International Journal of Engineering, Science and Mathematics
Vol. 7Issue 4, april2018,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

DIFFERENT ENCRYPTION ALGORITHMS IN CLOUD

Ashima Narang
Dr. Deepali Gupta

Abstract

Big data is something which has a huge amount of data that has to be processed. It handles all types of data may it be of any volume which may be further any types of data. It may be structured or unstructured or may be semi structured. Big data is used to get together the old and new data. There are tools designed to handle this huge data like Apache Hadoop. But the data kept over the internet is not safe. Cloud whereas provides the online storage system but providing the security is still an issue. Encryption and decryption is the old approach to provide the security to the data. Here, I will be discussing about the various encryption techniques available.

Keywords:

Cloud;
Cloud security;
Encryption;
DES;
AES;
Blowfish.

Author correspondence:

Ashima Narang,
Ph.D Scholar,
Maharishi Markandeshwar University, Sadopur, Ambala,India
Dr. Deepali Gupta,
Professor and Head, Computer Science Department,
Maharishi Markandeshwar University, Sadopur, Ambala,India

1. Introduction

Cloud computing helps you to provide the access to your data without being geographically placed yourself at the location of the servers. Everybody wants her/his data to be secured. There may also be the sensitive data in the data stored. Different organizations are focusing upon the issue of securing the sensitive data stored over the cloud and that the data can be accessed smoothly and security from the sources can be maintained. For processing the data from the big data, a platform named Hadoop was designed[12]. Initially, the security issues were not taken into consideration. But later, many different modifications were made to the Hadoop system, so that the reliable shared analysis and storage system can be processed.

In this digital world, people communicate using the internet through the different devices that may include mobile phones or computers or any other devices. The messages, photos or any other important files can be exchanged over the internet. Now, when we use such data which has to be transferred and side by side secure, then this also has to be protected against the various phishing, hacking, spoofing or any other cybercrime activities. In computer, network or in cloud, there is always some important data which requires security and has to deal with the protection of that important information. This particular information should not be replaced or any changes should not be made to the data without the knowledge of the creator. These kinds of files may include any types of emails or videos or photos etc. The main goal must be to protect this data from the vulnerable activities and to protect this data from the illegal use from the outside threats.

Cloud computing[3] uses a network of remote servers which are all hosted over the internet where we can manage or store the data when the data is not on the personal computer or on the local server. The data may be kept anywhere weather on the cloud or on the local server, security matters a lot.

Various security algorithms are used to protect the data sent via networks. Different security techniques are used to avoid hacking. This problem is a serious issue in the security of the data that is available over the

internet and the strategies are being proposed to find the solution to this issue and protect the data and provide the confidentiality to the users. Encryption and decryption are the old and successful approaches used to secure the data [1]. This concept of cryptography [8] where the data can be secured between the two parties can be explained better through figure1 given below:

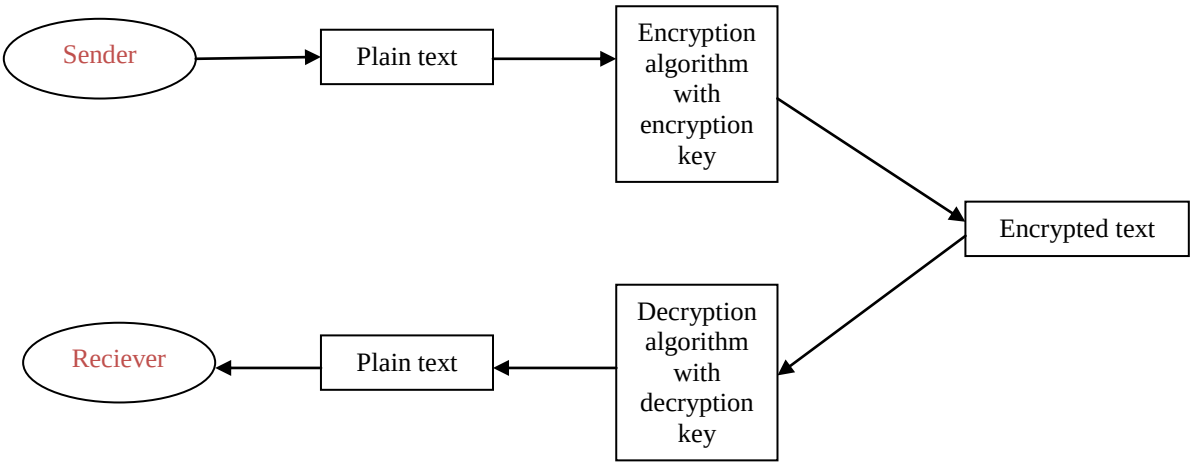

Figure 1.*Process for cryptography*

Figure 1 given above illustrates about the process of cryptography which can be further explained as that how the data sent by the sender is encrypted using the encryption algorithms available and then is decrypted by the reciever again using another decryption algorithm along with the encryption/decryption key sent by the sender, which may be private or public.

