 8, No. 6, pp. 963-972, June 2013.

[6] Lifei Wei a, Haojin Zhu, "Security and privacy for storage and computation in cloudcomputing", ELSEVIER Journal of Information Sciences, Vol. 258, pp. 371-386, Feb 2014.

[7] Gongjun Yan, Ding Wen, "Security Challenges in Vehicular Cloud Computing", In Proceedings of IEEE Transaction on Intelligent Transaction System, Vol. 14, No. 1, pp. 284-294, Mar 2013.

[8] Farrukh Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges,

Approaches and Solutions", ELSEVIER Journal of Procedia Computer Science on Applications of Ad hoc and Sensor Networks, Vol. 37, pp. 357-362, 2014.

[9] Maha TEBAA, Said EL HAJJI, "From Single to Multi-Clouds Computing Privacy and Fault

Tolerance", In Proceedings of IEEE International Journal of Future Information Engineering, Vol. 10, , pp. 112-118, 2014.

[10] Rizwana Shaikha, Dr. M. Sasikumarb, "Trust Model for Measuring Security Strength of Cloud Computing Service", ELSEVIER Journal of Advanced Computing Technologies and Applications (ICACTA), Vol. 45, pp. 380-389, 2015.

[11] Steve Jones, "Cloud computing procurement and implementation: Lessons learnt from a United Kingdom case study", ELSEVIER Journal of Information Management, Vol. 35, No. 6, pp. 712-716, Dec 2015.

[12] Changbo Ke a, Zhiqiu Huang a, "Supporting negotiation mechanism privacy authority method in cloud computing", ELSEVIER Journal of Knowledge Based Systems, Vol. 51, pp. 48-59, October 2013.

[13] Ibrahim Arpaci, Kerem Kilicer, "Effects of security and privacy concerns on educational use of cloud services", ELSEVIER Journal of Computer in Human Behaviour, Vol. 45, pp. 93-98, April 2015.

[14]Bharath K.Samanthula, YousefElmehdwi, "A secure data sharing and query processing framework via federation of cloudcomputing ", ELSEVIER Journal of Information Systems, Vol. 48, pp. 196-212, March 2015.

[15] Khaled Salah a, Jose M. Alcaraz Calero, "Analyzing the security of Windows 7 and Linux for cloud computing", ELSEVIER Journal of Computers and Security, Vol. 34, pp. 113-122, May 2013.

[16] Salim Bitam, Abdelhamid Mellouk, "Vanet-Cloud: A Generic Cloud Computing Model For Vehicular Ad Hoc Networks", In Proceedings of IEEE Wireless Communication, Vol. 22, No. 1, pp. 96-102, Jan 2015.

[17] R. Velumadhava Raoa, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", ELSEVIER Journal of Procedia Computer Science, Vol. 48, pp. 204-209, 2015.

[18] Tao Jiang, Xiaofeng Chena, "Towards secure and reliable cloud storage against data reoutsourcing", ELSEVIER Journal of Future Generation Computer Systems, Vol. 52, pp. 86-94, Nove 2015.

[19] Mehdi Sookhaka, Abdullah Gania, "Dynamic remote data auditing for securing big data storage in cloud computing", ELSEVIER Journal of Information Sciences, pp. 1-16, 2015.

[20] Vijay Varadharajan, Udaya Tupakula, "Security as a Service Model for Cloud Environment", In Proceedings of IEEE Transaction on Network and Service Management, Vol. 11, No. 1, pp. 60-75, March 2014.

[21] Jin Li, Zheli Liu, "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing", ELSEVIER Journal of Knowledge-based Systems, Vol. 79, pp. 18-26, May 2015.

[22] Hassan Rasheed, "Data and infrastructure security auditing in cloud computing environments", Vol. 34, No. 3, pp. 364-368, June 2014.