Cloud Security and DES Algorithm A Review

Mrs. Dhina Suresh
Research Scholar, Department of Computer Science
St. Joseph's College of Arts and Science for Women,
Hosur, India.
dhinadulcy@gmail.com

Dr. M. Lilly Florence
Professor, Department of Computer Applications
Adhiyamaan College of Engineering,
Hosur, India.
lilly_swamy@yahoo.co.in

***Abstract*-Cloud is an evolving trend today. It is an internet based service delivery model which provides internet based services, computing and storage for users. There are also disadvantages with cloud computing. Data security and privacy protection issues remain the primary problem in cloud. It is required to protect the stored data and applications in the cloud. This article discusses on the basics of cloud and the security issues in it. It gives a note on the existing cryptographic algorithms and it gives a detailed discussion on the DES algorithm.**

Keywords- cloud computing, virtualization, cloud security, data security, and privacy protection.

I. INTRODUCTION

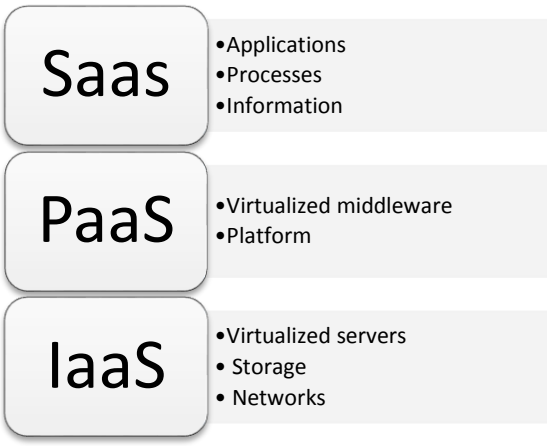
Cloud is where user is provided services by CSP (Cloud Service Provider).We should know that we will be surrendering all our sensitive information to a third-party cloud service provider. Cloud computing architectures consist of front-end platforms called cloud clients may be servers, clients, tablets and mobile devices. These client platforms interact with the cloud data storage via an application (middleware) or a web browser or through a virtual session. It is difficult to control the data in cloud. Cloud service providers must ensure the privacy of the data by protecting them from unauthorized access. The most important concern is to guarantee that data integrity and confidentiality is attained while data is stored in the cloud.

There are many cloud providers such as Google, Amazon, Microsoft and many more. The vital issue in the cloud is that of security. Security in cloud can be enhanced by implementing cryptography[3]. The concept of cryptography is the user has to encrypt the data to convert it into a text normally called as cipher text before he stores or uploads the data in the cloud so that the data remains secure from invaders. The cipher text is then decrypted to get the original data.The main aim of this paper is to explain the DES algorithm with example.

II. CLOUD COMPUTING MODELS

A. *Software-As-A-Service*

It provides the user a complete application running on cloud infrastructure that is hosted by CSP. Users need not buy or install it. Therefore in SaaS software application are shared as a service. Example of SaaS is Google Docs.



B. *Platform-As-A-Service*

The user develops an application through SaaS. The application has to be deployed. PaaS helps to deploy their application on the cloud. The user can control their application but not the infrastructure. PaaS delivers a computing platform as a service. Example of PaaS is Google App Engine.

C. *Infrastructure-As-A-Service*

Through the IaaS the user gets access to resources like storage, server, networks and data center space. It shares the computing resources. User can also deploy and run the application as well the operating system on IaaS. Example of IaaS is Amazon EC2.

III. CLOUD MODELS

A. *Public cloud*

In Public cloud the computing infrastructure is hosted by the cloud vendor. The computing infrastructure is shared between any organizations.The customer has no visibility and control over where the computing infrastructure is hosted.

B. *Private cloud*

The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Private clouds are more highly expensive and more secure when compared to public clouds.

C. *Hybrid cloud*

Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud.

D. *Community cloud*

Community cloud involves sharing of computing infrastructure in between organizations of the same community. We can consider as all theorganizationsrelated to the Government within the state may share computing infrastructure on the cloud to manage data.

IV. CLOUD SECURITY ISSUES

The CSA (Cloud Security Alliance) has identified the following computing threats for 2013.

- First on the list is a data breach.A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized. We have an option to encrypt the data to reduce data breaches.
- The second-greatest threat in a cloud environment, according to CSA, is data loss. Data loss is an error condition in which information is destroyed by failures or neglect in storage, transmission, or processing.

