IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 16-20

Securing Cloud Data Using DES Algorithm

Aparna Akare, Anagha Choukade, Prajwali Gandhare,
Ishwari Mahajan
Department of IT, DMIETR

Abstract: *Cloud computing is the delivery of computing service server, storage, databases, networking, software, analytics, intelligence and more over the internet the cloud to offer raster innovation, flexible resources and economics of scale. Software as a Service (SaaS) service is the top most layer of the cloud computing stack directly consumed by end user i.e. SaaS. However, the new technology has also created new challenges such as data security, data ownership and transcode data storage. Security is an important factor in cloud computing insuring clients data is placed on the secure mode in the cloud. This paper describes about the design and implementation of simplified algorithm based on data encryption standard (DES) algorithm. The data to be encrypted is manipulated with the private key that is created.*

Keywords: *Algorithms: DES, Cloud Computing, SaaS Services.*

I. Introduction

Cloud computing is an emerging computing technology that uses the internet and central remote services to maintain data and application. Cloud computing usually involves the transfer, storage, and processing of information on the 'providers' infrastructure, which is not included in the 'customers' control policy. In Network-based cloud computing software, application are big role. Cloud computing helps to use application without installation. Access the personal files at any computer with internet. This technology allows much more efficient computation by centralizing storage memory, processing and bandwidth. The benefits of cloud reduce spending on technology, Globalize your work force on the cheap. Reduce capital cost, improve flexibility, less personal training is needed. In cloud computing there are various types of cloud are as: 1) Public Cloud 2) Private Cloud 3) Community cloud 4) Hybrid cloud.

A Public Cloud is a type of computing in which a service provider makes resources available to the public via the internet. Resources vary by provider but may include storage capabilities, application or virtual machines.

A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate.

A hybrid cloud is an integrated cloud service utilizing both private and public cloud to perform distinct functions within the same organization.

A community cloud in computing is a collaborative effort in which infrastructure is shared between several organization from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or externally.

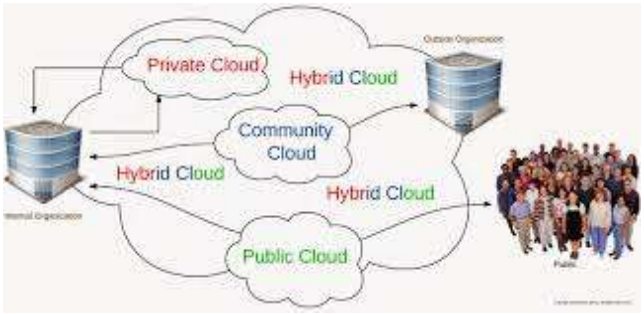

Fig.1: Type of Cloud

The concept Cloud Computing is linked closely with those of Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) all of which means a service oriented architecture. Here comes the first benefit of the Cloud Computing i.e. it reduces the cost of hardware that could have been used at user end. As there is no need to store data at user's end because it is already at some other location[5]. **Software as a service** is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software", and was formerly referred to as "software

plus services" by Microsoft. SaaS is typically accessed by users using a thin client via a web browser. SaaS has become a common delivery

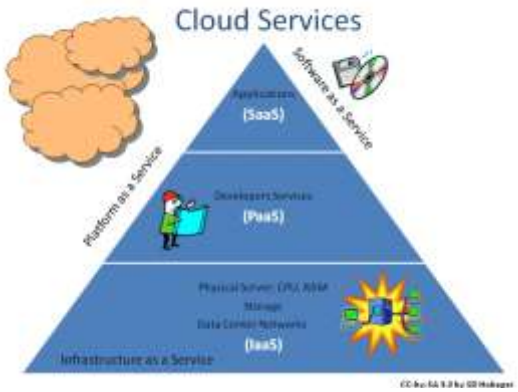

Fig.2: Cloud Services

model for many business applications, including office software, messaging software, payroll processing software, DBMS software, management software, CAD software, development software, gamification, virtualization,accounting, collaboration, customer relationship management (CRM), Management Information Systems (MIS), enterprise resource planning (ERP), invoicing, human resource management (HRM), talent acquisition, learning management systems, content management (CM), Geographic Information Systems (GIS), and service desk management. SaaS has been incorporated into the strategy of nearly all leading software companies[4].

II. Security Issues And Challenges of cloud Computing

Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security. Cloud Computing has several major issues and concerns, such as data security, trust, expectations, regulations, and performances issues[5].

