iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10166

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

Data Centric Security Algorithms In Cloud Computing - A Review

Kumari Sarita[1], Jawahar Thakur[2]
[1,2]*Department of Computer Science, H. P.University, Shimla, India*

Abstract: Cloud Computing is a shared pool of resources like services, infrastructure and platform to provide efficient and secure services to the users.Users store their data virtually on cloud. To secure data on cloudCryptographic techniques are usedby Cloud Service Providers (CSP) such as Symmetric Key, Asymmetric key and hashing algorithms. In this paper a fair comparison of data centric security algorithms in cloud computing has been presented.The comparison is done on the basis of common performance factors such as number of rounds, key size, scalability, encryption/decryption time, block size, security rate,power consumption and throughput.This review paper is concluded that Blowfish SymmetricCryptographic algorithm is most efficient among other algorithms.

Keyword-: Cloud, Data, Security, Cryptography, Symmetric, Asymmetric, Hashing.

I. INTRODUCTION

Cloud computing is a distributed kind of internet based technology.Cloud Computing is a technical upgrading that mainly works in designing computing systems, developing applications and power real [2]services for building software. It provides resources like infrastructure, platform, software, networks, servers, storage and applications.Online business applications (e-business, e-commerce), web-mails (Gmail, reddit), social networking sites such as Facebook, twitter and LinkedIn, online data storage (Amazon) are the examples of cloud computing.It is provided by the Cloud Service Providers (CSP) to the customers [1].

A. Characteristicsof Cloud Computing [1]:

1) Elasticity
2) On-demand Usage and Measured Services
3) Pay per Use and Low cost software
4) Broad Network Access and Virtualization
5) Resource Pooling and Multi-tenancy
6) Location Independence
7) Advanced security technologyTypes of Cloud Computing: [2]

Cloud computing is classified on the basis of services, infrastructure, platform, security, data and communication as shown in figure 1.1.

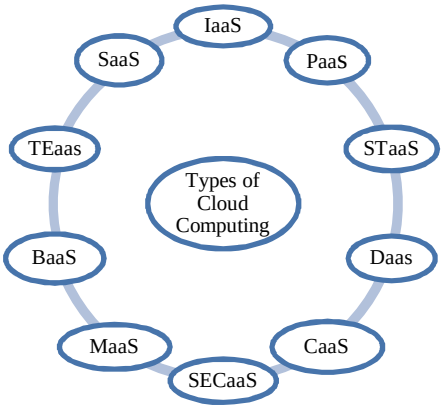


Fig. 1.1 Types of cloud computing

8) IaaS (Infrastructure as a Service):It offers virtualized resources like computation, storage and communication. GoGride and Amazon EC2 mainly offer IaaS services.
9) PaaS (Platform as a Service): It provides a higher level of illustration to make a cloud computing comfortably programmable. E.g. Java, Python, .Net, Force.com, Microsoft Windows Azure and Google App Engine [2].
10) SaaS (Software as a Service):Web applications spreadsheet and word processor Salesforce.com, Rackspace, web based mails are examples of SaaS [24].
11) STaaS (Storage as a Service): It is a buying and a selling layout in which service master of the house provides space in the form of lease to the user from their storage.
12) SECaaS (Security as a Service): These security providers provide users with security event management, intrusion detection, anti-virus and authentication.
13) DaaS (Data as a Service):DaaS is a member of software as a service. It is independent and dealers can easily approach to the data directly over the internet.
14) TEaaS (Test Environment as a Service):It's a testing and delivery model in which software and their data are groomed in the cloud centrally and are attained to users for their testing purposes.
15) BaaS (Backend as a Service): It's a layout for blending cloud storage with mobile app developers and provides other aspects like integration, push notifications and user management with social networking services.
16) MaaS (Monitoring as a Service):It is an outsourced service to provide security mainly to platforms that are run on the internet for conducting business [21].
17) CaaS (Communication as a Service):It enables the consumer to utilize the Enterprise level VoIP, VPNs, PBx and Unified communications without the costly investment of purchasing, hosting and managing infrastructure.

