Data Encryption Scheme for Large Data Scale in Cloud Computing

Mehdi Ebady Manaa, Moahmmed Ali Mohammed A
University of Babylon, College of IT, Department of Information Network
meh_man12@yahoo.com

***Abstract*—Cloud computing is a power full platform to deliver applications over the internet or a private network. It considers the next technology in data manipulating and retrieving. These technologies help to manage and manipulate data in various services and deployment models. The cloud services are delivered from cloud computing providers to the users in a manner of leased service which give users an ability to lease services in a specific scope. To handle the huge data in today's scenario, data cloud storages is suggested which gives a big relief for users as in local machines. Data protection is one of the most important issues in cloud computing. The researchers present many techniques, for data protection and security schemes such as Intrusion Detection Systems (IDS's), Access Control, Encryption and Secure Socket Layer (SSL), but the data security is still a challenging issue. The goal of this paper is to present the security techniques for cloud computing in different cloud services model. Furthermore, we propose a security data encryption technique for cloud services in SaaS model for large data scale. Salesforce.com SaaS service model provides a good tool for the users to register in the cloud and develop their applications.**

***Index Terms*— Cloud Computing; Cloud Data Storage; Data Protection; Salesforce; Security Challenges.**

I. INTRODUCTION

Cloud computing has been developed as the next generation of IT paradigms which offers dynamically scalable resources and cloud services over the internet [1]. Cloud computing include a group of interconnected computers over the world that is jointly used to reduce time, cost, to share storage and computing for the organization and companies. Formally, cloud computing is defined by National Institute of Standards and Technology (NIST) that : "Cloud computing is a model for enabling ubiquitous, 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" [2]. Many organizations invested in cloud computing to provide resources, storage, to access software and data from cloud such as Google, Cisco, Sun, Intell, Oracle, Amazon, IBM, Dell and HP [3].

Cloud computing simply means an internet computing that provides services over the Internet through the large data center and efficient servers. Web and cloud services are hosted on these servers to reduce the time and satisfying the scalable. Cloud computing is still suffer from many challenges regarding the data protection and data storage such as loss control, disruption of the service, data loss and attacks. The main factors for information security are Confidentiality, Availability and Integrity (CIA). The confidentiality means to protect the data from unauthorized access, availability ensures access to data by authorized user when required, and Integrity means consistency of the information losing any factor of these security criteria can cause harm for organization and loss of customer confidences [4].

II. LITERATURE REVIEW

Cloud computing considers the next generation of IT paradigms. The organizations tend to employ cloud resources due to inexpensive and scalability. Many researchers explore the security techniques and challenges in cloud computing. Manas Jog. And M. Madiajagan present a survey on the different types of security techniques to achieve trusted cloud at the layer Infrastructure as a Service (IaaS). International standard hardware is presented in the cloud to implement trusted computing using the Trusted Platform Module (TPM). The open platform for security and network access is designed using the Trusted Network Connect (TNC). However, the system administrator control on network access based on device health and identity [5].

Security on each cloud layers is examined by [6].They show that the vulnerabilities in IaaS layer are less common compared to other layers. In PaaS layer, the virtual machine included in this layer must be protected against unauthorized access of Trojan and malware where it is necessary to perform the examination at regular intervals to protect the cloud infrastructure from harmful software. The SaaS layer could provide access to the confidential information by unauthorized persons. Data hiding approach method is proposed as a security technique to protect data on cloud computing storage.

Tangavel, Varalakshmi, and Sridhar show a comparative study for privacy preservation in the cloud data storage. The study discusses many security techniques in cloud to provide a reliable security service where the privacy of data in transmitting and rest should be ensured. The study concludes many techniques such as access control, cryptography, attributes based encryption, key management services, identity-based, and proxy-based access control are ensuring the privacy in cloud storage [7].

Slawomir and Peter M. present Zero Knowledge Proof (ZKP) authentication approach to allow the user to transfer the service and rights within a trusted environment for home networks. The system is presented within a human level in a trusted environment, but there are risks from attackers who abuse the trusted environment and shutdown the system such as hi-jack attack [8]. Irish …etc designed a novel framework for the cloud using CCMP "(Counter with

Cipher Block Message Authentication Code Protocol" for secure data storage and management in cloud service [9].