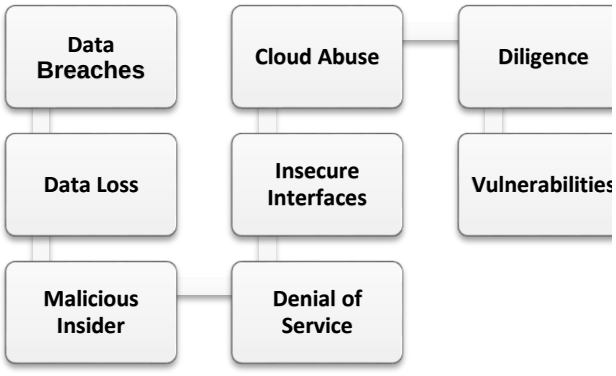


Figure 2. Cloud Security Issues

- Next on the list of threats are insecure interfaces and APIs. Weak interfaces and APIs can expose an organization to security issues pertaining to confidentiality, integrity, availability, and accountability.
- DoS (Denial of Service), the next threat whichhas been an Internet threat for years. It becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services.
- Fifth on the list is a malicious insider, which can be a current or former employee or someone who gains access to a network, system, or data for harmful purposes which leads security to great risk.

- Sixth on the list is cloud corruption or abuse, such as a daring person using a cloud service to break an encryption key, which is too difficult to crack on a standard computer.
- Seventh is due diligence. For example when using the cloud the organizationsmay face contractual issues with providers over liability and transparency.
- Last but not least shared technology vulnerabilities are the ninth-largest security threat to cloud computing. Cloud service providers share their services in a scalable way. The threat of shared vulnerabilities exists in all delivery models (SaaS, PaaS, IaaS) according to the report.

V. SECURITY ALGORITHM USED IN CLOUD

A. Symmetric key algorithms

In symmetric key encryption, only one key is used for both encryption &decryption [4]. The key is kept secret. To ensure secure communications between everyone in a group of n people a total of n(n - 1)/2 keys are needed, [1]which is the total number of possible communication channels. The other names of symmetric key algorithms are secret key, single key or shared key. There are two types of symmetric key encryption.

1) Block cipher symmetric key encryption

In this type the key is applied to the block of plain text and a block of cipher text is obtained [2]. Blocks of 64 bits have been commonly but modern techniques use 128-bit blocks.

2) Stream cipher symmetric key encryption

In stream cipher one bit is encrypted at a time and so it is time consuming.

Few examples of symmetric key algorithms [7] are as follows.

- DES (Data Encryption Algorithm)
- AES (Advanced Encryption Standard) / Rijndael
- Triple AES
- Blow fish

B. Asymmetric key algorithms

It is also called as public key encryption. It uses two keys , a public key known to everyone and a private or secret key known only to the recipient of the message. The first asymmetric key encryption was found in 1976 called Diffie Hellman algorithm.

Public key encryption is pretty good and popular for transmitting information via the Internet. They are extremely secure and relatively simple to use.

Few examples of Asymmetric key algorithms are as follows.

- RSA (Ron Rivest, Adi Shamir and LeonardAdleman)
- Diffie Hellman key exchange

VI. DES ALGORITHM MANUAL CALCULATION

DES is a block cipher symmetric key encryption.
The following are the features [1] of DES.

- Input / Output Block size = 64 bits
- Key size = 56 bits (in reality, 64 bits, but 8 are used as parity-check bits)
- Number of rounds = 16
- 16 intermediary keys, each key has 48 bits

To execute the entire DES algorithm it consumes much time and is tiresome. Let us see a sample DES [6].The following are the features of Sample-DES.

- Input / Output Block size = 8 bits
- Key size = 10 bits
- Number of rounds = 2
- K1 K2- sub or round keys normal DES has 16 round keys one in each round.

We use the term called Permutation. It can be defined as re arranging the bits. In DES algorithm we [6]rearrange the bits to perform encryption and decryption. Here P4, SW, P8, IP, P10, EP, Left shift all are example for Permutations. Table I gives a detailed description of all the permutations which we are going to apply for our sample DES algorithm.