One issue with cloud computing is that the management of the data which might not be fully trustworthy; the risk of malicious insiders in the cloud and the failure of cloud services have received a strong attention by companies. Whenever we discussed about security of cloud computing, there are various security issues arise in path of cloud. Some of the security concerns and solutions of them are listed and directed below**:**

1) With the cloud physical security is lost because of sharing computing resources with other companies. No knowledge or control of where the resources run.
2) Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exists.
3) Customer may be able to sue cloud service providers if privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.

III. Proposed Work

We have proposed securing cloud and making Private cloud, cloud is a term referring to accessing computer information technology and software application through a network connection often accessing data centers using local area networking. Cloud storage security is a top concern for organization information technology and security departments. Cloud computing is linked closely with software as service (Saas), Saas is the most familiar from cloud service for customer. SaaS moves the task of managing software and its development to third party services. Algorithm like: DES have been used comparative study among them have also been presented to ensure the security of data on cloud. DES is symmetric Key algorithm, in which a single key is used for Encryption/Decryption of message whereas DES(Data Encryption Standards) Was Developed in early 1970's by IBM. The key length of DES algorithm is 56 bits. We have implemented our idea in the form of encryption and decryption using DES algorithm.

IV. Security Algorithm Used In Cloud Computing

The Data Encryption Standard(DES)

DESis a block cipher. It encrypts data in blocks of size 64bits each. That is 64 bits of plain text goes as input to DES,which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore asymmetric key algorithm. The Data Encryption Standard(DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Festal Cipher. It uses 16round Festal structure. The block size is 64-bit. Though, keylength is 64-bit, DES has an effective key length of 56 bits,since 8 of the 64 bits of the key are not used by theencryption algorithm (function as check bits only).

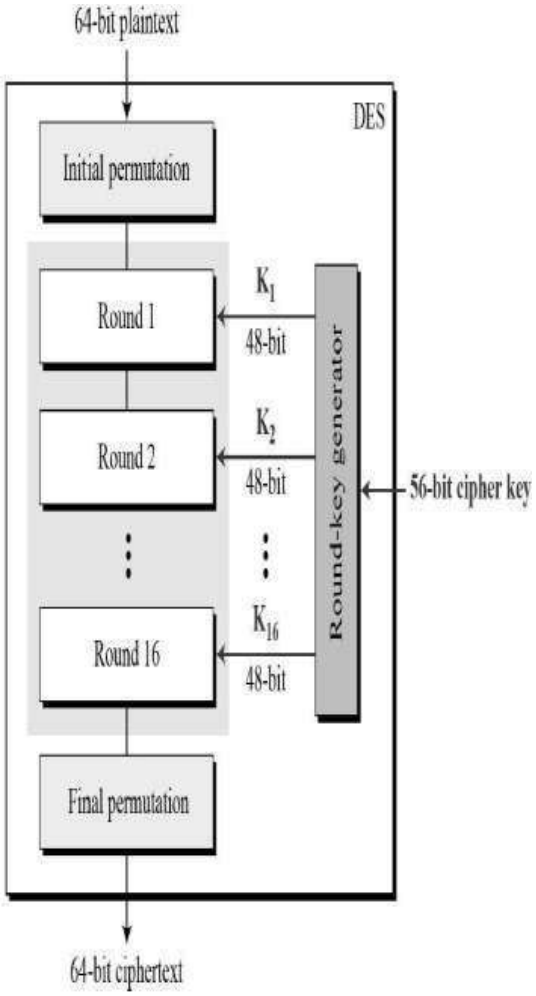

Fig 3:-Data Encryption Algorithm

The encryption process is made oftwo permutations(P-boxes), which we call initial and final permutations, and sixteen Festalrounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefinedalgorithm described later in the chapter. Figure 3 shows the elements of DES cipher at the encryptionsite.

Rounds

DES uses 16 rounds. Each round of DES is a Festal cipher, as shown in Fig:4.

