Secured Data Transmission in Cloud Environment with trusted party using authentication

A. Parkavi[*1], **R. Ramakrishnan**[*2]

*[*1]Department of Computer Science and Engineering, [*2]Asst Prof.,Department of MCA*
Sri Manakula Vinayagar engineering college, madagadipet, Pondicherry.

Abstract—**Off-site data storage is an application of cloud that relieves the customers from focusing on data storage system. However, outsourcing data to a third-party administrative control entails serious security concerns. Data leakage may occur due to attacks by other users and machines in the cloud. Wholesale of data by cloud service provider is yet another problem that is faced in the cloud environment. Consequently, high-level of security measures is required. In this paper, we propose Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE), a data security system that provides (a) key management (b) access control, and (c) file assured deletion. The DaSCE utilizes Shamir's (k, n) threshold scheme to manage the keys, where k out of n shares are required to generate the key. We use multiple key managers, each hosting one share of key. Multiple key managers avoid single point of failure for the cryptographic keys. We (a) implement a working prototype of DaSCE and evaluate its performance based on the time consumed during various operations, (b) formally model and analyze the working of DaSCE using High Level Petri nets (HLPN), and (c) verify the working of DaSCE using Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The results reveal that DaSCE can be effectively used for security of outsourced data by employing key management, access control, and file assured deletion.**

Keywords—**Data storage system, Data leakage, Employing key, File assured deletion.**

Introduction

Firstly, the pros and cons of different Attribute Based encryption methods are analysed. Secondly, a new encryption method based on Attribute Based Encryption (ABE) using hash functions, digital signature and asymmetric encryptions scheme has been proposed. This proposed algorithm is simplified yet efficient algorithm that can implemented for cloud critical application.

Cloud computing has emerged as a promising computing paradigm and has shown tremendous potential in managing the hardware and software resources located at third-party service providers. On-demand ac-cess to the computing resources in a pay-as-you-go manner relieves the customers from building and maintaining complex infrastructure s[1,10]. Cloud computing presents every computing component as a utility, such as software, platform, and infrastructure. The economy of infrastructure, maintenance, and flexibility makes cloud computing attractive for organizations and individual customers [2]. Despite benefits, cloud computing faces certain challenges and issues that hinder widespread adoption of cloud. For instance, security, performance, and quality are a few to mention [7, 10]. The development and operation of data storage sites is an on-going process in organizations. Off-site data storage is a cloud application that liberates the customer from focusing on data storage systems [7]. Representing system characteristics and capabilities as utility, causes the user to focus on aspects directly related to data (security, transmission, processing)[5,24]. However, moving data to the cloud, administered and operated by certain vendors requires high level of trust and security. Multiple users, separated through logical barriers of virtual ma-chines, share resources including storage space. Multi-tenancy and virtualization generate risks and underpins the confidence of users to adopt the cloud model [2, 3].

I. RELATED WORK

The authors employed a gate-way application in the enterprise to manage the integrity and freshness checks for the data. The Iris file system is designed to migrate organizations internal file system to the cloud. Moreover, a Merkle tree is used by gateway, which ensures freshness and integrity of data by inserting file blocks, MAC, and file version numbers at different levels of the tree. The gateway application also manages the cryptographic keys for confidentiality requirements. Moreover, Ref. [11] proposed an auditing framework that audits the cloud environment for ensuring the freshness of the data, data irretrievability, and resilience against disk failures. However, the technique depends on the user's employed scheme for data confidentiality. Moreover, data cannot be protected against service provider wholesale.

The client application generates a master key to be used for subsequent operations. The data processor encrypts the file to be uploaded with keys generated from the master key and uploads to the cloud. The data download involves the use of token generator that generates a token for the user to download data. Token also contains identity of files to be downloaded. The data verifier checks for the integrity of the data once the data is downloaded from the cloud. Attribute Based Encryption (ABE) is used for encryption. However, the key in [12] resides at client side and may be subject to a single point of failure.

