Hybrid Encryption based SHA2-256 Integration Techniques for High Security for Data Stored in Cloud Environment

Keerti Verma
Dept.Computer Science and Engineering OIST, Bhopal

Sreeja Nair
Dept.Computer Science and Engineering OIST, Bhopal

ABSTRACT
Cloud Computing is the pool of shared resources provided to the user by the Cloud service providers. Many software or application programs are made available to the user at low cost and the deployment environment also provided by the third party cloud providers which are having a full control over the application settings. Since user has no control on the settings of application programs there is always be trust and security issues. The data on the remote cloud server is not secure as a large amount of data is moving to and fro between large number of authorized and unauthorized users. The data can be easily modified by the intruders in the public deployment environment. Thus the using of security algorithms like makes it easier for the security of data to user.

General Terms
AES Encryption ,obfuscation ,Secure Hash Algorithm

Keywords
Cloud Computing, Data Security,integrity.

1. INTRODUCTION
For maintaining the data and software applications on the central remote servers there is use a technology called Cloud Computing. It allows the user to access their data which are saved on central remote servers using internet. It is and architecture of shared pool computing resource provided to the user to store their data which can be rapidly released with less managerial effort or clod provider interaction. Users have full access on featured applications provided by the cloud on rent. They can built application programs, deploy software and various applications at low cost. The data storage is the main feature which is provided by the cloud to the user with the use on internet and to computing infrastructure like network accessible data storage. Cloud Computing is basically an Information Technology Services provided to the User through Internet. Some of the leading large companies which are providing cloud computing services to the user are Google, Yahoo, Amazon and YouTube [1]. Cloud Computing uses the concept of virtualization that means hiding the detailed information and only showing the useful application information or providing only the network deployment environment. These deployment models of Cloud Computing are divided into three parts they are as follows

Public, Private and Hybrid. In the Public deployment environment, the services provided to the user by cloud are having full control of service provider and user can only use services on rent so the data stored on public cloud are less secure as there exists a large number of users' data which can be accidently or intentionally changed or lost. Private Deployment environment are the cloud services owned by the organization and the data in private cloud are more secure than public cloud as the data can move to and fro in public cloud in the network. Hybrid Cloud possess more than one deployment environment [2][3].

2. SERVICE MODELS OF CLOUD
There are three services models provided by the Cloud Computing Technology and they are as follows: Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) [4][5][6].

2.1 PaaS model
The platform to deploy the application programs or software are provided to the user by the cloud. Only the application program settings controls are given to the user and the physical settings are restricted by the service provider.

2.2 SaaS model
The software services are provided by the service provider to the end users only the application can be install and run by the user but cannot be changed as the infrastructure and physical setting controls are under service provider.

2.3 IaaS model
The blueprint or the infrastructure is provided to the user on which the application or software programs can be built and deployed. In this model the online data storage, servers and networking components are all provided by the cloud service provider.

3. SECURITY ISSUES
As the Cloud Computing is the fast growing technology, it has many new challenges with it. The main feature of cloud computing is its data storage service which has brought many small enterprises to a leading growth. There are lots of security issues in cloud data storage service which has to be look after and curbed [7].

Trust is the main issue as the user is not sure of the service provided by the cloud service provider is ethical or not. As the data can be modified or not secured by the intruders. There is a agreement between the user and the cloud service provider which is known a s Service Level Agreement (SLA) document. There is no standard maintained for the SLA that is why the trust issue is there in cloud environment.

Confidentiality [8] [9] of the data is again another security issue in Cloud computing as the important and sensitive data which need to be prevent from disclose. It is a big issue for which so many methods are used to protect confidential information like encryption and cryptography technique. These methods are really expensive and time consuming but to keep the data safe in cloud storage there is a need of them.

Authentication and data integrity is also another security issue as the data modification by the third party or intruders attacks can be possible. There is a need to verify each and every user control to the cloud data storage. For which encryption techniques are always built to work on it. It can also be resolved by using digital signature.

4. SECURITY ALGORITHM IN CLOUD

There are many security algorithms used in Cloud Computing using the various cryptography methods instead on any one to enhance the performance. In cryptography the data before sending to the cloud storage is encrypted using the encryption algorithms and decrypted back when the data is needed by the user using the secrete key. Some of the encryption algorithms used in cloud computing are [10][11] [12] [13].