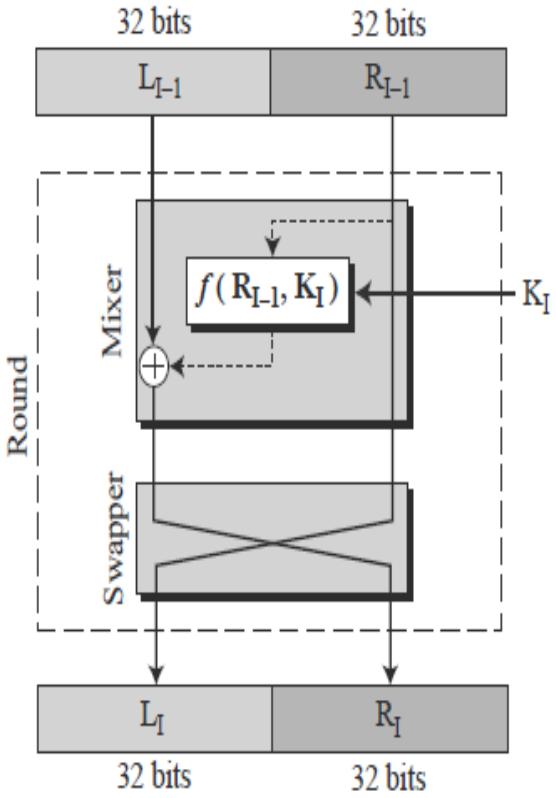

Fig.4 A Round in DES

The round takes LI−1 and RI−1 from previous round (or the initial permutation box) and creates LI andRI, which go to the next round (or fi nal permutation box). we can assumethat each round has two cipher elements (mixer and swapper). Each of these elements is invertible.The swapper is obviously invertible. It swaps the left half of the text with the right half. The mixer isinvertible because of the XOR operation.

Comparison Of algorithms

Table 1

Characteristics	**AES**	**RSA**	**DES**
Platform	Cloud Compu ting	Cloud Compu ting	Cloud Compu ting
Key Size	128,19 2,256 bits	1024 bits	56 bits
Key Used	Same key is used to encrypt and decrypt the blocks.	Public key is used for encrypt ion and private key,for decrypt ion	For encryption and decrypt ion same key is used.
Scalability	Scalabl e	Not Scalabl E	Scalabl e
Initial Vector Size	128 bits	1024 bits	64 bits
Security	Secure for both provide r and user.	Secure for user only	Securit y applied to both provide rs and user
Data Encrypti on Capacity	Used for encrypt ion of large amount of data	Used for encrypt ion of small data	Less than AES
Authentication Type	Best authenticity provide r	Robust authenticimpl ementation	Less authentic than AES.
Memory Usage	Low RAM needed	Highest memor y usage algorith m	More than AES
Execution Time	Faster than others	Require s maxim um time	Equals to AES

V. Conclusion And Future Scope

In this paper ultimate goal of purposed system to provide a proper data stored and securing on cloud also reducing data storage and processing cost is a mandatory requirement of any organization.Encryption algorithms have been proposed to make cloud data secure and gave concern to security issues, challenges and also comparisons have been made between AES, DES and RSA algorithms to find the best one security algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers.

Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms. DES algorithm consumes least encrypt-ion time. By doing implementation for all algorithms in PHP and mySQL, the desired output for the data on cloud computing has been achieved. In future proposed framework can be provided more security and to make a public cloud enhance security over the network.

References

[1]. Ghassan O. karame, Claudio Soriente, "Securing Cloud Data Under Key Exposure", is affiliated with NEC Labotatories Europe, Heidelberg, 69115 Germany, IEEE 2017.

[2]. Arjun Kumar 1 ,Byung Gook Lee2, HoonJaeLee"Secure Storage and Access of Data in Cloud Computing"Department of Ubiquitous-IT 2Department of Computer and Information Engineering Dongseo University, Busan, 617-716, Korea,IEEE2012.

[3]. Pearson,S., Benameue,A., "Privacy,Security and TZrust Issues arlses from cloud computing cloud computing technology and science (cloudCom)", IEEE second international conference,2010,On page(s):693-702.

[4]. Subhashinipallikonda,yashwanthreddy, "securing cloud data using encryption algorithm", MVSR engineering college, hydrabad 2017,

[5]. Zhifeng Xiao and Yang Xiao" Security and privacy in cloud computing" Department of Computer Science, The University of Alabama,Tuscaloosa, AL 35487-0290 USA,IEEE,2012.

[6]. Arjun Kumar and HoonjaeLee" Secure storage and access of data cloud computing" Department of Ubiquitous-IT, Dongseo University, Busan, 617-716, Korea,2012.