A cloud storage system based on secure erasure code is presented in [15]. The system uses threshold key servers for storing a user's key generated by a system manager. User encrypts the data divided into blocks and stores eve-ry block on randomly selected multiple servers. The sys-tem also provides the functionality of data forwarding by allowing any of the users to forward the data to any other users without downloading. The authors used proxy re-encryption method for forwarding the encrypted data. A similar scheme is presented by the same authors in [14] with the difference that the later does not provide data forwarding. However, aforesaid schemes require heavy implementation level changes on the cloud side. The following section presents the operational mechanism of the FADE protocol followed by details of DaSCE.

A. Security Implications

Cloud solutions have new security implications for consideration. Organizations in different industries have divergent requirements regarding privacy and data retention. This means that the solution selected by an organization or an enterprise must be carefully evaluated to ensure that the selected services allow the organization to remaining compliance. International companies may need to comply with regulations that vary by country or economic region. These must also be taken into consideration by the IT professional when selecting a cloud-based service.

Managing security and compliance involves translating enterprise compliance requirements into a technology implementation. This requires practical skills and an understanding of implementing compliance within the deployed solutions. IT professionals will benefit from sharpening their security skills, including knowledge around data protection, privacy standards, and secure message integrity. Secure messaging may include topics such as encryption, digital signing, and malware protection. Additional skill sets of value include identity management, authentication methods, and auditing.

It is common to divide cloud computing into three categories:

Infrastructure as a service (IaaS), Which provides flexible ways to create use and manage virtual machines (VMS).

PLATFORM AS A SERVICE(PAAS),

Focused on providing the higher level capabilities more than VMS requires supporting applications.

Software as a service (SaaS), that applications that provide business value for users.

Deployment Models

For each cloud computing category there are additional decisions regarding the type of cloud chosen. The type of cloud that is selected determines the placement and usage model of the physical infrastructure that is being removed from the customer's datacentre world. Essentially, the cloud computing deployment model describes where the software runs and includes the following options:

- **A private cloud** is a set of standardized computing resources that is dedicated to an organization, usually on-premises in the organization's datacenter. It works with the current capital investment and delivers the new functions as a service.
- A**hosted private cloud** has a dedicated infrastructure hosted by a third party, inaccessible to other organizations.
- A**public cloud** consists of computing resources hosted externally but shared with other organizations and dynamically provisioned and billed on a utility basis — the customer will pay for what is used as they use it.

Keeping these categories in mind, the next sections of the whitepaper discuss the service models and explore the roles and skills IT professionals and developers need to invest in for each of them.

Cloud computing technology has been a new buzzword in the IT industry and expecting a new horizon for coming world. It is a style of computing which is having dynamically scalable virtualized resources provided as a service over the Internet. It reduces the time required to procure heavy resources and boot new server instances in minutes, allowing one to quickly scale capacity, both up and down, as ones requirement changes. Nevertheless the technology is hot in the market and is ready to cater to the small and medium business segment. As per one of the estimates from Gartner, by year 2012, 20% of enterprise market e-mail seats will be delivered via Cloud. As per another estimate from Gartner, Software as a Service is forecast to have a compound annual growth rate of 17% through 2011 for CRM, ERP and SCM markets in SMB segment. While the enterprises are exploring the possibilities of adopting this technology, it is imperative for these enterprises to critically evaluate the feasibility of this technology for their specific businesses.

The typical characteristic of this technology:

Cloud computing customers do not generally own the physical infrastructure serving as host to the software platform in question. Instead, they avoid capital expenditure by renting usage from a third-party provider. The entire onus lies on the service provider who owns the huge scalable and variable host of infrastructure, software and bundle of other services. Cloud computing consumers consume resources as a service and pay only for resources that they use. Many cloud-computing offerings employ the utility computing model, which is analogous to how traditional utility services (such as electricity) are consumed, while others bill on a subscription basis. Sharing "perishable and intangible" computing power among multiple tenants can improve utilization rates, as servers are not unnecessarily left idle (which can reduce costs significantly while increasing the speed of application development).

II. MODULES

Creating database:
1.A database is an organized collection of data. It is the collection of schemas, tables, queries, reports, views and other objects. The data is typically organized to model aspects of reality in a way that supports processes requiring information, such as modelling the availability of rooms in hotels in a way that supports finding a hotel with vacancies.