4.1 RSA Algorithm

Rivest, Shamir and Adlem (RSA) algorithm is the most common public key generation algorithm it is named after all the three inventors. This is a block cipher algorithm which is asymmetric encryption and decryption algorithm in which there is one public key provided by which data can be encrypted but it can only be decrypted by the private key which is kept secret that is not distributed to everyone. This RSA algorithm is working in cloud environment to secure data by providing authentication to only authorized users and preventing the intruder to attack the data. In cloud environment after the encryption of the data is done it can be stored in cloud data storage and when the user demand to access the data it is must to request the cloud service provider. After the authentication is done by cloud service provider the data can be access by the user.

4. 2 AES Algorithm

Advanced Encryption Standard (AES) algorithm is the symmetric block cipher and named as Rijindael also. It uses substitution permutation design network. All the computation is done on the bytes hence 128 bits of plain text is treated as 16 bytes block. They are then arranged in 4*4 matrixes. The number of rounds for the computation in AES is variable and totally depends on the Key. It uses 10 rounds for 128 bit key and 12 rounds for 192 bit key. Different 128 bit key are used in each round of AES that are to be calculated from original AES key. This algorithm is used very much now-a-days due to security issues in cloud. In this user who wants to use cloud services will drift his data on cloud than the services requirement are submitted to the cloud service provider by the user. In this case whenever the data is to be stored by the user to the chosen cloud service provider is encrypted first using AES. In future when the data is requested to read it can only be done at the user end after the decryption of the data into plain text. Any data in the form of plain text is never written on cloud anywhere. This encryption solution can be integrated quickly and with ease without change into the application. The key generated in this algorithm is never kept next to the encrypted data. The key can be kept at the users' end using any physical key management on the server. For many applications AES has replaced DES as approved standard.

4.3. DES Algorithm

Data Encryption Standard is the symmetric key algorithm used for encryption and decryption of plain text. It has a 56-bit key size which is small and considered to be insecure. It uses 64bit data of block size for the encryption and generates 64-bit cipher text with 16 rounds of 56-bit key. For encryption and decryption both uses the same algorithm with very minor difference. That is why the security of the data is less due to only 64–bit encryption block cipher used. It also lower the performance of the data storage in Cloud Computing.

4.4 Blow Fish Algorithm

It is a symmetric algorithm which uses variable length 128-448bit which makes it more secure to the data. It is designed because the rate of encrypting the data at 32-bit microprocessor is 26 clock – cycles per byte which is really fast. It is compact as the execution of it requires only 5kb. It is also very simple to use as it provides basic operations like addition, XOR and table look up. The applications which requires key to be remains constant for long are suited by Blowfish but not where the key is changing.

5. RELATED WORK

Cloud Computing is metamorphoses information technology. Not only is the computation done also how it is achieving it while converting the information or data to the cloud. It has solved many problems like handling the peak loads and software update installation. But the technology along with ease brings up many new challenges like data storage security which can be achieved by many metaphoric security algorithms [14].

Cloud Computing is constructing an IT services which demands advanced computational power and not only the storage capabilities. It is new technology which is not the single system that can be describe but also very problematic in terms of security.. But there security issues can be solved by using some security algorithms like Diffie-Hellman Key Exchange and TDES algorithms that can also be combined along with RBAC methodology to avoid any intruder to access the sensitive data on the cloud storage [15].

Cloud Computing is the new generation attraction which has provided many IT services to the user at low cost. The main feature of cloud computing is its data storage at remote server which has lowered the burden of big data handling in traditional way. But security is always the issue to deal with in Cloud Computing. To overcome form the security of data in cloud environment RSA algorithm can be applied as it works on public key generation encrypting methodology. It is also very cost efficient and time consuming [16].

Cloud Computing makes the resources available to the user at low cost as some resources need huge investment to be used. As the resources are available in large amount the accessibility of that is also increased which tends the risk of malicious damage to sensitive data. Security of data in cloud environment is thus a major issue as the data can be accessed by any user. The data at the remote servers are under the control of third-party service provider which has a full control over it. It can be avoided by using some security algorithms like Blow Fish whish has a variable length key and fast in response [17].

6. PROPOSED WORK

This section deals with proposed work. This section contents two points which explain and express the proposed work. First thing is algorithm. How things are going in this proposed work is explain in the form of step by step explanation is covered here. Second portion handles flow chart of the proposed work.

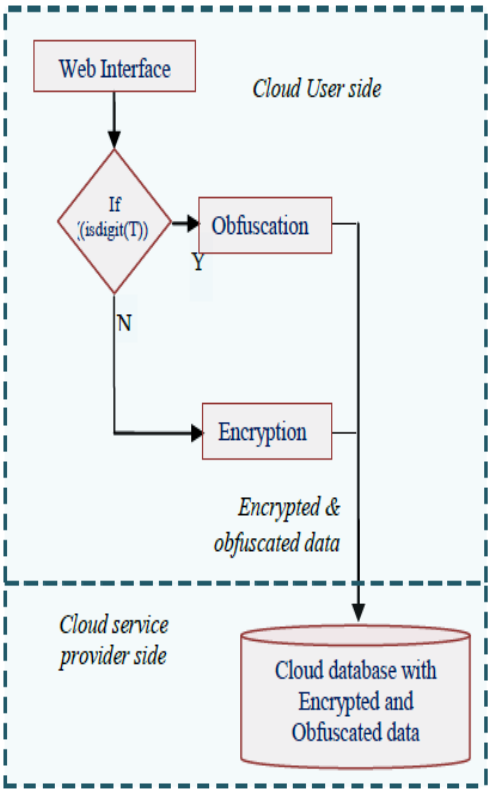


Fig 1: Proposed Technique for Cloud Storage Confidentiality using Encryption and Obfuscation

Step -1 Input The text
Stepc-2 Check for NUMERIC or ALPHANUMERIC input
Step -3 if(input==NUMERIC) //perform obfuscation
Step -4 array = {'a', 'b', 'c'}
Step -5 for(i=0 to lengthOfarray)
Step -6 ascii1 = (Input.charAt(i) + array[index++])
Step -7 BINARYSTRING = Convert ascii1 to binaryString
Step -8 Alter LSB bit of BINARYSTRING(0to1 or 1to0)
Step -9 output[i] =Convert BINARYSTRING to INTEGER
Step -10 Index = index%3 z
Step -11 END for
Step -12 CipherText = convert output array to string
Step -13 ELSE //AES-Encryption
Step -14 KEYINBYTEs = convert key into bytes
Step-15 CipherCiphertext = Cipher.getInstance("AES/CBC/PKCS5Padding")
Step-16 Ciphertext.init(Ciphertext.ENCRYPT_MODE, SecretKeySpec)
Step-17cipherInBytes = Ciphertext.doFinal(plainTextInBytes)
Step -18 ByteoutputStream.write(cipherInBytes);
Step -19 finalData = ByteoutputStream.toByteArray
Step -20 EncodedFinalData = convert finalData to String
Step -21 CipherText = EncodedFinalData
Step -22 END
Step -23 md = create MessageDigest
Step -24 md.update(CipherText.getBytes)
Step -25 byteData[] = convert MessageDigest into bytes
Step -26 for (i=0 to byteData.length)
Step -27 hex = convert byteData[i] to hexadecimal
Step -28 if (hex.length() == 1)
Step -29 hexString.append(0)
Step -30 END if
Step -31 hexString= append hex to final string
Step -32 END for
Step-33 SHAOutput = hexString
Step -34 String = CipherText + SHAOutput+KEY
Step-35 md = create MessageDigest
Step -36 md.update(String.getBytes)
Step -37 byteData[] = convert MessageDigest into bytes
Step -38 for (i=0 to byteData.length)
Step -39 hex = convert byteData[i] to hexadecimal
Step -40 if (hex.length() == 1)
Step -41 hexString.append(0)
Step -42 END if
Step -43 hexString= append hex to final string
Step -44 END for
Step -45 SHAFinalOutput = hexString
Step -46 FinalCipherText = SHAFinalOutput // Round off the square value

7. RESULT ANALYSIS

This section is dealing with System and software configuration along with the software requirement in first section.

Table 1: System Configuration

Processor	Dual Core
RAM	4 GB
CloudSIM	3.0.3
OS	Window7

Table 2: Various Plain Texts

S.NO	CODE	INPUT TEXT
1.	PT-1	ape from Old English apa is a word of uncertain origin
2.	PT-2	wildlife is an invaluable treasure but it is being exploited due to illegal trade of many of its species
3.	PT-3	the present era is classified as part of a mass

Table 3: Various Keys

S.NO	CODE	KEY
1.	K1	abcdefabcdefabcd
2.	K2	efabcdeabcddefab

Table 4: Various Decryption Time with K-1

Input Text	Key	Existing Work Decryption Time(ns)	Proposed Work Decryption Time(ns)
PT-1	K-1	223814	485171
PT-2	K-1	452441	720537
PT-3	K-1	192047	476026

Table 5: Various Decryption Time with K-2

Input Text	Key	Existing Work Decryption Time(ns	Proposed Work Decryption Time(ns)
PT-1	K-2	213225	480840
PT-2	K-2	434151	510681
PT-3	K-2	184827	469769

Table 4 shows the decryption time required by the proposed work along with the existing work with Key 1 and Table 5 shows the same thing with key 2. The higher value of the decryption time shows that proposed work will take higher time to decode the original text. This thing will provide better security against any text. These various texts are already shown through PT-1, PT-2 and PT-3. The whole process is graphically shown by Graph 1 and 2.

Avalanche Effect It is a quantity which measures the effectiveness of the algorithm or in other words we can set sensitivity of any algorithm. The higher value of it shows the effectiveness of the algorithm.

Avalanche Effect = Number of bits change in cipher text / Number of bits in cipher text

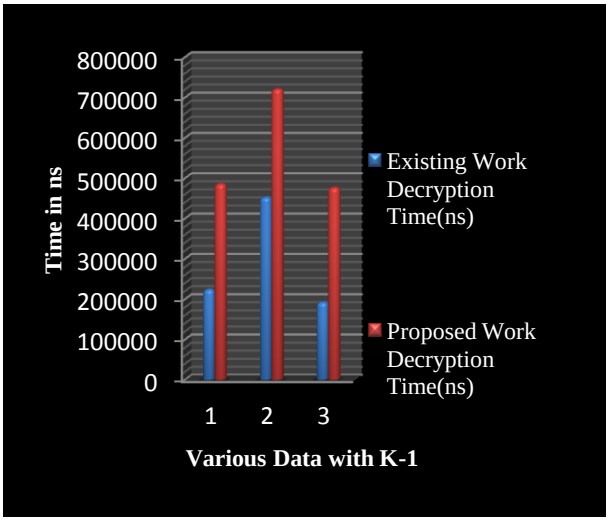
Table 6: Various Avalanche Effects with K-1

Input Text	Key	Existing Work Avalanche Effect	Proposed Work Avalanche Effect
PT-1	K-1	36	272
PT-2	K-1	65	484
PT-3	K-1	19	210

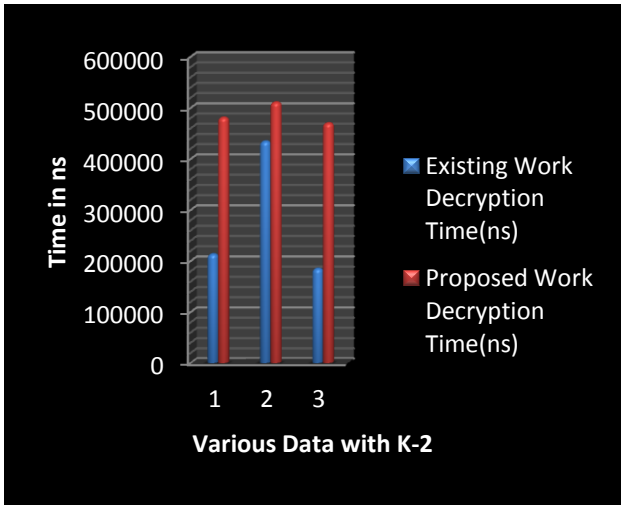
Table 7: Various Avalanche Effects with K-1

Input Text	Key	Existing Work Avalanche Effect	Proposed Work Avalanche Effect
PT-1	K-2	29	288
PT-2	K-2	39	466
PT-3	K-2	24	203

Table 6 and 7 along with the graph 3 and 4 show that the proposed work is having higher avalanche effect and graph shows comparison between proposed and existing Avalanche effect. Here it is needed to mention that proposed work is having variable avalanche effect as it is use AESs-256 encryption algorithm which itself is dynamic in nature. We have mentioned a random value in these table but all value are much better than available avalanche effect for existing work.

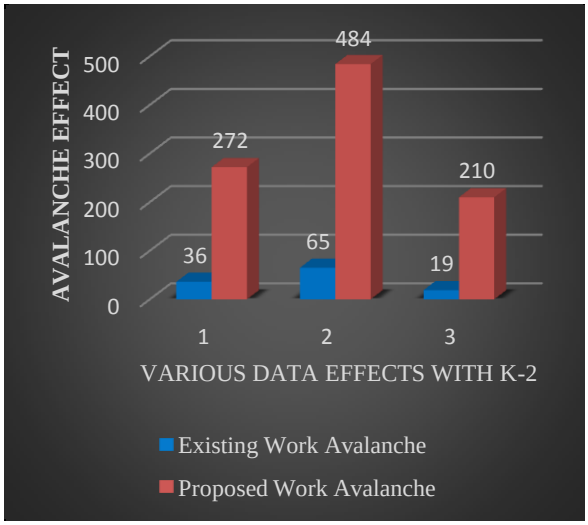


Graph 1: Various Decryption Time with K-1



Graph 2: Various Decryption Time with K-2

Graph 3: Various Avalanche Effect with K-1



Graph 4: Various Avalanche Effect with K-2

8. CONCLUSION

Cloud Computing has provided many benefits to the user. It is a widely used technology which provided many services and deployment environment to the user. But the security issues in cloud are directly related to the advantages provided by the Cloud. It is very much profitable for both the business purpose and the intruders as they can track the sensitive data. Many security algorithms are proposed for the security of data in the remote server of cloud environment like RSA, Blow Fish and TDES. The current schemes or security algorithms are efficient to secure the data but many aspects can also be recovered by new researches. Table 2-7 along with the Graph 1-4 clearly show the effectiveness of the proposed work. Here the efficiency of the proposed work is evaluated on the parameter of the Decryption Time along with Avalanche Effect.

9. REFERENCES

[1] Karandeep Kaur, "A Review of Cloud Computing Service Models," International Journal of Computer Applications (0975 – 8887), Volume 140 – No.7, April 2016.

[2] M. Chandni Jain," Cloud Computing: Network/Security Threats and Counter measures," international Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015.

[3] Roman Nedzelský,"Hybrid Cloud Computing: Security Aspects and Challenges," 2016.

[4] Imran Ashraf, "An Overview of Service Models of Cloud Computing," International Journal of Multidisciplinary and Current Research, July/Aug 2014.

[5] Dimpi Rani and Rajiv Kumar Ranjan," A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering," Volume 4, Issue 6, June 2014.

[6] Polshetwar Poonam and Saad Siddiqui," Comparison of Cloud Computing Service Models: SaaS, PaaS, IaaS," International Journal & Magazine of Engineering, Technology, Management and Research, Volume No: 1(2014), Issue No: 11 (November).

[7] Diogo A. B. Fernandes, Liliana F. B. Soares, Jo~ao V. Gomes, M´ario M. Freire and Pedro R. M. In´acio," Security Issues in Cloud Environments | A Survey," International Journal of Information Security (IJIS, 2013.

[8] Ms. Disha H. Parekh and Dr. R. Sridaran,"An Analysis of Security Challenges in Cloud Computing," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013.

[9] Abhinay B.Angadi, Akshata B.Angadi and Karuna C.Gull," Security Issues with Possible Solutions in Cloud Computing-A Survey," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

[10] Dr. Nandita Sengupta,"Designing of Hybrid RSA Encryption Algorithm for Cloud Security, "International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2015.

[11] Abha Sachdev and Mohit Bhansali," Enhancing Cloud Computing Security using AES Algorithm," International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.

[12] Garima Saini and Naveen Sharma," Triple Security of Data in Cloud Computing," International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014.

[13] Rachna Arora and Anshu Parashar," Secure User Data in Cloud Computing Using Encryption Algorithms," International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, Jul-Aug 2013.

[14] Deepika Verma and Er. Karan Mahajan," To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithm," International Journal of Advances in Science and Technology (IJAST), Vol 2, Issue 4 (December 2014).

[15] Aized Amin Soofi, M. Irfan Khan and Fazal-e-Amin,"Encryption Techniques for Cloud Data Confedentiality," IJGDC, Vol. 7, No. 4, 2014.

[16] V.Masthanamma and G.Lakshmi Preya," An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm," International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, March 2015.

[17] Parsi Kalpana and Sudha Singaraju," Data Security in Cloud Computing using RSA Algorithm," Parsi Kalpana, et al, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.