B. Deployment model

A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size and access.[3] There are four common cloud deployment models as shown in fig 1.2

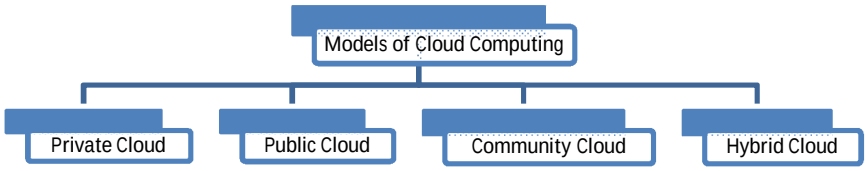


Fig. 1.2 Deployment model

1) PrivateCloud: This cloud authority is cultivated for the use of only single organization which is being composed of multiple consumers.
2) CommunityCloud: This cloud authority is maintained for defining communities of consumers from organizations that have to experience the same data within each other. It is organized by single or more of the organizations in the community.
3) PublicCloud: This cloud authority is maintained for generic public. It is maintained and managed by third parties (cloud provider) itself.
4) HybridCloud: This cloud authority is association of more than two cloud authorities i.e.private, public or community.[21]

Cloud computing is a distributed and shared pool of resources like platform, services and environment. It is classified in various types. It has three service models. In this paper the comparison of cryptographic algorithms has been presented on the basis of performance factors.Section II describe about Cryptography, its principles and types also. Section III will give a brief review of all the concerned research papers. Section IV gives the conclusion and future scope of this paper.

II. CRYPTOGRAPHY

Cryptography is usually referred to as "the study of secrets". It is a technique of converting data into unreadable form during storage and transmission. The unreadable data is known as cipher text while original form is known as plain text. Encryption is the procedure of conversion plain text to cipher text. Decryption is the process of conversion of cipher text to plain text [22].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

A. Cryptography [22] principles

Cryptography can be directly used to help ensure these security properties. There are five main principles of cryptography as shown in figure 2.1.

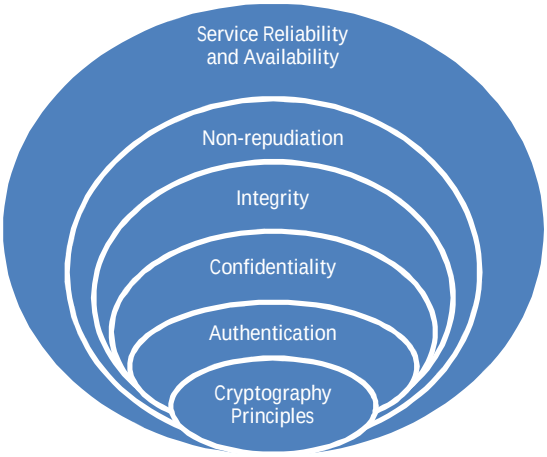


Fig. 2.1 Cryptography Principles

1) Authentication :Authentication means to provide one's identify. E.g. Username and password. Before sending and receiving the data, sender and receiver should be identified.

2) Confidentiality :It means that data is understandable to the receiver only, for intruders it would be waste. It helps in preventing the intruder disclosure of sensitive information. Ensuring that no one can access the information except the intended receiver.

3) Integrity:Integrity means that the originality of the data should be maintained after receiving information on receiver side. It helps in preventing the modification from unauthorized user.

4) Non- Repudiation A mechanism to prove that the sender really sent thismessage means that neither the sender nor the receiver can : falsely deny that they have sent a certain message.

5) Service Reliability and Availability :Availability refers to assurance that user has access to information anytime and from any network. Such systems provide a way to grant their users the quality of services they expec

6) *Types of cryptography [22]:*Cryptography is divided into three main categories which are shown in the figure 2.2.

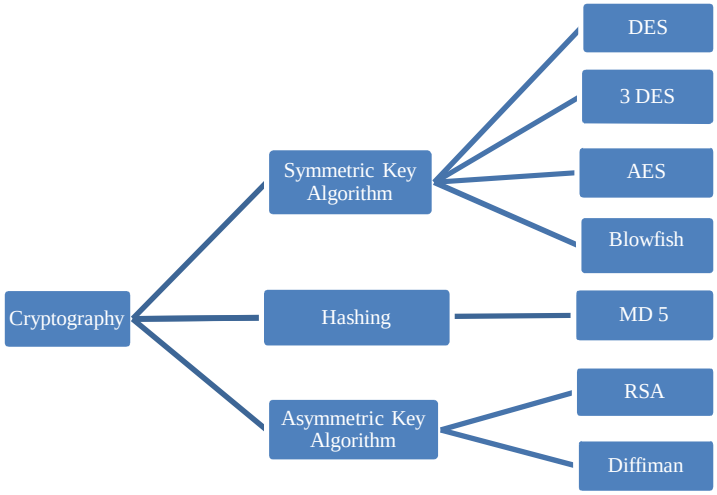


Fig. 2.2 Types of Cryptography

7.)Symmetric Key Algorithm:In symmetric key cryptosystem, single and same key is used for encryption and decryption.