Thu, Huaglory, and Quentin presents root kit and malware detection system to protect underlying virtualization platform in cloud computing against cyber-attacks. They use a hash function and Support Vector Machine (SVM) classifier with VMI (Virtual Machine Introspection). The SVM classifier allows for quick attack detection in offline phase [10].

III. Material and Method

Cloud Computing Service Models The cloud computing provides service over the Internet for organization and companies by using three main service models (Saas, PaaS, and IaaS) [2][11][12].

- *Software as a Service (SaaS)*
  It is the first layer of cloud computing which focuses on the end-user requirements and sometimes referred as "on-demand Software". In this model, all the application and service is accessed through web-based (browser) by the users. The SaaS model infrastructure (Hardware/Software) is managed and controlled by the service provider. Examples of SaaS model are Salesforce.com, Facebook, and YouTube.
- *Platform as a Service (PaaS)*
  In this model, all the application and services are controlled and managed by the clients. Actually, the cloud infrastructure (hardware, software, and O.S) are managed by cloud provider with higher level of abstraction. The users do not necessary know about their platforms. Google App and Microsoft Azure are examples of PaaS.
- *Infrastructure as a Service (IaaS)*
  This model provides to users physical data centers (servers and networks) to install and manage their O.S and applications. The user has full control over the storage, application and operating systems. It is considered the bottom level of cloud computing layers. Examples of IaaS model are Amazon and GoGrid.

Cloud deployment models. they are categorized into public, private, hybrid, and community depending on company policies in term of cost and sharing.

- *Public cloud*
  it is used to share resources for general public purpose "pay-as-you-go". It may be managed and controlled by the government organization. The users are not aware of the users that sharing the cloud.
- *Community cloud*
  It may be managed and controlled by a group of users companies to share policies and security requirements.
- *Private cloud*
  It is established to serve one company or organization.
- *Hybrid cloud*
  It results from one or more cloud (private, community, and public). Figure 1 shows the cloud services layers and deployment models.

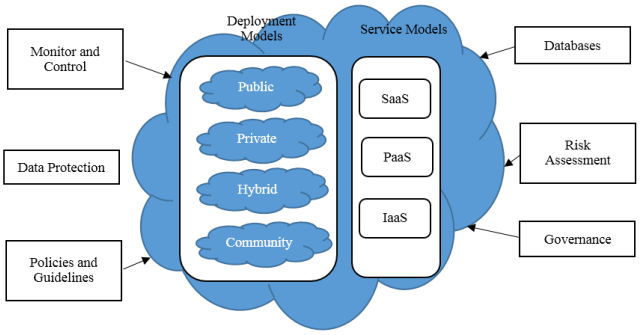

Figure 1: Cloud deployment and service models

There are many essential characteristics of the cloud model. These characteristics are listed in NIST as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Security in Cloud Computing: Hackers try to access cloud services in the unauthorized way and to steal a sensitive information for an unauthorized way. Table (1) shows the main threats that may expose the cloud resources.

Table 1
Cloud Main Threats

Threat Name	Description
DDoS Attack	This attack jeopardizes the three security criteria by sends a bogus packet to shut down the service on the victim [13]. In cloud computing, the attacker tries to register as authenticated user and then employs many handlers to send the bogus packets in short time due to the power computational resources that is available in the cloud.
Web browser attacks	These attacks try to access the cloud resources either internally or externally. It exploits the authorization, authentication, malware injection, and account vulnerability [14].
Viruses and Trojan horse	Viruses attach itself to program or file that may damage hardware, software, and files. Trojan horse is a malicious code seems to be trusted for the first time and then runs in the victim which causes serious damage by deleting files and destroying information on the system. Trojan and viruses can be uploaded to cloud and cause damage [15].
Brute-force attack	This attack is a technique that used to break the password. It depends on power computing capability that needs thousands of possibility to be sent to a victim account until it finds the success access. Cloud computing provide a perfect platform to run this attack [16].
SQL Injection	SQL injection attack is one type of malicious code that use to inject of SQL query using botnet attack to exploit cloud resources. The successfully inject attack exploits the administrator's privileges to update, insert and delete the sensitive information. The attacker is remotely executing system command and takes control for DBMS (Data Base Management System) for further criminal [17].
Cross-Site Scripting attack	Cross-site Scripting attacks (XSS) is one type of the computer security breaches by FireHost client's web application [18]. Hackers to different malicious code using VBScript and JavaScript into an infected web page to execute the scripts on victim's web browser.
Man-in-the-Middle attack	The attacker tries to intrude the conversation between the cloud clients and cloud services to inject a false information and to access the protected data [19].
Sniffer Attack	The attacker tries to launch malicious code by application to capture the networking ongoing traffic and read the unencrypted packets.
Data loss / leakage	It is happened by unauthorized access or deleting data without backup. The attacker may access to encoding key and reveal the information [20].