<table>
<tr><td colspan="4">Standard per mutate definitions used in this example</td></tr>
<tr><td>P10 Per mutate
i/p 1 2 3 4 5 6 7 8 9 10
o/p 3 5 2 7 4 10 1 9 8 6</td><td>P8 Select & per mutate
i/p 1 2 3 4 5 6 7 8 9 10
o/p 6 3 7 4 8 5 10 9</td><td>P4 Per mutate
i/p 1 2 3 4
o/p 2 4 3 1</td><td>EP expand &Per mutate
i/p 1 2 3 4
o/p 4 1 2 3 2 3 4 1</td></tr>
<tr><td>IP initial permutate
i/p 1 2 3 4 5 6 7 8
o/p 2 6 3 1 4 8 5 7</td><td>IP⁻¹ inverse of IP
LS-1 left shift 1 position
LS-2 left shift 2 position</td><td colspan="2"><table><tr><td colspan="4">S0</td></tr><tr><td>01</td><td>00</td><td>11</td><td>10</td></tr><tr><td>11</td><td>10</td><td>01</td><td>00</td></tr><tr><td>00</td><td>10</td><td>01</td><td>11</td></tr><tr><td>11</td><td>01</td><td>11</td><td>10</td></tr></table></td><td><table><tr><td colspan="4">S1</td></tr><tr><td>00</td><td>01</td><td>10</td><td>11</td></tr><tr><td>10</td><td>00</td><td>01</td><td>11</td></tr><tr><td>11</td><td>00</td><td>01</td><td>00</td></tr><tr><td>10</td><td>01</td><td>00</td><td>11</td></tr></table></td></tr>
<tr><td colspan="4">Assume the following 10 bit key and 8 bit text</td></tr>
<tr><td colspan="2">10 bit key
1010000010</td><td colspan="2">8 bit plain text
01110010</td></tr>
</table>

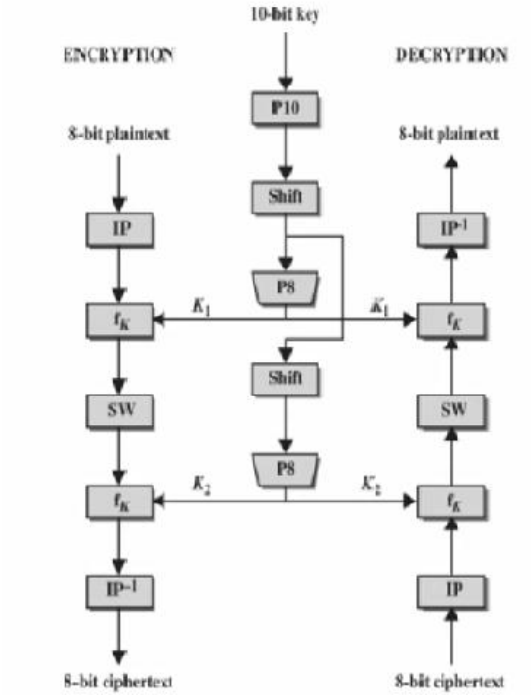


Figure 3. Sample DES Algorithm Flow

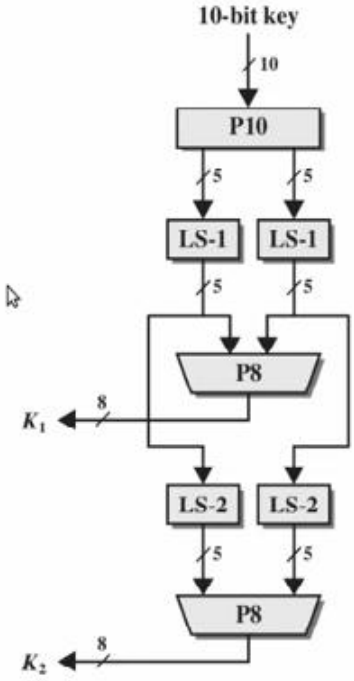


Figure 4. Sample DES Key Generation

We divide our sample DES algorithm of block size 8 bits, key size 10 bits in to three phases.

- Key generation phase
- Encryption phase
- Decryption phase

A. Key generation phase

Let us generate the key for our sample DES [6]. The key is same for both the sender and receiver. The assumed 10 bit key **1010000010** is sent and it is permutated.

1) ***Step1***

P10 Permutate

I/P	1	0	1	0	0	0	0	0	1	0
P10	3	5	2	7	4	10	1	9	8	6

Re arrange the bits of the key as per the P10 permutation that is defined in table I. The following is the output obtained after P10 permutation.

O/P	1	0	0	0	0	0	1	1	0	0

2) ***Step 2***

The permuted value is now divided in to a pair of 5 bits each. To the divided pairs left shift LS is done. The output of LS1 is obtained.

L/S1	0	0	0	0	1	1	1	0	0	0

LS1: 1 0 0 0 0 = 0 0 0 0 1

LS1: 0 1 1 0 0 = 1 1 0 0 0

3) ***Step3***

The value obtained after left shift 1 is to be re arranged. So P8 Per mutation is applied.

LS1	0	0	0	0	1	1	1	0	0	0
P8	6	3	7	4	8	5	10	9		

Two bits are eliminated after P8 Permutation. P8 permutation is done and the output of 8 bits is obtained.