B. Des: data encryption standard

1) DES is a block encryption algorithm.It was the first encryption standard published by NIST (National Institute of Standards and technology) [23].
2) It uses one 64-bit key.In which 56 bits are independent key, 8 bits are used for error detection.
3) The main operation is bit permutation and substitution in one round of DES.
4) DES is an insecure block cipher key.

C. 3DES:TRIPLE DATA ENCRYPTION STANDARD [4]

1) 3DES is an enhancement of Data Encryption Standard.
2) It uses 64 bit block size with 192 bits of key size.
3) The encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time.
4) 3DES is slower than other block cipher methods [4]

D. AES: ADVANCED ENCRYPTION STANDARD

1) AES is also known as the Rijndael algorithm is a symmetric block cipher.
2) It can encrypt data blocks of 128- bits using symmetric keys 128, 192, 256.
3) It encrypts the data blocks of 128 bits in 10, 12 14 round depending upon the key size.
4) AES encryption is fast and flexible.
5) It can be implemented on various platforms especially in small devices.
6) Brute force attack is the only effective attack known against it.

E. BLOWFISH:Blowfish was designed in 1993 by Bruce Schneider.

1) Blowfish has a 64- bit block size and variable key length from 32-bits to 448 bits.
2) Blowfish has variants of 14 rounds or less.
3) Blowfish is a very secure cipher.
4) It has a simple structure and its implementation is easy.

F. Asymmetric Key Algorithm

In asymmetric, two different keys are used for encryption and decryption.

G. RSA: Rivest, Shamir and Adleman

1) It is the most common public Key algorithm and asymmetric block cipher.
2) It is capable to support public key encryption and digital signature.
3) It uses large integers like 1,024 bits in size.
4) It has only one round of encryption.

H. diffiman: ii is a public key algorithm which uses discrete logarithms in a finite field.

1) It is also known as key exchange algorithms
2) It is considered to be secured for mathematical groups [21].

I. Hashing

the primary application of hash function in cryptography is message integrity.

J. MD5: Message Digest 5

1) It is developed by Cryptographer Ronald Rivest in 1991.
2) It takes an input of arbitrary length and produces a message digest i.e. 128 bits long.

3) The most common application is the creation and verification of digital signatures. [21]

III. RELATED WORK

This section gives background study ofCryptography algorithms. This study is carried out from journal papers, survey papers, books, articles and internet.

Pratap Chandra Mandal [4] provided a fair comparison between four most common and easily used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of different parameters: number of rounds, block size, key size, encryption/decryption time, and throughput and power consumption. It was concluded that Blowfish is best algorithm.

Shweta Singh [21] haveproposed the work on existing 128 bit-AES algorithm.It was analyzed that improvement and modifications in the existing 128- bit AES algorithm was to achieve a robust and secure encryption algorithm. And also worked on an enhancement in the existing cloud simulator tool CloudReports. It was based on cloudsim and used for the selection of best encryption algorithm for implementation of security layer in EnDeCloudReports tool.The results are compared on the basis of encryption/decryption time, throughput time, and speedfor files ranging from 10 MB to 120 MB.It was concluded that experiment used for limited ranges files.

Aarti Devi et al. [10]provided the comparison between three symmetric key cryptographic techniques namely as DES, AES and Blowfish algorithms in terms of time and security by using image simulation. The tool used for the work was Net Beans IDE 7.4. It was observed that Blowfish algorithm took least time for simulation of encryption and decryption.

Shweta Singh [20] surveyed and analyzed the performance of AES, DES and RSA on the basis of packet size, encryption time and decryption time. It was observed that AES algorithm consumes least encryption time and RSA consumes largest encryption time. It was concluded that AES is better algorithm.