IV. ATTACKS COUNTERMEASURES IN CLOUD COMPUTING

Cloud computing includes an essential information that need to protect against unauthorized access. Attack countermeasures in cloud are presented in the following:

1. Data Encryption
   The users transfer and receive data from cloud that exploits from attackers. These data need to encrypt using different encryption algorithms, hash function and key management in transit and receive.

2. Backup and Recovery
   It is an essential countermeasure in case of disaster and errors. Backup process is used by many organizations that make deal with cloud provider.

3. Access Control
   The Intrusion Detection System and firewall are used to protect the cloud services for illegal access.

4. Using Authentication Scheme in cloud service

5. Monitoring Mechanism
   Many tools are used to monitor and analysis the cloud traffic such as DSniff, Cain, Ettercup, WSniff, and Airjack.

6. Cloud Architecture
   Cloud providers need to make cloud assessment, management of secure access, network scanning and storage security.

7. Filtering Schemes
   Cloud filtering techniques is used to check the user input against SQL injection such as proxy-based architecture and SQL control sequence. In another way, Active content filtering, content-based data leakage, preventing techniques and web application vulnerability detection scheme are used to prevent XSS attack.

8. Cloud Data Encryption
   Cloud data encryption includes many techniques that translate data into another form where only people with authorized access key can read it. Many encryptions mechanism can be used to protect data cloud. The RSA, Triple DES, AES, BlowFish, and TwoFish, quantum key distribution, and honey encryption are prompting techniques to protect data in cloud computing [21]. These techniques provide privacy and confidentiality for cloud service and some time we can combine these techniques with other technique to reduce time complexity. One of these platforms are man/ reduce technique which can be implemented in cloud SaaS platform such as www.salesforce.com. Combining Map/reduce technique with AES encryption in cloud computing will result in a powerful capability in data encryption.

V. MAP / REDUCE TECHNIQUE IN CLOUD FOR LARGE DATA SCALE

Map/ Reduce technique is a promising tool to implement and process a large data scale in a parallel and an efficient time. It was introduced to handle the execution of parallel jobs. It was implemented by Google to use Map/Reduce functions to process a large amount of web data in a parallel way. The general framework of the map/ reduce is as follow: the map stage takes the input from the distributed file and produce a sequence of (key, list[values]) pairs. In the second stage, it aggregates the mapper output to the related reduce function. The map output sorts by the key values. The reduce function combines all the values which related to one distinct key in some way, the manner of aggregation values is determined by the user program [22]. Figure 2 illustrates the architecture of the Map/ Reduce framework.

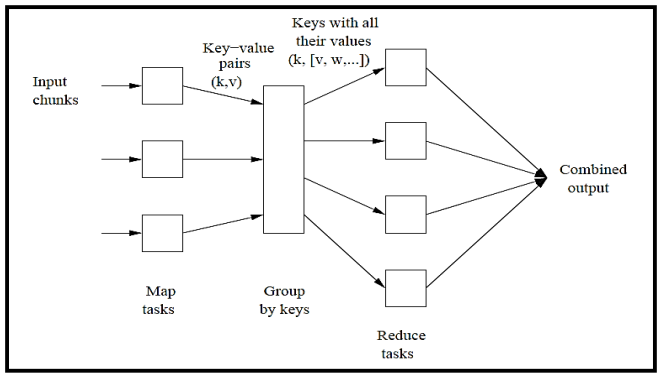

Figure 2: Architecture Of map/ reduce programming model [22]

VI. RESULTS AND DISCUSSION

A. Proposing Data Encryption Scheme for Cloud Computing

Data encryption is one scheme to achieve the security criteria (confidentiality, privacy and integrity). The proposed method consists of two stages. We can use the AES data encryption algorithm with Map/reduce technique for data that submitted to the cloud by users. The first stage saves these data to HDFS (Hadoop Distributed File System) which then implement using AES and Map/reduce technique in the second stage. The implementation of the proposed system can be implemented and submitted to SaaS cloud model Platform www.salesforce.com or pay and go platform. Figure 3 shows the proposed system.