The sharing of data and the use of internet is quite extensive these days and so it becomes necessary to keep the data from hacking or interferences. Cryptography is one of the commonly used technique for securing data. It helps protecting the data while transmission amoungst the users. The information sent is converted nto the non readable form and when recieved by the reciever it can be converted back into the original, plain form. This non readable text is called the cypher-text and when converting this cypher-text into the plain data is known as decryption process[2].

Figure 2 illustrates the classifications of encryption algorithms with some examples of each.

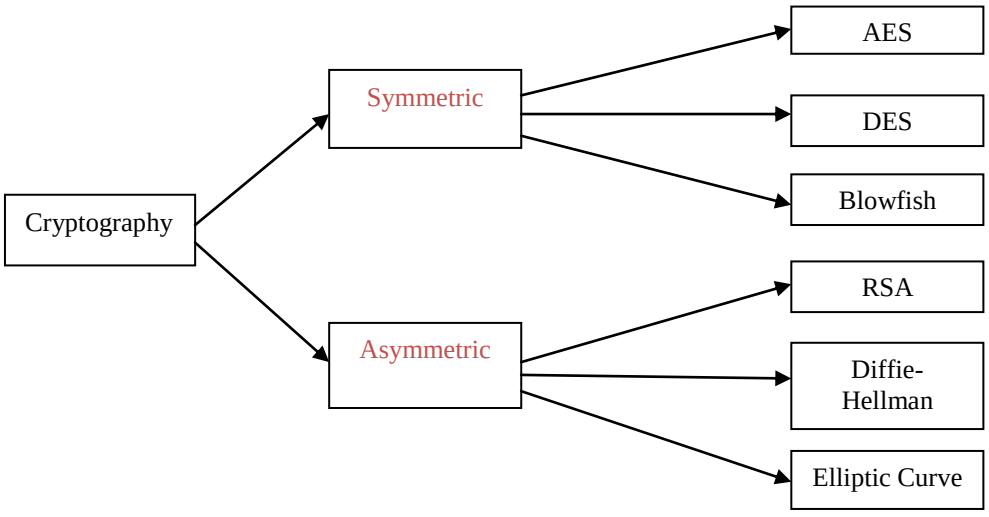

Figure 2. *Classification for encryption algorithms*

International Journal of Engineering, Science and Mathematics
Vol. 7Issue 5, May2018,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

In Cloud computing, when the data is to be secured, cryptography is widely used. The classification for cryptography can be done as: Symmetric and Asymmetric key encryption. Symmetric is used for the private key and asymmetric is used for public key. In symmetric key, the sender sends only one key to the reciever which is called the secret key. Whereas, in Asymmetric encryption, public keys are used for encryption and another different, private key is used for decryption.However, public key is not very efficientfor small mobile devices hence it is based on mathematical functions and need more computations[15]. Symmetric encryption algorithms are far faster than asymmetric algorithms as they require less processing power for consumption[14].

2. Symmetric Encrytion Algorithms

This uses the same key to encrypt or decrypt the information[10]. This technique is used to protect the sensitive data. The following algorithms are used for symmetric encryption.

i) Data Encryption Standard (DES)

National Institute of standards and technology(NIST) developed the first encryption standards called DES. It adopted the national standards in 1997 whereas IBM developed these standards around in 1974[16]. DES algorithm provides various standards for protecting sesitive and unclassified data [9]. DES was used in various commercial domains, military domains and many more over the last years [13]. Initially, DES used a input block for 64-bits and a 56-bit key and the left over 8 bits were used for odd parity check. But still, many attacks could prove it insecure which made it insecure block cipher[5].

ii) Advanced Encryption Standard (AES)

To replace DES a newer encryption standards were recommended by NIST called Advanced Encryption Standards (AES). Rijndael named block cipher was developed by Joan Daemen and Vincent Rijnmen in 1197. It has keys with the length of 128, 192 or 256 where in 256 is said to be as default.Depending on the key lengths the encryption techniques are seected with the variable rounds. It needs 10,12 and 14 rounds respectively for 128, 192 and 256 bits keys. The iterative numbers are dependent on the length of the key. Each step is transformed inversely as the sequence of encryption while the process of decryption.

iii) Blowfish

This type of encryption algorithm was provided by Bruce Schneier in 1993 [13]. 64 bits block cipher is used and the variable length key can vary from 32 bits to 448 bits. Blowfish is said to be the fastest of the all as it was created as a replacement of DES. It is free for all the users and is license free [11]. Each round consists of two parts: key dependent permutation, and a key- and data- dependent substitution[6].