Omer K. Jasim et al. [14]provided the various encryption algorithms Symmetric Key Algorithms such as AES, DES, 3DES, Blowfish and Asymmetric Keyalgorithms like RC4, RSA andDiffi-Hillman. The performance parameter for algorithms was input block data size, which observed that how the change in size of the files took place after encryption was complete. It was concluded that the symmetric key encryption are faster than asymmetric key algorithm.

AkashdeepBhardwaj etal. [13]provideda brief overview and comparison of Cryptographic algorithms such as Symmetric key algorithms and hashing algorithms which was used for cloud based applications and services that required data and link encryption. It was analyzed thatin Symmetric key algorithms, AES is best for keyencryption and MD5is faster when encoding.

Afolabi et al. [12] proposed a performance comparison between four encryption key algorithms: symmetric key encryption algorithms (DES, 3DES, AES) and RSA is an asymmetric key encryption algorithm. The comparative analysis was carried out on their Architecture, Scalability, Flexibility, Reliability, Security and Limitations that were essential for secured communication (wired or wireless).It took the different sizes of data blocks(0.5 MB-20 MB). During this analysis it was observed that AES algorithm was the best among all the encryption algorithms in terms of Security, Flexibility, memory usage, Encryption performance and power consumption rate. Although the other algorithms were also effective but most of them have a tradeoff between memory usage and encryption performance.

Shakeeba S. Khan [11]haveprovidedwork onDMS (Document Management System) using cryptography algorithms for. They proposed multilevel encryption and decryption algorithm for data privacy. DES, AES, RSA and homomorphic algorithms were analyzed by using parameters such as architecture scalability, security, use of web browser, storage and backups.DES and RSA were used mainly for first level and second level encryption/decryption process. Implementation was done on HeidiSQL_3.2 IDE with Java Server pages.It was concluded that multilevel encryption will provide more security for Cloud storage than single level encryption.

Tin Zar New et al. [9]analyzed the performance of audio files with the help of RSA and ElGamal algorithms. The audio(.mp3) file format were used with the various file sizes (386MB-1191MB).This system provided the performance analysis of RSA and Elgamal algorithm for audio security depending on the execution time. The system was implemented by using C# programming language. This system was intended to apply in the real data communication environment in order to obtain the confidentiality, secrecy of important data and can choose the better cryptographic algorithms. It was analyzed that RSA is significantly faster than Elgamal algorithm.

ShivlalMewada et al.[16] have proposed the cloud computing environment in which various algorithms like RSA, DES, AES and DEsede were analyzed. By using these algorithms, input variable size were observed on local as well as on Google App engine. It was run on eclipse and got the results through graphs and tables to shown the best algorithm among these. It was analyzed and concluded that AES algorithm was mostly preferred to secure the data. AES algorithm was good in buffer size.

KaulPal Narang[19] proposed the comparison between RSA and 3DES algorithms on the basis of parameters. These factors were scalability, memory required, simulation time, confidentiality, power consumption, key used for encryption/decryption and avalanche effect. The implementation of algorithms was doneon simulators and software libraries having file size of 250 MB – 1 GB.

Odeh Ashraf[17] provided comparison among symmetric key algorithms and Secure Watermark System.DES, AES and Blowfish are symmetric key algorithms. Packet size, CPU time, memory used and power consumption were analyzed in this implementation. The implementation was done on Windows 8, XP and Linux OS.

Khanezaei [5] proposed the comparison between RSA and AES in cloud environment. The parameter used for this experiment was fie size varied from 2048 bit to 256 bytes. The experiment was done on framework of Secure Cloud Storage System. It was concluded that AES had better performance.

Harinath [18] proposed the comparison between different symmetric key algorithms such as DES, 3DES, AES and Blowfish. The experiment was carried out 290 KB to 2.54 MB file size only.The performance factors were encryption /decryption time, key size, block size, throughput and execution time. The implementation was done Netbeans IDE 7.4 on platform JDK 1.7.

IV. COMPARISON BETWEEN CRYPTOGRAPHIC ALGORITHMS

The Comparison of Cryptographic algorithms are done on common parameters such as key size, block size, security rate, power, throughput, encryption/decryption time, scalability and speed are shown in table 1.1.

Table 1.1 Comparisons of Symmetric Key, Asymmetric key and hashing algorithms.