B. Salesforce.com

Salesforce is a SaaS cloud service model used to access information for organization and develop application by developer. Salesforce uses Visualforce and Apex to develop application in its platform. Visualforce include tag-based markup language that is similar to HTML. Apex is a strongly object oriented program developed by salesfoce.com. It allows to developer to execute transaction control with calls of Application Programming Interface (API). Figure 4 shows a Visualforce code from developer console to execute tags and API together.

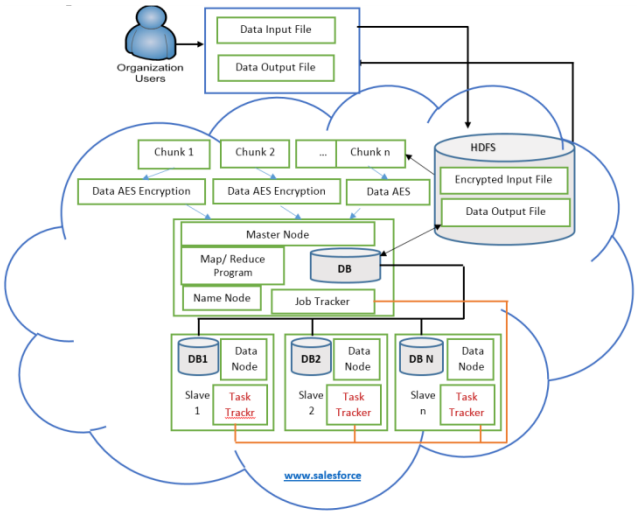

Figure 3: Data encryption proposed system in cloud computing using map/ reduce technique

```
<apex:page sidebar="false">
<p> The year of today is {!year(today())} </p>
<p>Tomorrow will be day number {! day(today() + 1)}</p>
<p> It is true/ False {! contains('visualforce','force')}</p>
<p> Today's Date is {!TODAY()} </p>
<p> Next week it will be {!TODAY() + 7} </p>
 {! IF (day(today()) >14, 'After the 14 day', 'before or on the 14')}
<apex:form >
<apex:pageBlock title="Main Menu" >
<apex:pageBlockSection title="A Section Title" >
I'm three components deep!
</apex:pageBlockSection>
<apex:pageBlockSection title="A Second Title">
This is another Level
</apex: pageBlockSection>

<apex:pageBlockButtons title="File" ></apex:pageBlockButtons>
</apex:pageBlock>
</apex:form>
</apex:page>
```

Figure 4: Snapshot of visualforce code using developer console in salesforce.com

The output of this code is shown in Figure 5.

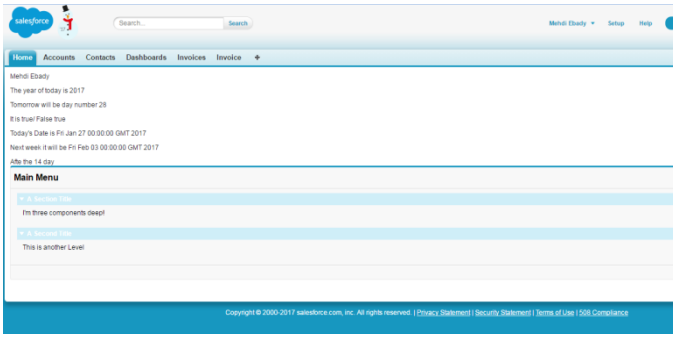

Figure 5: The output page on Salesforce.com

VII. CONCLUSION

The cloud computing encryption techniques are play an integral role to protect the data from unauthorized access. Many techniques are presented to save these data in cloud storage but the data security is still a challenge problem. To address the security data problem in cloud service, this paper proposed a security mechanism for large data scale using AES encryption with Map/ Recue techniques. The maps are associated with chunks of input data in the form (key, value) and produce (key, list[values]) pairs. The reduce combines all the maps outputs and aggregate the data is some approach that defined by user application. Master node is a server that schedule the processing tasks and monitor them in case of failure to re-execute it. The main task of master node is to split data to HDFS for processing and then store the output for the user. AES encryption technique is a promising technique for the future because it is not breakable by the attackers for many years. The service model www.salesforce.com can be accessed by the developer to run application using Visualforce and Apex.