3. Assymetric Encryption Algorithms

i) Rivest-Shamir-Adleman (RSA)

Ron Rivest, Adi Shamir and Leonard Adleman developed an algorithm for encryption in 1977 using public key and private key. Weather for digital signatures or for the key exchange algorithms, RSA is a block cypher. RSA uses both variable length key as well as variable length block for encryption. The sender which may be a cloud service provider encrypts the message and the reciever, the service customer decrypts the message. The information is encrypted using a public key and later decrypted using a private key available with the reciever. RSA algorithm consides of three different steps, which goes as:key generation, encryption followed by decryption. But brute-force attacks, timings attacks, mathematical attacks or chosen cyphertext attacks cannot be resolved using RSA [6].

ii) Diffie-Hellman Algorithm

The first public key algorithm was constructed in 1976 by Witfield Diffie and Martin Hellman and is now known as Diffie-Hellman algorithm [17]. This algorithm is somewhere related to discrete algorithm problem. This algorithm is used for key exchange algorithm and is constructed under insecure connection channel[2]. This consists of two different keys: private key of his own and a public key of that of sender's. Once reciever gets the message he decrypts the message with his own private key and sender's public key [6].

iii) Elliptic Curve Cryptography (ECC)
Koblitz and Miller constructed another algorithm using the theory of elliptic curve in the year 1985 and was called ECC. It uses some complicated algebric and geommetric equations to generate the public key [6] since it is a cryptography with public key. In ECC, for decryption the private key is used and for generating signatures and encryption the public key is used. ECC is also used by many researchers to enhance the other algorithms. ECC has also been used to improve performance to reduce computing power and battery resource consuming [7] which gives us chance to use it in mobile device applications, hence it provided faster, efficient and secure model for secured application in the cloud [7].

4. Conclusion

In this study, we gave a detailed survey over cryptography and its types i.e. Symmetric and Asymmetric wherein further for Symmetric we studied about DES,AES and blowfish algorithms and for asymmetric we discussed about RSA, Diffie-Hellman and Elliptic Curve algorithms. There performances and efficiency may differ depending upon the various parameters. As the security is the major issue these days in Cloud environment, these algorithms may be used to resolve some security issues. In my future work, I will be comparing and analysing these algorithms over few parameters to find the best out of them which may be futher used for the security of data, robustness, efficiency and speed in Cloud environment.

References

[1] Cordova R.S, Maata R L R, Halibas A.S. and Al-Azawi R., " Comparitive analysis on the performance of selected security algorithms in Cloud Computing", *International conference on Electrical and Computing Technologies and Applications*,2017.
[2] Yassein M.B, Aljawarneh S. and Qawasmeh E., "Comprehensive Study of Symmetric Key and Assymetric key encryption algorithms", *ICET 2017, IEEE transactions*, June 2017
[3] Narang A., "A review- Cloud and Cloud security", *International journal of Computer Science and mobile Computing*, Vol6, isuue1, pp178-181, 2017.
[4] Goyal A., Kaur Mandeep, Narang A., "Handling the Threats on Mobile Security: AES, DES, Blowfish- Symmetric Key Cryptography Algorithms", *IJSTM*,Vol6. Issue1, May, 2015.
[5] Kaur, Randeep, and Supriya Kinger. "Analysis of security algorithms in cloud computing." *International Journal of Application or Innovation in Engineering and Management 3.3: 171-6*, 2014.
[6] Stallings, William, and Mohit P. Tahiliani. "Cryptography and network security: principles and practice." Vol. 6. *London: Pearson*, 2014.
[7] Alowolodu, O. D., et al. "Elliptic curve cryptography for securing cloud computing applications." *International Journal of Computer Applications 66.23*,2013.
[8] Ebrahim M, Khan S., and Khalid U.B., "Symmetric AlgorithmSurvey: A Comparative Analysis,"*International Journal of Computer Applications*, vol. 61, no. 20, pp. 975–8887, 2013.
[9] Mahajan, Prerna, and Abhishek Sachdeva. "A Study of Encryption Algorithms AES, DES and RSA for security." *Global Journal of Computer Science and Technology* ,2013.
[10] Padmapriya, A., and P. Subhasri. "Cloud computing: security challenges and encryption practices." *International Journal of Advanced Research in Computer Science and Software Engineering 3.3, 2013*.
[11] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." *International journal of emerging technology and advanced engineering 1.2* , pp 6-12, 2011.
[12] Xiao Z, Xiao Y, "Accountable map reduce in Cloud computing " *proceedings computer communications workshops (INFOCOM WKSHPS), IEEE transactions*, pp 1082-1087, 2011.
[13] Nie, Tingyuan, and Teng Zhang. "A study of DES and Blowfish encryption algorithm." *Tencon 2009-2009 IEEE Region 10 Conference IEEE*, 2009.
[14] Hardjono, Thomas, and Lakshminath R. Dondeti, "Security in Wireless LANS and MANS (Artech House Computer Security)." *Artech House, Inc.*, 2005.
[15] Ruangchaijatupon, N., and P. Krishnamurthy. "Encryption and Power Consumption in Wireless LANs-N,'' *The Third IEEE workshop on wireless LANS*. 2001.
[16] Standard, Data Encryption. "Federal information processing standards publication 46." *National Bureau of Standards, US Department of Commerce*, 1977.
[17] Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." *IEEE transactions on Information Theory 22.6 : 644-654*, 1976.
[18] Shivangi Kaushal, Jagpuneet Kaur Bajwa, "Analytical review of user perceived testing techniques", *IJARCSSE,Vol2, issue 10*,Pg no 213-216, 2012