S. No	ALGORITHMS	PARAMETERS	IMPLEMENTATION TECHNIQUES	ENVIRONMENT	FILE SIZES
1	DES, 3DES, AES AND BLOWFISH [4]	• Block size • Key size • Encryption time • decryption time • throughput • power consumption	• Java Programming	Networking	50 KB to 22300KB
2	Modified AES [6]	• Encryption time • decryption time • throughput • processing time	• EnDEcloudReportsSimulators	Cloud computing	10 MB to 120MB
3	DES, AES and Blowfish [10]	• Security • encryption/ decryption time	• Netbeans IDE 7.4	Network	100 KB to 1000 KB
4	AES, RSA [20]	• Block size • Key size • Power consumption • Encryption time • decryption time • Security • Key used • Deposit keys(yes/no) • H/w and S/w implementation • Rounds	• Cloudsim, • EnDeCloudreports, • Java Virtual Machine (JVM), • MATLAB • Octave	Cloud Computing	Packet Size

		• Trojan Horse • Simulators speed • Ciphering algorithm • deciphering algorithm			
5	DES, 3DES, AES, RSA,Diffi-Hillman [14]	• Key length • Rounds • Block size • Security rate • Execution time	• Citrix XenServer 5.6	Cloud networking computing	500 KB to 3500 KB
6	DES, 3DES, AES, Blowfish, RSA, Diffi-Man, MD5 and SHA [13]	• File size • Encryption computation time • Encoding computation time • CPU processing time • Battery power	• Java • Cloud simulator • .NET Security Framework	Cloud based applications	1KB to 25 MB
7	DES, 3DES, AES and RSA [12]	• Architecture • Scalability • Flexibility • Reliability • Level of Security • Memory usage • Output Bytes • Power Consumption rate	• .NET for Simulation • C# programming language, • Visual Studio IDE	Networking	0.5MB to 20 MB
8	RSA and ElGamal [9]	• Execution time • Encryption time • Decryption time	• C# programming language	Communication environment	Only Audio file (.mp3) 386MB to 1191MB
9	DES, AES, Blowfish and RSA, DeSede [16]	• Encryption time • Decryption time • Buffer size	• Eclipse, • Google App engine	Cloud Computing	10 KB to 56 KB

10	RSA, 3DES [19]	• Scalability • Memory required • Simulation time • Through time • Confidentiality • Power consumption • Key used for encryption, decryption • Avalanche effect	• Software libraries • Simulators	Cloud Computing	
11	DES, AES, Blowfish and SWS (Secure Watermark System) [17]	• Packet Size • CPU time • Memory usage • Power Consumption	• Linux • Windows 8 • Windows XP	Network	250 MB to 1 GB
12	AES, RSA [5]	• File size	• Framework of Secure Cloud Storage System	Cloud Computing	2048 bit to 256 Bytes
13	DES, 3DES, AES and Blowfish [18]	• Encryption time • Decryption time • Memory used • Throughput • Execution time	• Netbean IDE 7.4 • JDK jdk 1.7_45	Network	290 KB to 2.54 MB

