International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Review: Enhancing Data Security in Cloud Computing with WEBOS using TSFS Algorithm

Pooja Saini[1], Kanchan Narula[2]

[1]Student, CSE, HCTM Technical Campus, Kaithal, India

[2]Assistannt Professor, CSE, HCTM Technical Campus, Kaithal, India

Abstract: ***The paper is about the study of the Cloud computing concepts which contains the different services such as the IaaS, PasS, SaaS and DaaS. There are so many other services offered by the cloud. But in cloud, the security of data is the main aim due to centralized information that is shared among the users and the examples of cloud provider are Google, Amazon, Salesforce.som and Microsoft etc. The data can be hamper include data leakage, insecure interface, sharing of resources, data availability and inside attacks. These services offered by internet and are on demand as the user required and these services are pay per use of it. The user can access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. This paper aims to be study the security algorithm about TSFS algorithm.***

Keywords: Cloud Computing, TSFS, IaaS, PasS, Saas, Webos

1. Introduction

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing has started to obtain mass appeal in corporate data centres as it enables the data centre to operate like the Internet through the process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner. The Cloud computing is a rapidly emerging distributed system paradigm that offers a huge amount of IT resources as utility services at a reduced cost and flexible schemes. The key of such flexibility is an efficient load balancer that offers better management and utilization of virtualized underlying cloud infrastructures. For a small and medium size business, the benefits of cloud computing is currently driving adoption. In the small and medium size business sector there is often a lack of time and financial resources to purchase, deploy and maintain an infrastructure (e.g. the software, server and storage). In cloud computing, small businesses can access these resources and expand or shrink services as business needs change. The common pay-as-you-go subscription model is designed for small and medium size business and easily adds or removes services.

Types of Cloud Services

Cloud computing offers a variety of ways for businesses to increase their IT capacity or functionality without having to add infrastructure, personnel, and software. There are seven different types of cloud computing and offer to businesses:

a. Web-based cloud services
These services provide the web service functionality, rather than using fully developed applications. For example, it might include an API for Google Maps, or for a service such as one involving payroll or credit card processing.

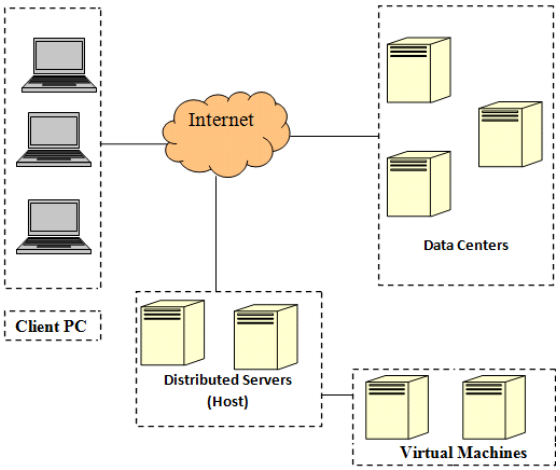

Figure 1: Cloud Components

b. IaaS (Infrastructure as a Service)
This service provides access to computing resource in a virtualized environment across a public connection through the internet. In the case of IaaS the computing resource provided is specifically that of virtualized hardware i.e. computing infrastructure. This includes such offerings as virtual server space, network connections, bandwidth, IP addresses and load balancers. Physically, the pool of hardware resource is pulled from a multitude of servers and networks usually distributed across numerous data centres. The client is given access to the virtualized components in order to build their own IT platforms. IaaS can be utilized by enterprise customers to create cost effective and easily scalable IT solutions where the complexities and expenses of managing the underlying hardware are outsourced to the cloud provider. If the scale of a business customer's operations fluctuate, or they are looking to expand, they can tap into the cloud resource as and when they need it rather than purchase, install and integrate hardware themselves.

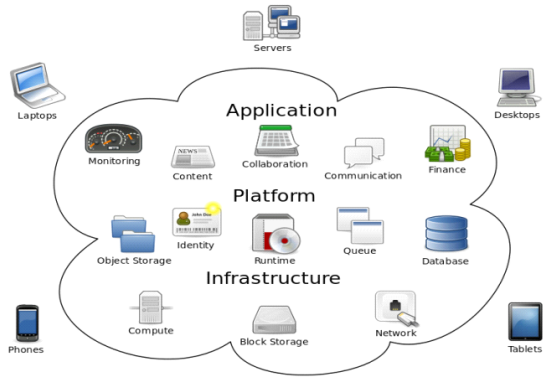

Figure 2: Cloud Computing Structure

c. SaaS (Software as a Service)
This provides a given application to multiple tenants (Users), typically using the browser. SaaS solutions are common in sales, HR, and ERP. SaaS is accessed by users using a thin client via a web browser. SaaS has become a common delivery model for many business applications, including office & messaging software, DBMS software, management software, CAD software, Development software, virtualization, accounting, collaboration, customer relationship management (CRM), management information systems (MIS), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management.