P8	1	0	1	0	0	1	0	0		

This output is the Round Key K1:

K1	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**		

4) ***Step 4***

The L/S value obtained in step 3 is divided in to two pairs each of 5 bits. Two times Left shift is done. The output LS2 is obtained.

L/S1	0	0	0	0	1	1	1	0	0	0

L/S2	0	0	1	0	0	0	0	0	1	1

LS2: 0 0 0 0 1= 0 0 1 0 0

LS2: 1 1 0 0 0= 0 0 0 1 1

5) ***Step5***

The value obtained after left shift 2 is to be re arranged. So P8 Per mutation is applied again.

LS2	0	0	1	0	0	0	0	0	1	1
O/P	6	3	7	4	8	5	10	9		

Two bits are eliminated after P8 Permutation. P8 permutation is done and the output of 8 bits is obtained.

P8	0	1	0	0	0	0	1	1		

This output is the Round Key K2:

K2	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**		

Thus we have generated two pairs of keys successfully. In the original DES algorithm the size of the key is 56 bits and 16 rounds will take place in key generation. Since we taken the key size of 10 bits, we have done only 2 rounds.

B. Encryption

Now we have to encrypt the text. The plain text is encrypted to cipher text[1]. We have to define two S-boxes here. We can define it as a matrix. B1 & B4 tells the rows. B2 & B3 tells the columns. The first matrix is S0 and the next S1. Both are pre-defined. The rounds performed are given in Fig 5 diagrammatically.

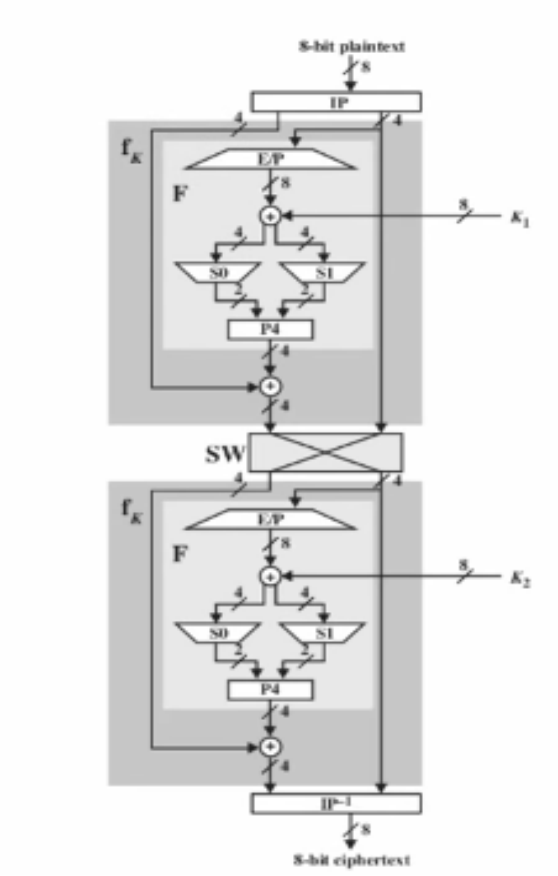


Figure 5. Sample DES Encryption Algorithm Flow

1) ***Step1***

In the first step Initial Permutation is done as per the values given in table 1. The plain text is taken as the input and the initial permutation is done [6].

Our 8 bit sample Plain text is: 0 1 1 1 0 0 1 0

Plain text	0	1	1	1	0	0	1	0
IP	2	6	3	1	4	8	5	7

The output after initial permutation of the plain text is as follows.

O/P	1	0	1	0	1	0	0	1

2) ***Step 2***

The output obtained is divided in to 2 pairs of four bits each. Let us consider left and right.

Left	1	0	1	0	Right	1	0	0	1

3) ***Step 3***

We then apply the expanded permutation for the right bit.

Right	1	0	0	1				
EP	4	1	2	3	2	3	4	1

The output obtained after expanded permutation is as follows.

EP	1	1	0	0	0	0	1	1

4) ***Step 4***

The obtained output is Ex-Ored with the first key K1 obtained in key generation. We know that Ex-Or operation will return 0 when both the inputs are same and 1 when they are different.

EP	1	1	0	0	0	0	1	1
K1	1	0	1	0	0	1	0	0
Ex Or	0	1	1	0	0	1	1	1

5) ***Step 5***

The obtained output is to be put in to the S-Boxes. The pre-defined values for the S-Boxes are given in table I. Divide the Ex-Or values into 2 pairs with four bit each.
The values of S0 & S1 can be checked from the table I given above.