A database management system (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze data. A general-purpose DBMS is designed to allow the definition, creation, querying, update, and administration of databases. Well-known DBMSs include MySQL, PostgreSQL,Microsoft SQL Server, Oracle, Sybase and IBM DB2. A database is not generally portable across different DBMSs, but different DBMS can interoperate by using standards such as SQL and ODBC or JDBC to allow a single application to work with more than one DBMS. Database management systems are often classified according to the database modelthat they support; the most popular database systems since the 1980s have all supported the relational model as represented by the SQL language.

2. Uploading shared files:

In cryptography, **encryption** is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-randomencryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

3.Key searching

Search engines prominently use inverted indexing technique to locate the Web pages having the keyword contained in the users query. The performance of inverted index, fundamentally, depends upon the searching of keyword in the list maintained by search engines. This paper presents a new technique for keyword searching. It uses a trie data structure to index the keyword up to a certain optimum level. While searching a keyword, this index is used to get two offset values, in constant amount of time for every keyword, within which the keyword might lie. Using the two offsets, a binary search is initiated to locate the keyword in the list, and hence the Web pages containing the keyword. Research shows that subsequently increasing the levels of trie will increase the performance of retrieval but also increase the required memory. It also shows that on an average with indexing up to level 2 requires 56% less number of comparisons, as required by binary search, to search a keyword in the list.

4.Registering(decrypt)

Decryption is the process of converting encrypted data back into its original form, so it can be understood. Encryption and **decryption** should not be confused with encoding and decoding, in which data is converted from one form to another but is not deliberately altered so as to conceal its content.

5.Public keys

In cryptography, a **public key** is a value provided by some designated authority as an encryption **key** that, combined with a private **key** derived from the **public key**, can be used to effectively encrypt messages and digital signatures.

Proposed work

Multi-level Authentication Technique for Accessing Cloud Services

Cloud computing is an emerging, on-demand and internet-based technology. It provides variety of services over internet such as, software, hardware, data storage and infrastructure. This technology has been used by worldwide customers to improve their business performance. However, to utilize these services by authorized customer, it is necessary to have strict authentication check. At present, authentication is done in several ways: such as, textual, graphical, bio-metric, 3D password and third party authentication. This paper presents the strict authentication system by introducing the multi-level authentication technique which generates/authenticates the password in multiple levels to access the cloud services. In this paper, details of proposed multilevel authentication technique are presented along with the architecture, activities, data flows, algorithms and probability of success in breaking authentication.
Once they forget the username and password then they can easy to retrieve the data easily by using pass key.

A **password** is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access.

The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or *watchword*, and would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable

TV decoders, automated teller machines (ATMs), etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online.

Despite the name, there is no need for passwords to be actual words; indeed passwords which are not actual words may be harder to guess, a desirable property. Some passwords are formed from multiple words and may more accurately be called a passphrase. The terms **passcode** and **passkey** are sometimes used when the secret information is purely numeric, such as the personal identification number (PIN) commonly used for ATM access. Passwords are generally short enough to be easily memorized and typed.

Key word searching algorithm.

Search engines prominently use inverted indexing technique to locate the Web pages having the keyword contained in the users query. The performance of inverted index, fundamentally, depends upon the searching of keyword in the list maintained by search engines. This paper presents a new technique for keyword searching. It uses a trie data structure to index the keyword up to a certain optimum level. While searching a keyword, this index is used to get two offset values, in constant amount of time for every keyword, within which the keyword might lie. Using the two offsets, a binary search is initiated to locate the keyword in the list, and hence the Web pages containing the keyword. Research shows that subsequently increasing the levels of trie will increase the performance of retrieval but also increase the required memory. It also shows that on an average with indexing up to level 2 requires 56% less number of comparisons, as required by binary search, to search a keyword in the list.

REFERENCES

[1] M. ARMBRUST, A. FOX, R. GRIFFITH, A.D. JOSEPH, R. KTAZ, A. KONWIN-SKI, G. LEE, D. PATTERSON, A. RABKIN, I. STOICS, AND M. ZAHARIA, "A VIEW OF CLOUD COMPUTING," *COMMUNICATIONS OF THE ACM*, VOL. 53, NO. 4, 2010, PP. 50-58.

[2] M. S. BLUMENTHAL, "IS SECURITY LOST IN THE CLOUDS?"*COMMUNICA-TIONS AND STRATEGIES*, NO. 81, 2011, PP. 69-86.