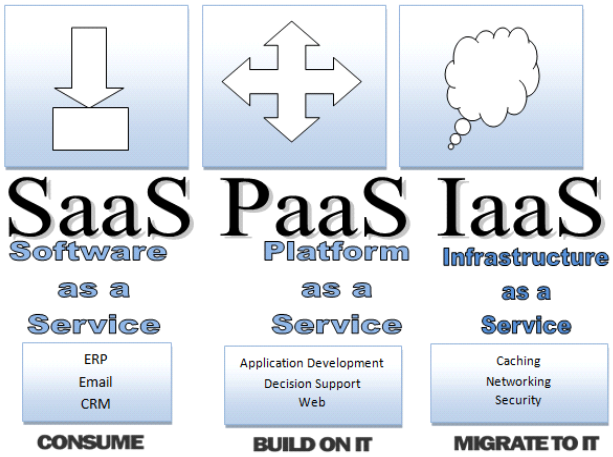

Figure 3: Implementation Architecture

Web OS

Web Operating Systems (WebOS) is a software platform that interacts with the user through a web browser and does not depend on any particular local operating system. Web operating systems are also commonly referred to as Web desktops or WEBTOPS. Web desktop or WEBTOPS is a virtual desktop on the web, running in a web browser as software. The WebOS functions much like a traditional operating system, although it doesn't include drivers for computer hardware. In cloud computing, users work with Web-based, rather than local, storage and software. These applications are accessible via a browser and look and act like desktop programs. With this approach, users can work with their applications from multiple computers. In addition, organizations can more easily control corporate data and reduce malware infections. Now, a growing number of organizations are adding to the cloud concept by releasing commercial and open source Web-based operating systems.

Desktop as a Service
Desktop as a Service (DaaS) solutions are emerging in parallel to Software as a Service(SaaS) solutions. A traditional workstation is mostly equipped with local computing resources such as data storage, processing capacity and applications. Desktop as a Service can be seen as a SaaS solution, bundling several computing resources in the form of a desktop while mimicking local computing resources, which in reality are residing on a remote server. In other words, Desktop as a Service is taking the SaaS value-proposition a step further.

DaaS offers a complete virtual working environment including applications, storage and related services that reside on the cloud on a remote server, but used locally. These are the most important perceived benefits of using DaaS:

Computing resources are presented on desktop interface that looks and feels like as if these resources would have been local

a) End-users of Desktop as a Service do not need to adapt to new ways of using computers
b) Location and hardware independent use of computing for greater flexibility and mobility
c) Computing resources can be scaled up and down easily, such as file and data storage, application availability and processing capacity.
d) Modifying, monitoring, managing and backing up data requires significantly less effort from IT staff
e) DaaS could cater for increased data security by the means of centrally managed data centers.

About the Algorithm

Enhanced TSFS (transposition, substitution, folding and shifting) algorithm uses four techniques of transformations, which are transposition, substitution, folding and shifting. There are many research studies in the database security field. Some of them have efficient implementations. Also, many encryption algorithms have been proposed, some of which have appealing features but still need further development, one such algorithm is the Transposition, Substitution, Folding and Shifting TSFS algorithm, known as the TSFS algorithm. The TSFS algorithm provides a high degree of security, using a number of features. However, it supports only numbers and alphabetic characters that are not enough to protect different types of sensitive data.

a. Transposition
Transposition transformation changes the location of the data matrix elements by using diagonal transposition that reads the data matrix in the route of zigzag diagonal starting from the upper left corner after getting the data and pads it with *s if it is less than 16 digits.

b. Substitution
The second algorithm is substitution transformation. It replaces one data matrix element with another by applying certain function. If the element represents an alphabetic character, it then will be replaced with another character. If the element represents a number, it will be replaced with a number and if it represents a symbol, it will be replaced with a symbol.