V. CONCLUSIONAND FUTURE WORK

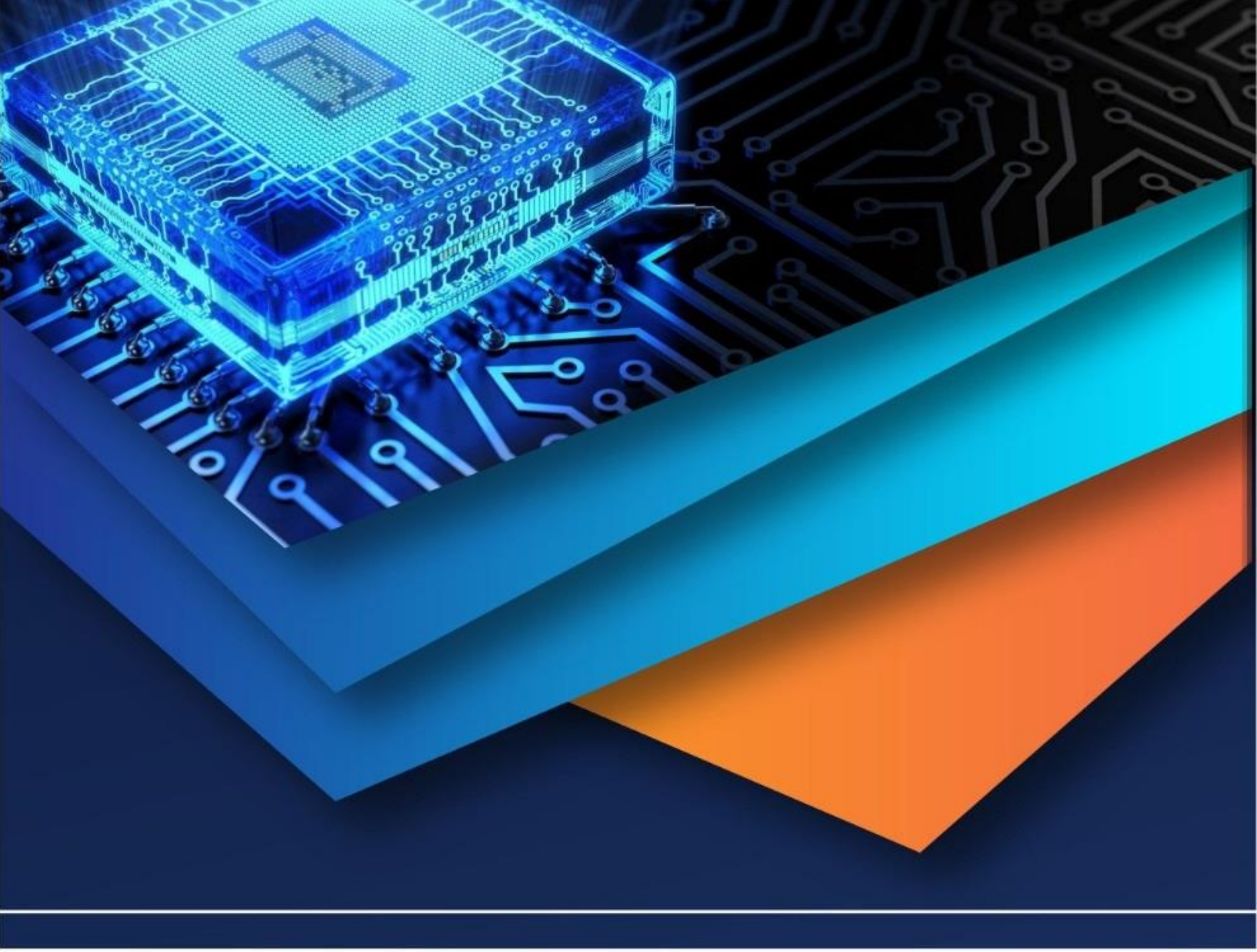
Cloud Computing is a shared pool of resources. Data is stored virtually on cloud. Data centric security provides Cryptographic techniques against unauthorized users. Cryptographic algorithms have three types such as Symmetric Key Algorithms(DES, 3DES, AES and Blowfish), Asymmetric Key algorithms like (RSA, Diffi-man)and hashing Key Algorithms (MD5). In this paper, comparison is performed on existing research done by the researchers based on the different performance factors such as parameters, implementation techniques, environment and file size. These parameters are key size, block size, security rate, power, throughput, encryption/decryption, scalability and speed. However it is concluded that Blowfish Symmetric Cryptography algorithm is efficient among DES, 3DES, AES, RSA, Diffiman, MD5.

The future scope of Cryptographic Algorithms can be used to analyzeand implementon many cloud computing simulator tools with the help of different programming languages.This analysis gives better results and performances on new versions of simulators and with upcoming new languages.

REFERENCES

[1] Parveen Kumar et al. “An Overview and Survey of Various Cloud Simulation Tools” Journal of Global Research in Computer Science, Volume 5, No. 1, January 2014.
[2] SurabhiKaul “Cloud Computing and its Emerging Need: Advantages and Issues”, International Journal of Advance Research in Computer Science, Volume 8, no.3, March-April 2017.
[3] SultanAldossary “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions”, International Journals of Advance Computer Science and Applications, Vol. 7. No. 4, 2016”
[4] Pratap Chandra Mandal “Evaluation of Performance of the Symmetric Key Algorithm:DES, 3DES, AES and Blowfish” Journal of Research in Computer Science, Volume 3, No. 8, August 2012.
[5] NasrinKhanezari “2014 IEEE Conference Systems Process and control (ICSPC 2014)” 12-14 December, Kuala Lumpur Malaysia.