REFERENCES

[1] A. Thomas, Geethu; Prem, Jose V; P., "Cloud computing security using encryption technique," *CoRR abs/1310.8392*, pp. 1–7, 2013.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," *NIST Spec. Publ.*, vol. 145, p. 7, 2011.

[3] K. Jakimoski, "Security Techniques for Protecting Data in Cloud Computing," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 1, pp. 49–56, 2012.

[4] W. Bhaya and M. E. Manaa, "Review Clustering Mechanisms of Distributed Denial of Service Attacks," *J. Comput. Sci.*, vol. 10, no. 10, pp. 2037–2046, 2014.

[5] M. Jog and M. Madiajagan, "Cloud Computing: Exploring security design approaches in infrastructure as a service," in *Proceeding of International Conference of Cloud Computing, Technologies, Applications & Management*, 2012, pp. 156–159.

[6] Y. Yesilyurt, Murat; Yalman, "New approach for ensuring cloud computing security : using data hiding methods," *Sādhanā*, vol. 41, no. 11, pp. 1289–1298, 2016.

[7] M. Thangavel, P. Varalakshmi, and S. Sridhar, "An analysis of privacy preservation schemes in cloud computing," in *Proceeding of International Conference on Engineering and Technology*, 2016, no. March, pp. 146–151.

[8] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services : User Authentication for Social Enhancement of Home Networking," *IEEE Trans. Consum. Electron.*, vol. 57, no. 3, pp. 1424–1432, 2011.

[9] I. Singh, K. N. Mishra, A. M. Alberti, A. Jara, and D. Singh, "A Novel Privacy and Security Framework for the Cloud Network Services," in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2015, pp. 3–7.

[10] T. Y. Win, H. Tianfield, and Q. Mair, "Detection of Malware and Kernel-Level Rootkits in Cloud Computing Environments," in *Proceedings of the International Conference on Cyber Security and Cloud Computing*, 2016, pp. 295–300.

[11] T. Saxena and V. Chourey, "A Survey Paper on Cloud Security Issues and Challenges," in *International Conference on IT in Business, Industry and Government*, 2014, pp. 1–5.

[12] B. Cristina, Andreea; Ştefan, "The Gap between Cloud Computing Technology and the Audit and Information Security Supporting Standards and Regulations," *Audit Financ. J.*, vol. 5, no. 125, pp. 115–121, 2015.

[13] W. Bhaya and M. E. Manaa, "A Proactive DDoS Attack Detection Approach Using Data Mining Cluster Analysis," *J. Next Gener. Inf. Technol.*, vol. 5, no. 4, pp. 36–7, 2014.

[14] T. Chou, "Security Threats on Cloud Computing Vulnerabilities," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 79–88, 2013.

[15] Sophos, "Threatsaurus The A-Z of Computer and data Security threats." Boston, USA, pp. 1–130, 2012.

[16] I. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey," *Computers*, vol. 3, no. 1, pp. 1–35, 2014.

[17] R. Singh, Niharika; Jangra, Ajay; LAkhina, Upasana, Sharma, "SQL Injection Attack Detection & Prevention over Cloud Services," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 4, pp. 256–261, 2016.

[18] P. Mosca, Y. Zhang, Z. Xiao, and Y. Wang, "Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services," *Int. J. Commun. Netw. Syst. Sci.*, vol. 7, no. 12, pp. 529–535, 2014.

[19] K. Munir and S. Palaniappan, "Security Threats / Attacks Present in Cloud Environment," *Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 12, pp. 107–114, 2012.

[20] C. S. Kumar, "A novel Technique : Data Leakage Hindering in Cloud computing using Swarm Intelligence," *Int. J. Technol. Appl.*, vol. 5, no. 6, pp. 1886–1891, 2014.

[21] G. C. Kessler and G. C. Kessler, "An Overview of Cryptography

(Updated Verision, 3 March 2016)," *http://commons.erau.edu/publication/127*, no. March, 2016.

[22] J. Leskovec, A. Rajaraman, and J. D. Ullman, *Mining of Massive Datasets, Book*. Stanford University, 2014.