[3] C.CACHINAND M.SCHUNTER, "A CLOUD YOU CAN TRUST,"*IEEESPECTRUM*,VOL. 48, NO. 12,2011,PP. 28-51.

[4] C. CREMERS, "THE SCYTHER TOOL: VERIFICATION, FALSIFICATION, AND ANALYSIS OF SECURITY PROTOCOLS." *IN COMPUTER AIDED VERIFICATION, SPRINGER BERLIN HEIDELBERG*, 2008, PP. 414-418.

[5]CLOUD SECURITY ALLIANCE HTTPS://DOWNLOADS.CLOUDSECURITYALLIANCE.ORG/INITIATIVES/CDG/ CSA_CCAQIS_SURVEY.PDF (ACCESSED MARCH 24, 2013).

[6] W. DIFFIE, P. C. V. OORSCHOT, AND M. J. WIENER, "AUTHENTICATION AND AUTHENTICATED KEY EXCHANGES,"*DESIGNS, CODES AND CRYPTOGRAPHY*,VOL. 2, NO. 2, 1992, PP. 107-125.

[7]M. Ali, K. Bilal, S. U. Khan, B. Veeravalli, K. Li, and A. Y. Zomaya, "DROPS: Division and Replication of Data in the Cloud for Opti-mal Performance and Security," *IEEE Transactions on Cloud Computing*, 2015, DOI: 10.1109/TCC.2015.2400460.

[8] N. En and N. Srensson, "An extensible SAT-solver," *Lecture Notes in Computer Science*, vol. 2919, Springer, 2003, pp. 502-518.

[9] C P. Gomes, H. Kautz, A. Sabharwal, and B. Selman, "Satisfia-bility solvers," *In Handbook of Knowledge Representation, Elsevier*, 2007.

[10] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud compu-ting: Opportunities and challenges,"*Information Sciences*,Vol. 305, 2015, pp. 357-383.

[11] A. Juels and A. Opera, "New approaches to security and availabil-ity for cloud data," *Communications of the ACM*,Vol. 56, No. 2, 2013, pp. 64-73.

[12] S. Kamara and K. Lauter, "Cryptographic cloud storage," *Financial Cryptography and Data Security*,Springer Berlin Heidelberg, 2010, pp. 136-149.

[13]M. Kaufman,"Data security in the world of cloud compu-ting,"*IEEE Security andPrivacy*,Vol. 7, No. 4, 2009, pp. 61-64.

[14] H. Lin and W. Tzeng, "A secure decentralized erasure code for distributed network storage," *IEEE Transactions on Parallel and Dis-tributed Systems*, vol. 21, no. 11, Nov. 2010, pp. 1586-1594.

[15] H. Lin and W. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, June 2012, pp. 995-1003.

[16] S. U. R. Malik, S. K. Srinivasan, S. U. Khan, and L. Wang, "A Methodology for OSPF Routing Protocol Verification," *12th Inter-national Conference on Scalable Computing and Communications (ScalCom)*, Changzhou, China, Dec. 2012.

[17] L. Moura and N. Bjrner, "Satisfiability Modulo Theories: An appetizer," *Lecture Notes in Computer Science*, Vol. 5902, Springer, 2009, pp. 23-36.

[18] T. Murata, "Petri Nets: Properties, Analysis and Applications," *Proc. IEEE*, Vol. 77, No. 4, pp. 541-580, Apr. 1989.

[19] A. Shamir, "How to Share a Secret," *Comm. ACM*, Vol. 22, No. 11, Nov. 1979, pp. 612-613.

[20]H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments,"*IEEE Security andPrivacy*, Vol. 8, No. 6, 2010,pp. 24-31.

[21] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 6, Nov. 2012, pp. 903-916.

[22]A. Yun, C. Shi, and Y. Kim, "On protecting integrity and confiden-tiality of cryptographic file system for outscored storage," *Proceed-ings of 2009 ACM workshop on cloud computing security CCSA'09*, pp. 67-76, 2009.

[23] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds," *IEEE Systems Journal*,2015,http:// dx.doi.org/10.1109/JSYST.2014.2379646.

[24] A. R.Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey of mobile cloud computing application models,"*IEEE Communica-tions Surveys and Tutorials*,2013,1-21.