[6] Shweta Singh"Security Layer Implementation in EnDeCloudReports Simulator Tool through Modified AES" International Journal of Engineering Technology Science and Research (IJETSR), Volume 4, Issue 8 August 2017.
[7] Thomas Lenz, Bernd Zwattendorfer and Arne Tauber "A Secure and Confidential Javascript Crypto-Framework for Cloud Storage Applications", IADIS International Conference www/internet, 2013, pp. 219-226.
[8] NiveditaBisht, Sapnas Singh "A Comparative Study of Some Symmetric and Asymmetric Key Cryptographic Algorithms", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3. March 2015.
[9] TIN NEW ZAR, SU WAI PHYO "Performance Analysis of RSA and ElGamal for Audio Security ", International Journal of Scientific and Technology Research, Issue 11 june-2014, Vol. 03. pp:2494-2498.
[10] Aarti Devi, Ankush Sharma, AnamikaRangra "Performance Analysis of Symmetric Key Algorithms: DES, AES and Blowfish for image encryption and Decryption", International Journals of Engineering and Computer Science, Volume 4. Issue 6 June 2015.
[11] Shakeeba S. Khan, "Security in Cloud Computing using Cryptography Algorithms", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue1, January 2015.
[12] Afolabi, A.O. and Atanda, O.G. "Comparative Analysis of Some Selected Cryptographic Algorithms", Computing Information Systems, Development Informatics & Allied Research Journal, Vol. 7 No. 2 June 2016.
[13] AkashdeepBhardwaj, GVB Subramanyam, VinayAvasthi, HanumatSastry "Security Algorithms for Cloud Computing", International Conference on Modeling and Security"2016
[14] Omer KJasim, Safia Abbas, El-Sayed M. El-Horboaty and Abdel-Badeeh M. Salem "Efficiency of Modern Encryption Algorithm in Cloud Computing", Volume 2, Issue6, November-December 2013.
[15] JahangeerQadiree "Security and Privacy Approach of Cloud Computing Environment", International Journal of Advance Research in Computer Science, Vol. 8, July- August 2017.
[16] Shivlal Mewada, ArtiSharivastva, Pradeep Sharma, S. S. Gautam and N Purohit "Performance Analysis of Encryption Algorithm in Cloud Computing", International Journal of Computer Sciences and Engineering, Volume-3, Issue-2.
[17] AshrafOdeh et al. "A Performance Evaluation of Common Encryption Techniques with Secure Watermark System", International Journal of Network Security and its Applications (IJNSA) Vol.7, No.3, May 2015.
[18] DepavathHarinath et al. "Cryptographic Methods and Performance Analysis of Data Encryption Algorithms in Network Security", Volume 5, Issue 7, July 2015.
[19] Narang Pal Kual "Comparison between RSA and Triple DES in Cloud Environment", International Journal on Recent and Innovation Trends in Computing and Communication Vol. 1, Issue:9.
[20] Shweta Singh, "Analysis of EnDeCloudReports for encrypting and Decrypting Data in Cloud" International Journal of Computer Applications, Volume 136, Issue 12 February 2016.
[21] www.google.com//whatiscloud.com//
[22] ForouzanBehrouz A, "Data Communication and Networking", Fourth Edition, 2006, New York: Tata McGraw- Hill.
[23] https://www.google.co.in/search/
[24] Prince Jain, "Security Issues and their Solutions in Cloud Computing", International Journal of Cloud Computing,
[25] S. Venkata Krishna Kumar et al. "A Survey on Cloud Computing Security Threats and Vulnerabilities", International Journal of Innovative Research in Electrical, Electrical, Instrumentation and Control Engineering, Vol. 2, Issue 1, January 2014.
[26] ManpreetKaur et al. " A Review of Cloud Computing Security Issue" International Journal of Advance in Engineering and Technology, June 2015
[27] R. Pushpalatha "Cloud Computing and Security Issues", International Journal of Engineering and Computer Science, Vol. 3. Issue 5, May 2014.
[28] MeenaKumari et al. "Data Centric Security in Cloud Computing", IJCST Vol. 7, Issue 1, Jan- March 2016.
[29] Rashmi et al. "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing Service and Architecture (IJCCSA). Vol. 3, No. 4, August 2013.
[30] PoojaShelke et al. "Data Centric Security Approach: A way to Cloud Computing Security and Privacy", IOSR Journal of Computer Engineering (IOSR-JCR), 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY