International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-12, November 2022

Design and Implementation of Strong Security Architecture for Amazon Web Service based on Cloud Applications

Madan Solanki, Vrinda Tokekar

Abstract: ***Cloud applications are becoming a necessary part of modern life. Security is one of the most important non-functional requirements of every solution. Early days, security and data privacy was just luxury part of software development and it was an optional requirement but nowadays it plays a critical role in daily life. The presented work will be made to observe the need for symmetric security algorithms in Cloud application with Amazon web service. This work observes that the current security level of existing applications recommend improved security solutions to enhance the security level as well performance of proposed architecture. This work recommends Blowfish, RC6 algorithm (symmetric key cryptography) can be used to achieve confidentiality during communication Amazon web service Platform. It also considers the MD5 algorithm to maintain the integrity and modified Kerberos algorithm to achieve authentication. The complete work will propose a security architecture having solution to achieve confidentiality, integrity with strong authentication policy for Cloud application development in Amazon web service. The strong security architecture provide for data and minimum executive time in upload and download file, different key size, file size and chunking size in file. File size divided into chunk 512 bit, 1024 bit, 2048 bit after process in Amazon web service, we are found the optimum time are chunking file size 2048 bits reduce time in encryption and decryption data process and maintain strong security data file in communication including file size 5, 10, 15 and 20 Megabyte.***

Keywords: Cloud Computing, RC6, Blowfish, Kerberos Authentication, MD5

I. INTRODUCTION

Cloud computing consist of resources, serving with services and providing with infrastructure. It is bulk storage of resources with convenient computations and operations and provides with ease to access on-demand services. Cloud is an emerging technology, which copes with changing trends. This technology is flexible to use with low cost and in an advantageous way.

Manuscript received on 13 October 2022 | Revised Manuscript received on 20 October 2022 | Manuscript Accepted on 15 November 2022 | Manuscript published on 30 November 2022.
*Correspondence Author (s)
Madan Solanki*, Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya Khandwa Road Indore (M.P.), India. E-mail: mdvda112@gmail.com
Prof. (Dr.) Vrinda Tokekar, Professor and Head, Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya Khandwa Road Indore (M.P.), India. Email: vtokekar@ietdavv.edu.in

Security policies of cloud are studied in introduction part for achieving authentication of data for security purpose. Security and privacy always comes as future challenge for researchers and authors, these challenges are authentication, authorization, integrity, confidentiality, availability and privacy. These challenges are the major concern due to dependency on third party, because it leads to loss of data. Bulk data is communicated in cloud that comes up with the issue of generating risk of accessing data in cloud by attackers. Amazon Web Service are various type service provider in cloud computing, for example elastic cloud compute, containers, database, storage, developer tools, strong security service, serverless, networking & content delivery, media service, IoT, front-end web and mobile etc. AWS are on demand service provide, free service offers some time duration in cloud computing.

Many organization cloud computing service used Google, Microsoft, facebook, Twitter et cetera.

Amazon Web Service provide at 2006 in IT infrastructure service to ecommerce businesses.

Architecture of cloud computing service-

I. SaaS - Software as a service:- End-user service provide, web application, customers are provided with application anytime and any-where. cloud provider are salesforce.com, etc.

II. PaaS- Platform as a service:- Runtime environment for applications development & data processing hosted in cloud. examples- Google app engine, Microsoft azure.

III. IaaS (infrastructure as a service)- Infrastructure clouds, Rent processing, storage and other fundamental computing resources, drop box, Amazon web services, Mozy and Akamai.

Since cloud are broad field in computing. there is abundance of research method and defiance that can be research survey. Research paper focus on strong security architecture provide for communication data and minimum executive time in upload and download file, different key size, file size and chunking size in file.

1. Authentication

Authentication is one of the security concern in security policies and it cannot be removed ever. Authentication checks user identity and system identity for the purpose of communication.

2. Confidentiality

Confidentiality explains privacy; some parameters are required for securing delivery of information to any wrong person by making sure that message will delivered to right person. Only the authorized people have the right to access data.

3. Integrity

Integrity means accuracy, where data cannot be modified or altered while transmission by unauthorized user. Alteration is the activity where error is created or unauthorized user while transferring of data deletes some sensitive part of the data. thus we are create cloud application help of tools are eclipse Integrated development environment (JEE), WAMP mysql database , tomcat server and JWT(java web token) service JSON token used for ticket generate. It is used Kerberos server for Authentication, Symmetric crypto algorithm Blowfish and RC6 used for Confidentiality, MD5 used to check originality of file, after complete application deploy on amazon web service ec2 instance

II. LITERATURE SURVEY

Many area of researchers have addressed cloud security issues in cloud computing. Some related work are sakshi narula et al [1] security research have presented the working of aws cloud computing which not only provides the excellent cloud service. this paper is to make cloud computing security as a core operation not add on operation. A Monika Gogna [2] research paper the comparison of three protocols X.509, Kerberos 5 and PKINIT have been presented in a distributed network to analyse whether mapping between these protocols is possible or not.

P. Princy [3] IJCSET published paper different symmetric algorithm used and compared these algorithm AES, DES, 3DES, BLOWFISH, RC4, RC6. Result found are Blowfish are best secure and less time in processing. D Rachmawati et al[4] there research are two integrity algorithm compare.Message digest 5 (MD5) and SHA256. Both algorithm are advantages and disadvantages. The parameters which used to compare, two algorithms are the running time and complexity. The research results obtained from the complexity of the Algorithms MD5 and SHA256. Speed MD5 algorithm are better. Piyush Gupta et al [5] there are compare the time taken to build a hash value and deep analysis for two algorithm. Dr D.I. George Amalarethinam et al [6] data security related work in cloud computing. Swedha K et al [7] Proposed solution are deploy and tested in a virtual private network, this research are security and authentication based in Amazon web service. Shrujana Murthy et al [8] encryption, decryption process and record these paper in cloud application. Milind Mathur et al [9] this research paper are performance of different algorithm different according to data load. M. Harini et al [10] Authentication, confidentiality and integrity used md5, AES, and RSA algorithm used in cloud application. Kirtiraj Bhatele et al [11] this research area used symmetric and asymmetric algorithm. Neha Gupta et al [12] Hybrid cryptography service and different algorithm replaced, modified Kerberos protocol used in these proposed paper. Arpana kumara et al [13] Data divided into chund and key generation and java technology used for cloud application. Ali kadhim Bermani et al [14] this research paper data protection model for encryption using hybrid cryptographic. Mohammed Nazeh Abdul Wahid et al [15] comparison of cryptographic algorithm different symmetric algorithm include Blowfish. DIAO Zhe et al[16] Research paper used cloud storage, security policy and data security in cloud application. Zachariah pabi Gariba et al[16] Challenges of popular cloud computing services existing within the last four years . Jung Feng et al [17] Revealed the vulnerability in the aws cloud and technical approaches are potential effective solution. Zain Ul Abedin et al [18] Cryptographic solution in cloud computing security implement are new discipline technology accustomed to defend methodology used . Mansoor Ebrahim et al [22] Different symmetric algorithm used include Blowfish and RC6. Diaa Salama Abdul et al [23] there are evalution has been conducted encryption algorithm at different setting for each algorithm. U. Thirupalu et al [24] maily focus on comparative analysis symmetric, asymmetric and hashing algorithms. Research Paper [19] [20] [21] are related these proposed solution.

Comparative statement for authentication.

Table - 2.1

Keys For Comparision	We used Kerberos	AWS used X.509
Channel	One to One	Many to One
Encryption	Symmetric	Asymmetric
Generate	Ticket	Certificate
Storing	Private Key	Public Key
Pros	Single-Sign on, non transmission of passwords, strong authentication	Authentication, Integrity
Trusted Third Party	KDC	CA

Comparative statement for confidentiality.

Table - 2.2

Keys For Comparision	We used RC6	We used BLOWFISH	AES	3DES
Key size	128,192, 256 bits	32-448 bits	128,192,256 bits	112 or 118 bits
Block size	128 bits	64 bits	128 bits	64 bits
Round	20	16	10,12,14	48
Time consumption	Fast	Fast	Fast	Very slow

Comparative statement for integrity.

Table - 2.3

Keys For Comparision	We used MD5	AWS used SHA256
Security	Secure	More Secure
Message Digest	128 Bits	160 Bits
Speed	Faster, only 64 iteration, Fast calculation	Slower than MD5, 80 iteration, 20% slower, difficult to handle because size.
Complexity	θ(N)	θ(N)
Generate	32 hexadecimal digit	64 hexadecimal digit

comparative statement table 2.1, 2.2, 2.3 authentication, confidentiality and integrity. We are used and AWS used algorithm.

III. PROBLEM DOMAIN

Disadvantages of Cloud necessary a persistent net connection, does not work excellent on slow connections, if net speed slow, can have minimal functionality, Net speed slow data are insecure and data can be destroy.

1. Whenever any organization stores data on public cloud then there is a risk of accessing sensitive data, attackers may attack the data internally.

Retrieval Number: 100.1/ijitee.L932411111222
DOI: 10.35940/ijitee.L9324.11111222
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

2. Difficult X.509 Protocol is maintain the database of Private keys owned by certificate authority and public keys is distributed to the user
3. AES Algorithm Memory Space, Battery consumption and 3DES Memory Space, Slow process and takes the large time of data transfer, AES Key size 128,192,256 bits and 3DES key size 112 or 118 bits.
4. SHA256 is difficult to handle because of its size 256 bit digest size for single input and 64 hexadecimal digit generate. Performance-wise,20-30% slower to calculate than MD5.

We are used tools and algorithm: - The need of security model integrating authentication, confidentiality and integrity inside one solution.

Kerberos server- Used for Authentication, Kerberos is which eliminates this need of processing, securing the private keys and strong authentication, when the user login and Kerberos server authenticate to check credential, If credential are valid authentication server generate the ticket and send the token. User token submit service server, server check the token if valid use the service.

Blowfish and RC6 - Used for Confidentiality, RC6 and Blowfish fast data encryption and Less Memory use, key size RC6 128-256 bits and Blowfish key size 32-448 bits. RC6 and Blowfish more secure other symmetric algorithm . File is taken and divided into chunks are 512 bits, 1024 bits and 2048 bits, dependent to file size control and checks by administrative.

MD5 - Used for Integrity, MD5(message digest), 128 bit digest size for single input and fast calculation 32 hexadecimal digit generate. when user file uploading and md5 applied to before encryption which generate 128 bits md5 hash value, after downloading file recalculation and check the originality file. if value is matched file download otherwise reject process.

We are achieved authentication, confidentiality and integrity are implemented one solution in cloud application to the parameter are Amazon web service ec2 instance. Only for secure uploading and downloading file.

IV. SYSTEM ARCHITECTURE AND METHODOLOGY

System architecture and methodology are flow of complete work is described step by step with the encryption and decryption of flow diagram. Systematic procedure is cited below:-

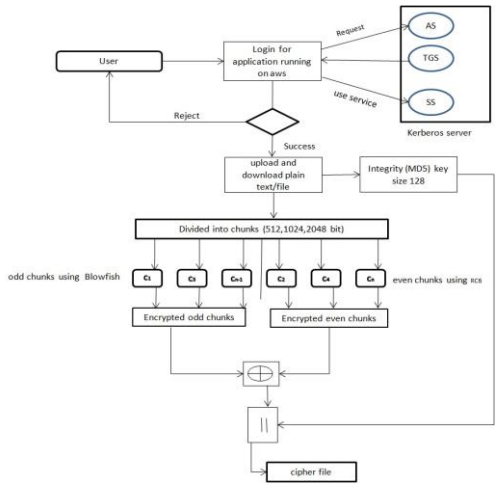


Figure 4.1: System Architecture

Step 1: Authentication User:

- Login user from application in authentication server
- Gererate encrypted token from ticket granting server and send it to be User
- Match the token Login user from Ticket Granting Server.
- Resource server starts providing service to user.

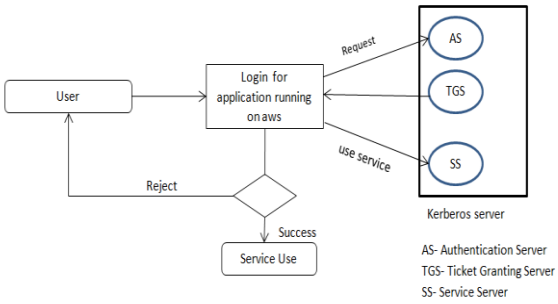


Figure 4.1: Authentication User

Step 2: Calculate Integrity:- MD5 calculate integrity when file is uploading and applied on it generation 512 bit digest size**.** Integrity of the file will be checked in this process.

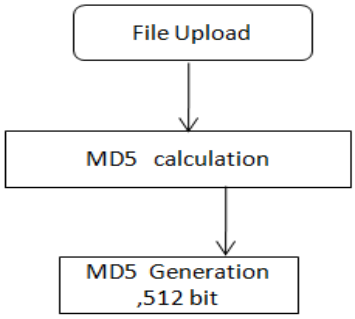


Figure 4.2: Integrity Calculation

Step 3: Encryption Process:- When confidentiality is used to keep data private and safe from unauthorized used. RC6 and Blowfish maintain the confidentiality when data transfer unauthorized network**.** when file user upload on application then divided given administrative user chunk size, Even chunks takes RC6 algorithm and Odd chunks takes Blowfish algorithm. Encrypted and unreadable formed into cipher chunks file.

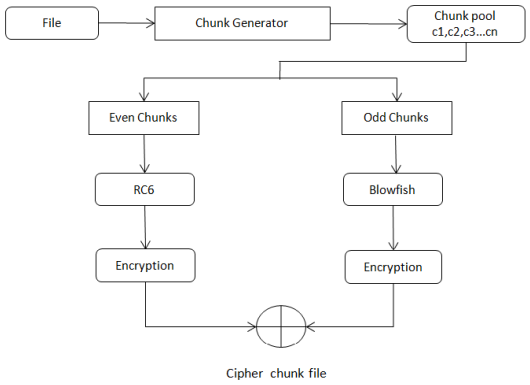


Fig. 4.3: Encryption Process

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

- Chunks are addressed with some chunk id.
- These chunks are stored in Map Index.
- On the chunks the generated multiple keys are applied.
- Cipher chunks that are addressed as key_id in map index using Blowfish and RC6 symmetric algorithm.
- After cipher text is stored in database.
- The chunk_id that are stored in Map index are encrypted using MD5.
- **Step 4: Decryption:-** A decryption process that takes an encrypted piece and then identifies the even and odd pieces. Even fragments are decrypted using RC6 to get simple fragments and Blowfish are odd chunks to get simple fragments. These fragments are rewritten to produce a complete file.

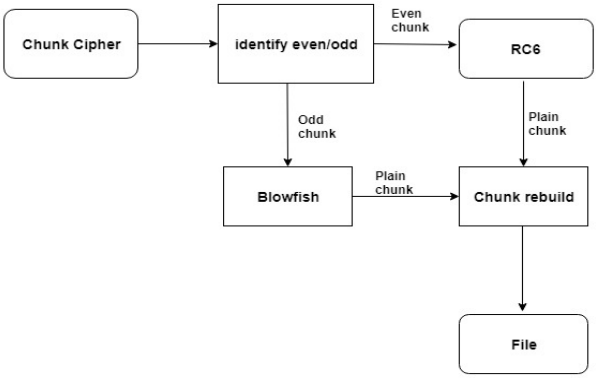


Figure 4.4: Decryption Process

- **Step 5:** Original File Comparison: Recalculation of fragment file integrity is done using MD5. The recalculated files are then compared to the counted files and if they match, they are accepted rather than rejected.

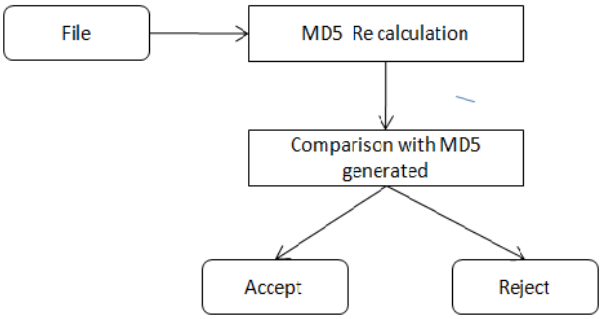


Figure 4.5: Comparison of original file

V. RESULT ANALYSIS

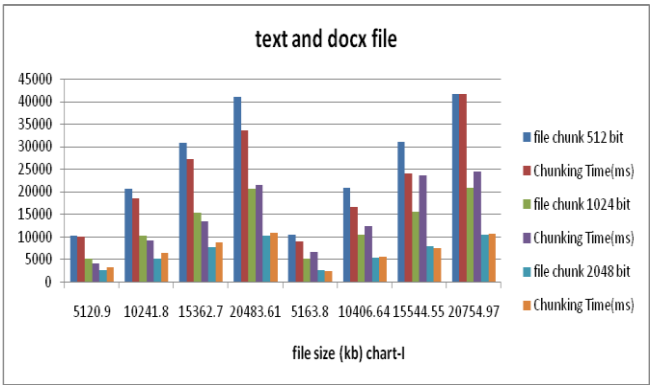
Result analysis complete work describes the uploading and downloading with encryption, decryption file using Rc6, Blowfish MD5 algorithm, calculate time taken by proposed cloud application model deploy in amazon web service. We are calculate the computational time different size of files and file chunking size used are 512, 1024, 2048 bits, tested file of size 5, 10, 15 and 20 megabyte text and docx file.

We reduced processing time when file execute in encryption and decryption and file chunking size 512, 1024, and 2048 bits with key size change RC6 and Blowfish.

5.1 **Upload file**:- Comparative Execution Times(text, docx file size , chunking time campare with different chunking size, key size RC6-192, Blowfish-128) of encryption algorithms with different file size.

Table 5.1

	File	file size(kb)	RCb Key Size(Bit)	Blowfish Key Size(Bit)	MDb Key Size(Bit)	file chunk 512 bit	Chunking Time(ms)	file chunk 1024 bit	Chunking Time(ms)	file chunk 2048 bit	Chunking Time(ms)
Encryption crypto time	text	5120.9	192	128	128	10242	9871.51	5121	4067.8016	2561	3093.496
Encryption crypto time	text	10241.8	192	128	128	20484	18986.2	10242	9019.1928	5121	6461.629
Encryption crypto time	text	15362.7	192	128	128	30725	27097.2	15363	13334.196	7682	8719.612
Encryption crypto time	text	20483.61	192	128	128	40968	33830.8	20484	21446.972	10242	10838.91
Encryption crypto time	docx	5163.8	192	128	128	10328	8865.3	5164	6511.4698	2582	2412.644
decryption crypto time	docx	10406.64	192	128	128	20814	16604.5	10407	12309.331	5204	5473.403
Encryption crypto time	docx	15544.55	192	128	128	31090	23923	15545	23517.576	7773	7531.802
Encryption crypto time	docx	20754.97	192	128	128	41510	41604.5	20755	24371.731	10378	10563.95



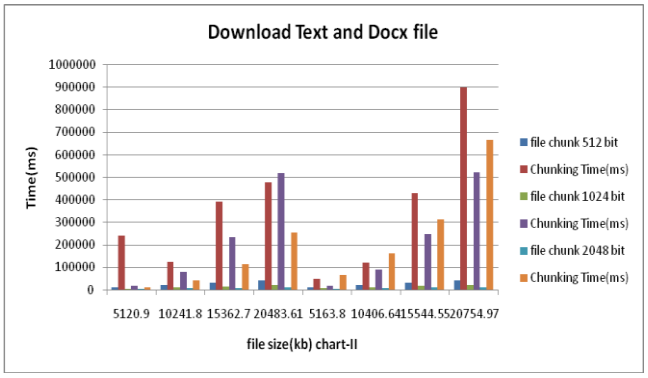
Above shown table-5.1 are different file size uploading in application running on amazon web service, Used key size symmetric encryption algorithm are RC6-192 and Bbowfish-128 bit key size operated in three file chunks size 512,1024, 2048 bit**.** We found that file chunk size 2048 bit less time other file chunk size. file size 5mb,10mb, 15mb and 20mb are optimum performance file chunk size 2048 bit other file chunks size.

Figure 5.1 it is represented in graphical form to show a statistical view.

5.2 Download file:- File chunks and chunking time compare with different chunking size, decryption algorithm.

Table5.2

	File	file size(kb)	RC6 Key Size(Bit)	Blowfish Key Size(Bit)	MD5 Key Size(Bit)	file chunk 512 bit	Chunking Time(ms)	file chunk 1024 bit	Chunking Time(ms)	file chunk 2048 bit	Chunking Time(ms)
decryption crypto time	text	5120.9	192	128	128	10242	238301	5121	17228.202	2561	9180.175
decryption crypto time	text	10241.8	192	128	128	20484	121607	10242	80427.111	5121	40967.67
decryption crypto time	text	15362.7	192	128	128	30726	391174	15363	234441.68	7682	113813.3
decryption crypto time	text	20483.61	192	128	128	40968	475108	20484	518063.84	10242	253727.9
decryption crypto time	uuux	5163.8	192	128	128	10328	48281	5164	17803.99	2582	64600.23
decryption crypto time	docx	10406.64	192	128	128	20814	119343	10407	88406.442	5204	159655.4
decryption crypto time	docx	15544.55	192	128	128	31090	429386	15545	245621.6	7773	311534.3
decryption crypto time	docx	20754.97	192	128	128	41510	896379	20755	520315.42	10378	662873.6



When Different file size Downloading in application running on amazon web service, symmetric algorithm are reverse process when downloading.

Retrieval Number: 100.1/ijitee.L932411111222
DOI: 10.35940/ijitee.L9324.11111222
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

file size 5mb,10mb, 15mb and 20mb used in downloading table- 5.2 and show graphical form. Downloading time is taking more than uploading time.

5.3 Upload file:- Uploading file size, when change the key size used RC6-128 and Blowfish-256, encryption algorithm.

Table-5.3

	File	file size(kb)	RC6 Key Size(Bit)	Blowfish Key Size(Bit)	MD5 Key Size(Bit)	file chunk 512 bit	Chunking Time(ms)	file chunk 1024 bit	Chunking Time(ms)	file chunk 2048 bit	Chunking Time(ms)
decryption crypto time	text	5120.9	128	256	128	10242	9861.41	5121	4057.811	2561	3474.96
decryption crypto time	text	10241.8	128	256	128	20484	18485.1	10242	9149.679	5121	6511.559
decryption crypto time	text	15362.7	128	256	128	30726	27196.7	15363	13434.159	7682	8743.579
decryption crypto time	text	20483.61	128	256	128	40968	33731.8	20484	21549.972	10242	10994.1
decryption crypto time	docx	5163.8	128	256	128	10328	8865.31	5164	6592.467	2582	3743.114
decryption crypto time	docx	10406.64	128	256	128	20814	16694.5	10407	12228.581	5204	7760.715
decryption crypto time	docx	15544.55	128	256	128	31090	23889.4	15545	24506.414	7773	10432.89
decryption crypto time	docx	20754.97	128	256	128	41510	41704.2	20755	24280.89	10378	10274.78

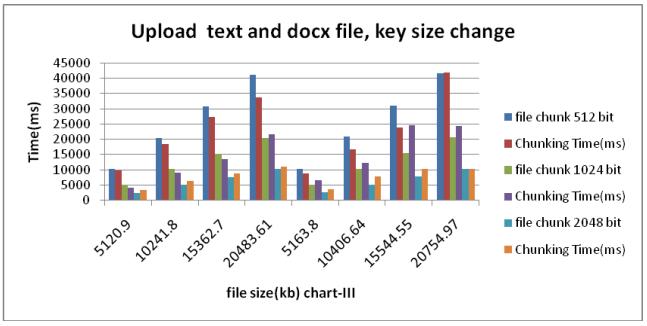
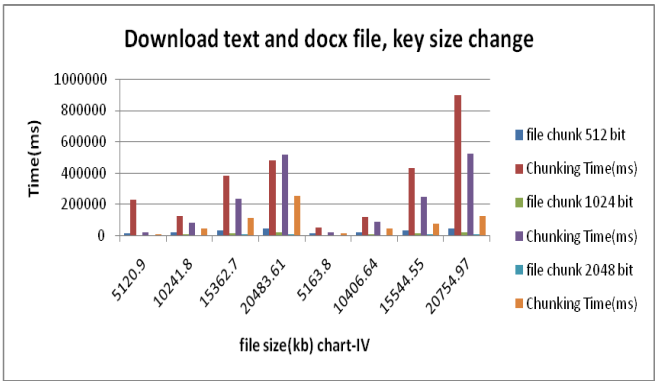


Table-5.3 Encryption executive time Symmetric crypto algorithm key size change RC6-128 bit and Blowfish-256 bits executive time improve uploading file. Figure 5.3 Show the graphical form.

5.4 Download file:- Decryption file size, when change the key size used RC6-128 and Blowfish-256 used in Downloading file.

Table5.4

	File	file size(kb)	RC6 Key Size(Bit)	Blowfish Key Size(Bit)	MD5 Key Size(Bit)	file chunk 512 bit	Chunking Time(ms)	file chunk 1024 bit	Chunking Time(ms)	file chunk 2048 bit	Chunking Time(ms)
decryption crypto time	text	5120.9	128	256	128	10242	228310	5121	17126.456	2561	8976.175
decryption crypto time	text	10241.8	128	256	128	20484	123616	10242	80316.153	5121	40558.29
decryption crypto time	text	15362.7	128	256	128	30726	382771	15363	233452.62	7682	113120.8
decryption crypto time	text	20483.61	128	256	128	40968	478123	20484	517172.58	10242	251449.8
decryption crypto time	docx	5163.8	128	256	128	10328	47290	5164	17158.184	2582	10889.26
decryption crypto time	docx	10406.64	128	256	128	20814	118314	10407	87416.698	5204	44330.47
decryption crypto time	docx	15544.55	128	256	128	31090	428385	15545	244637.66	7773	72445.6
decryption crypto time	docx	20754.97	128	256	128	41510	893621	20755	520202.69	10378	122630.7



Above shown table-5.4 and figure-5.4 are display Execution time variations Symmetric crypto algorithm key size change RC6-128 bit and Blowfish-256 bits executive time are improved in downloading file.

Existing solution are file size maximum 10 mb, file chuking size not change and key size also not change. So do not compared over proposed solution.

VI. COMPRATIVE RESULT ANALYSIS

File uploading Execution Times better than Downloading Execution Times. RC6 and Blowfish Algorithm Key size change, variations of Uploading Downloading Execution Times. When RC6 Key size 192, Blowfish key size 128 use less execution time in text and docx file Variation of key size change better execution time 20mb docx file.

Administrative decided File chunks size 512,1024 and 2048 bit (we are file size divided into 512 bit, 1024bit, 2048 bit)File size 5mb,10mb,15mb,20mb better perform of execution time use in file chunking size 2048 bit. text and docx file encryption crypto time better than decryption crypto time .If file chunking size greater than execution time less in Upload and download Process. The lesser file size, less execution time. RC6 and Blowfish fast data encryption and Less Memory use, key size RC6 128-256 bits and Blowfish key size 32-448 bits. RC6 and Blowfish more secure other symmetric algo. MD5, 128 bit digest size for single input and fast calculation,32 hexadecimal digit generate.

VII. CONCLUSION

Amazon web service (cloud computing) obviously offers various facility and numerous advantages, other than it also has many issues. Conventional encryption methods do not guarantee accurate and reliable data protection. The raise in internet use and automation of regular industry influence the way of business. Client always demand for security and data privacy.

They always demand to keep their data safe and secure. AWS are best performance network, rest data in provide strong security. Kerberos server is the solution for network security problem since it provides strong security secret key over the insecure network. Using BLOWFISH and RC6 algorithm with splitting data into chunks and encrypting even and odd chunks with cryptographic technique. The integrity (MD5) of file or data. We Achieved Authentication, confidentiality, Integrity one solution of application in cloud computing with AWS. Deploy Application at AWS Environment. Dependent Execution time on system configuration and internet speed. One year free EC2 instance Application at t2. Micro AWS environment and after minimum cost pay use service, We used cipher file upload and download for confidentiality, integrity strong security service.

Limitation these cloud Application are provide only uploading and downloading file service for text and docx file, Cloud application parameter used for only amazon web service instance.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In the Future Implement different file type uploading and downloading for JPG, PDF, XlSX, etc**.** Also Implement Application various Symmetric and Asymmetric Algorithm use in amazon web service security instance**.**

REFERENCES

1. Sakshi Narula, Arushi Jain, Prachi (2015) Cloud Computing Security: Amazon Web Service. Fifth International Conference Advanced Computing & Communication Technologies. https://doi.org/10.1109/ACCT.2015.20 [CrossRef]
2. Monika Gogna (2018) comparison of x.509, Kerberos 5 and PKINIT for open distributed network. Journal of Emerging Technologies and Innovative Research. www.jetir.org (ISSN-2349-5162)
3. P. Princy (2015) A comparision of symmetric key algorithm AES, DES, 3DES, BLOWFISH, RC4, RC6: A survey. International Journal of Computer Science & Engineering Technology 2229-3345
4. D Rachmawati et al(2017) A comparative study of Message Digest 5(MD5) and SHA256 algorithm. 2nd International Conference on Computing and Applied https://doi.org/10.1088/1742-6596/978/1/012116 [CrossRef]
5. Piyush Gupta et al (2014) A Comparative Analysis of SHA and MD5 Algorithm. International Journal of Computer Science and Information Technologies 0975-9646
6. Dr. D.I. George Amalarethinam et al (2016) Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud. 2016 World Congress on Computing and Communication Technologies 978-1-5090-5573-9. https://doi.org/10.1109/WCCCT.2016.50. [CrossRef]
7. Swedha.K, Tanuja Dubey (2018) Analysis of Web Authentication methods using Amazon Web Services., IISC – Bengaluru 18166993. https://doi.org/10.1109/ICCCNT.2018.8494054, [CrossRef]
8. Shrujana Murthy, Kavitha C.R (2019) Preserving Data Privacy in Cloud using Homomorphic Encryption. Proceedings of the Third International Conference on Electronics Communication and Aerospace Technology 978-1-7281-0167-5 [CrossRef]
9. Milind Mathur, Ayush Kesarwani (2013) Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES. Proceedings of National Conference on New Horizons in IT 978-93-82338-79-6
10. M. Harini, K. Pushpa Gowri, C. Pavithra, M. Pradhiba Selvarani (2017) A Novel Security Mechanism Using Hybrid Cryptography Algorithms. International Conference on Electrical, Instrumentation and Communication Engineering 17430972. https://doi.org/10.1109/ICEICE.2017.8191910 [CrossRef]
11. Kirtiraj Bhatele, Prof Amit Sinhal, Prof Mayank Pathak(2012) A Novel Approach to the Design of a New Hybrid Security Protocol Architecture. International Conference on Advanced Communication Control and Computing Technologies 4673-204846 [CrossRef]
12. Neha Gupta, Vivek Kapoor (2020) Hybrid cryptographic technique to secure data in web application.Journal of Discrete Mathematical Sciences and Cryptography. https://doi.org/ 10.1080/09720529.2020.1721872 [CrossRef]
13. Arpana Kumari, Vivek Kapoor (2020) Competing secure text encryption in intranet using elliptic curve cryptography. Journal of Discrete Mathematical Sciences and Cryptography. https://doi.org/ 10.1080/09720529.2020.1729509 [CrossRef]
14. Ali Kadhim Bermani et al (2021) A hybrid cryptography technique for data storage on cloud computing. Journal of Discrete Mathematical Sciences and Cryptography. https://doi.org/ 10.1080/09720529.2020.1859799 [CrossRef]
15. Mohammed Nazeh Abdul Wahid et al (2018) A comparison of cryptographic algorithms: DES,3DES,AES,RSA and Blowfish for Guessing Attacks Precention. www.symbiosisonlinepublishing.com ISSN Online: 2474-9257
16. DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan (2017) Study on Data Security Policy Based On Cloud Storage. IEEE 3rd International Conference on Big Data Security on Cloud 978-1-5090-6296-6. https://doi.org/10.1109/BigDataSecurity.2017.12 [CrossRef]
17. Zachariah Pabi Gariba et al (2017) Security failure trends of cloud computing. 2017 IEEE 3rd International Conference on Collaboration and Internet Computing 0-7695-6303-1. https://doi.org/ 10.1109/CIC.2017.00041
18. Jun Feng et al (2010) Bridging the Missing Link of Cloud Data Storage Security in AWS. IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2010 proceedings 978-1-4244-5176-0 [CrossRef]
19. Zain Ul Abedin, et al (2019) An Advance Cryptographic Solution in Cloud Computing Security. 2019 ICOMET-978-1-5386-9509-8. [CrossRef]
20. Haosila Yao, et al (2022) Data Storage Security System based on Cloud Computing. 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference. https://doi.org/10.1109/ITAIC54216.2022.9836548 [CrossRef]
21. Deepika et al (2022) Security Enabled Framework to Access Information in Cloud Environment. 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing. https://doi.org/10.1109/COM-IT-CON54601.2022.9850906 [CrossRef]
22. Chitra Biswas, Udayan Das Gupta (2019) An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography. International Conference on Electrical, Computer and Communication Engineering 978-1-5386-9111-3 [CrossRef]
23. Mansoor Ebrahim et al (2013) Symmetric Algorithm Survey: A Comparative Analysis. International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.
24. Diaa Salama Abdul et al (2008) Performance Evaluation of Symmetric Encryption Algorithms. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008. [CrossRef]
25. U. Thirupalu et al (2019) Performance Analysis of Cryptographic Algorithms in the Information Security. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 NCISIOT - 2019 Conference Proceedings.

AUTHORS FROFILE

Madan Solanki, ME (IT) Department of Information Technology Specialization Information Security, in Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya Khandwa Road Indore-452017 (M.P.) India. currently working as Lecturer at Govt. Polytechnic College Ujjain, department of information Technology. Having a 09 year of experience in teaching. Interested area cloud computing, cyber security, IoT, Deep Learning. My strengths are disciplined, Believe hard work. mdvda112@gmail.com

Dr. Vrinda Tokekar, Phd, Professor and Head of Department In Information Technology, Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya Khandwa Road Indore-452017 (M.P.) India. **Research Area:** Computer Networks, Wireless Network Protocols, Network and Information Security, Software Engineering and Phd Guide, Email: vtokekar@ietdavv.edu.in