Ex Or	0	1	1	0	0	1	1	1

	B1	B2	B3	B4
S0	0	1	1	0
S1	0	1	1	1

B1, B4 gives the row values and B2, B3 gives the column values. From the row and column value obtained get the values from the S boxes given in table 1.
S0: row 00 col 11 which gives 10 from S0 matrix
S1: row 01 col 11 which gives 11 from S1 matrix

S Box value	1	0	1	1

6) ***Step 6***

The S-Box value is now to be permutated with P4 permutation.

S Box	1	0	1	1
P4	2	4	3	1

The following output is obtained after p4 permutation.

O/P	0	1	1	1

7) ***Step 7***

Now we take the 4 left bits from step 2. The left half is to be Ex-Ored with the above output.

O/P	0	1	1	1
Left	1	0	1	0
Ex OrValue	1	1	0	1

8) ***Step 8***

The Ex Ored value is to be swapped with the 4 right bits which is mentioned in step 2.

Ex Or	1	1	0	1
Right	1	0	0	1

Right	1	0	0	1
Ex Or	1	1	0	1

The output obtained after swapping is given below.

O/P	1	0	0	1	1	1	0	1

9) ***Step 9***

The above output forms the input to the second round where the same procedure is followed but Key 2 is used Fig 5. We have to repeat the same procedure as we did in round one.

The output obtained in round two is given below

O/P	1	1	1	0	1	1	0	1

10) ***Step 10***

After we apply the inverse permutation we get the eight bit cipher text

O/P Cipher Text	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**1**

I mention it again that we got the cipher in two rounds because we are using only 8 bit input and 10 bit key. But for original DES algorithm we use 64 bit input block with a key size of 56 bits. Therefore we repeat the above steps 16 times to get the cipher text.

C. Decryption

Decryption which is the reverse process is done as per the given diagram [6]. The above processes are repeated in the reverse way and the 8 bit plain text is retrieved.

The same process occurs in original DES[1] but there are 16 rounds with 64 bit block size and also there are 8 S boxes [9] with64 bits in each box and all the permutation tables are of 64 bits. This gives high security.

VII. DES ALGORITHM REVIEW / CONCLUSION

- DES was the 1st encryption standard approved by National Institute of Standards and Technology [5]. It was a standard algorithm in 1974.
- Because of the 56 bit key size it can generate many possible keys which increases its security.
- Differential Cryptanalysis involves comparing the XOR of 2plaintexts to the XOR of the 2 corresponding cipher texts. DES was feebly resistant to it.
- Avalanche Effect:The strength of all cryptographic algorithms can be reviewed from its Avalanche Effect [8]. A good algorithm has high Avalanche Effect. This effect can be stated that if an input is changed to a small extent, let us say a single bit is changed/ flipped in the plain text, more than half the output cipher bits are changed.

Avalanche effect = (No of flipped bits in the cipher text / no of bits in cipher text) X 100%

As per few reviews, after 16 rounds of DES there were 35 flipped bits. Therefore the Avalanche effect is 54.68% in DES which is good.

- DES is possible to brute-force(attack on encrypted data) in less time on modern processors.
- Many DES secured password systems match or check only the first 8 characters.
- If the encryption is more complex the processing time is also more.
- DES shares the key, so if the key is lost the data cannot be read.

ACKNOWLEDGMENT

I would like to thank THE LORD MY SAVIOR for guiding and showering HIS blessings throughout my life. I take immense pleasure in thanking my guide Dr. M. Lilly Florence for rendering her valuable knowledge and guidance. I would like to thank my husband for his love and support. I would like to thank my parents and my son for their patience and care.

REFERENCES

[1] Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design, Electronic Frontier Foundation

[2] Janan Ateya Mahdi, "Design and Implementation of Proposed B-R Encryption Algorithm", IJCCCSE, Vol. 209, No.1.2009.

[3] William Stallings, "Cryptography and Network Security: Principles & Practices", fourth edition.

[4] Yogesh Kumar, Rajiv Munjal, "comparison ofsymmetric and asymmetric cryptography withexisting vulnerabilities" IJCMS-Oct.2011.

[5] Eli Biham and Adli Shamir, "DifferentialCryptanalysis of full DES".

[6] https://www.youtube.com/watch?v=qHZKze24kVo

[7] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, HamidA.Jalab, M.Shabbir and Y. Al-Nabhani "NewComparative Study Between DES, 3DES and AES withinNine Factors," Journal Of Computing, Volume 2, Issue 3,March2010,Issn2151-9617

[8] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect," IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[9] A. F. Webster, Stafford Tavares, "On the Design of S-Boxes," *CRYPTO'85* (1985).