c. Folding
The third algorithm is folding transformation. It shuffles one of the data matrix elements with another in the same entered data, like a paper fold. The data matrix is folded horizontally, vertically and diagonally. The horizontal folding is done by exchanging the first row with the last row. The vertical one is done by exchanging the first column with the last column. The diagonal fold is done by exchanging the inner cells, the upper-left cell with the down-right cell and the upper-right cell with the down-left cell

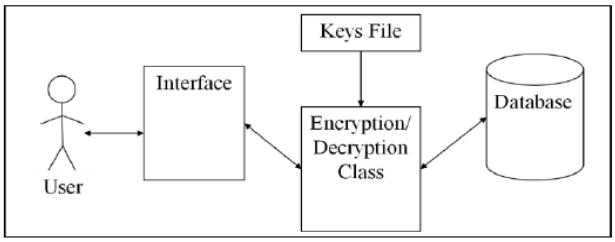

Figure 4: Implementation Architecture

d. Shifting
The last part of the algorithm is the shifting transformation, which provides a simple way to encrypt. We will use these four steps with our purposed algorithm to encrypt data. TSFS use 1 array while we will increase array size to achieve encryption which will also support special characters.

2. Literature Review

Author has been assimilated the knowledge about the Data Security and the issues occur during data privacy. Data encryption is an effective means of preventing the database during data storage and transmission. The idea of encryption is based on certain algorithm to transformed raw data (i.e. plain text) into a format that cannot be directly identified (i.e. cipher text), thus the person who does not know the decryption algorithm cannot obtain the data content [7].

This paper proposes an efficient symmetric searchable encryption to achieve in distinguish ability of indexes and trapdoors. Previous symmetric searchable encryptions are either insecure because their trapdoor generation algorithms are not probabilistic or inefficient because of the heavy cost due to pairing-based computation. Our searchable encryption is the first that satisfies both requirements of efficiency and indistinguishable (security). Furthermore, we introduce a limitation of the latest definition of indistinguishability for searchable encryption when each cell in the database is encrypted. We hereby define a new game for database usage and show that our scheme is provably secure in this new game [8].

At present, the security issue of large amount of computer data storage, sensitive defense data theft and tamper-proof issue has attracted people's attention increasingly. Database system as the core component of computer information system, database files as information aggregation, and their safety will be the top priority of the information industry. The core of information security is the database security, and database encryption security is one of the core questions of database security, compared with other safety means, in comprehensive consideration of safety degree, price, use maintenance costs, upgrade cost etc., the performance-price ratio of database encryption is the highest security means. This paper on database security, has discussed the application of database file in database security strategy and the related encryption technology, encryption algorithm and encryption method and data encryption technology [9].

In this paper, the author has been explained the concept of database encryption. But many companies are not willing to adopt the use of encryption in their existing DBs due to the degradation in performance. In this paper, they proposed and implemented a high speed database encryption model using Graphics Processing Units (GPU) that can perform parallel data processing. As a result, there was a performance improvement of about 40% to 60% compared to the CPU case. They expect our paper can be used to increase the encryption performance of database [10].

The author has been described the TSFS Algorithm. Database encryption is an important mechanism to secure databases from attacks and unauthorized access. The Transposition-Substitution-Folding-Shifting encryption algorithm (TSFS) is a symmetric database encryption algorithm that uses three keys with an expansion technique to provide high security: it improves the efficiency of query execution time by encrypting the sensitive data only [11].

3. Objectives

The proposed system will cover the following objectives:
1) To identify the security challenges and suggest some counter measures for the future challenges to be faced in Cloud Computing.
2) To improve the security issues in webOS & eyeOS which are the base of cloud computing by using AJAX
3) To Design an effective algorithm for more security in Web OS.
4) To implement the proposed algorithm to see the results outcome.
5) To Generate Results.

4. Proposed Methodology

API's are the interfaces that customers use to interact with cloud services, for secure processing, interfaces must have secure verification, access control, encryption mechanisms especially when third parties start to build on them. For this purpose we need to analyse.

- Security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in performance with encrypted transmission.
- Understand the dependency chain associated with the API. Furthermore when data deleted without any backupor encoding key loss/unauthorized access, data is always in danger of being lost or stolen.

To provide solution for this, we need to:

- Implement fault free API access control.
- Mechanism used for encryption and protection of data should be secure.
- Data protection analysis done at both design and run time.
- Provider backup and preservation strategies must be defined.

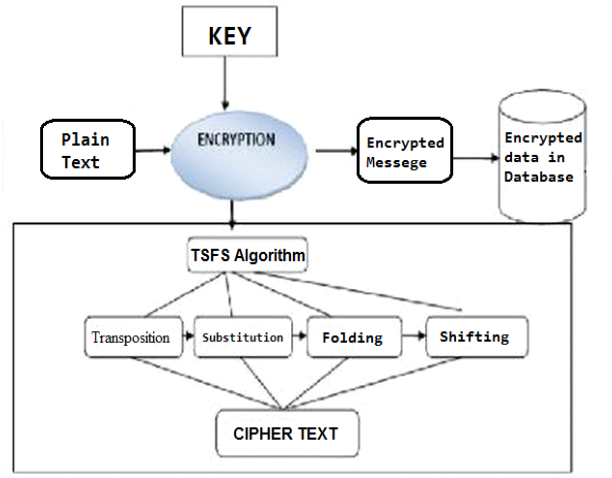

Figure 5: Data Encryption using TSFS

We focus on summarized details of what cloud computing is, its various models regarding to services and deployment ,main security risks and issues and to propose a possible solution that will provide more security to data of customers from that are currently present within the cloud computing services.

Security Issues in Cloud Computing

Abuse and Nefarious Use of Cloud Computing: Abuse and nefarious use of cloud computing is the top threat identified by the Cloud Security Alliance. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

Insecure Application Programming Interfaces: As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

Malicious Insiders: The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or

how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

Data Loss/Leakage: Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.

Account, Service & Traffic Hijacking: Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of service attacks.

5. Conclusion and Future Work

In this paper, we have been proposed the Data Security issues and algorithm for secure the Cloud Data. The objectives have been defined for handle the security problem. The proposed work will be elaborated in the research paper with the Data Security techniques. The TSFS Algorithm steps encrypt the information with four steps such as transposition, Substitution, Folding and Shifting.

References

[1] Kaur, K. ; Dhindsa, K.S. ; Singh, G. (2009), “Numeric To Numeric Encryption of Databases: Using 3Kdec Algorithm”, Advance Computing Conference, 2009. IACC 2009. IEEE International, Publication Year: 2009 , Page(s): 1501 – 1505.

[2] Zhu Yangqing ; Yu Hui ; Li Hua ; Zeng Lianming (2009), “Design of a New Web Database Security Model”, Electronic Commerce and Security, 2009. ISECS ‘09. Second International, Publication Year: 2009, Page(s): 292 – 295

[3] D. Manivannan, R .Sujarani, (2010) Light weight and secure database encryption using TSFS algorithm.

[4] Wu Xing-hui ; Ming Xiu-jun, “Research of the Database Encryption Technique Based on Hybrid Cryptography”, Computational Intelligence and Design (ISCID), 2010 International Symposium, Publication Year: 2010 , Page(s): 68 – 71

[5] Jiang Yu-yan ; Pi Xiao-yan ; Xing Guo-Zheng , “Database Encryption and Confirmation Mechanism Research”, Multimedia Technology (ICMT), 2010 International Conference, Publication Year: 2010 , Page(s): 1 – 4.

[6] Jacob, S. (2010), “Cryptanalysis of a fast encryption scheme for databases”, Information Theory Proceedings (ISIT), 2010 IEEE International, Publication Year: 2010, Page(s): 2468 – 2472

[7] Zhao Yong-Xia, "The Technology of Database Encryption Multimedia and Information Technology (MMIT)", 2010 Second International Conference, Publication Year: 2010 , Page(s): 268 – 270.
[8] Yoshino, M. ; Naganuma, K. ; Satoh, H., "Symmetric Searchable Encryption for Database Applications", Network-Based Information Systems (NBiS), 2011 14th International, Publication Year: 2011 , Page(s): 657 – 662.
[9] Yanhua Pan, "Research on network database encryption technology", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International, Publication Year: 2011 , Page(s): 690 – 693
[10] Inkyung Jeun ; Hyun-Chul Jung ; Nan Ki Lee ; Dongho Won (2012), "Database Encryption Implementation and Analysis Using Graphics Processing Unit", Mobile, Ubiquitous, and Intelligent Computing (MUSIC), Page(s): 109 – 113.
[11] Hanan A. Al-Souly, Abeer S. Al-Sheddi, Heba A. Kurdi.,(2013) Lightweight Symmetric Encryption Algorithm for Secure Database.