International Journal of
Science Inventions Today
www.ijsit.com
ISSN 2319-5436
Research Article

AN IMPROVED SECURE MODEL FOR CLOUD DATA STORAGE

Ewulonu O. V[1], Nwachukwu E. O[2] and Onyejegbu L N[3]

Department Of Computer Science, University Of Port Harcourt, Nigeria

ABSTRACT

Scientific computing has metamorphosed to a dimension where phenomenal data are reposited in cloud for safe storability, which make data readily available for decision making. Cloud computing is recent computing paradigm and innovation that has removed the danger of unexpected data loss. But cloud computing adoption and diffusion are threatened by unresolved security issues that affect both the Cloud provider and the cloud user especially in the area of cloud data storage. Security becomes an essential issue. A secure data storage is needed in cloud computing to lower the risk involved in moving sensitive data to cloud storage environment. This thesis is aimed at developing an improved secure model for cloud data storage. The methodology employed in our research is Object–Oriented Analysis and Design(OOAD) and experimentation in conjunction with selected sub set of Unified Modelling Techniques. The technique used in solving the existing security issues are: triple Advanced Encryption Standard (3AES) algorithm and Audio Steganography mechanism to provide a multi layered data security. Experimental data from our software; based on the proposed improved secure model for cloud data storage were collected and presented in tables with existing experimental result data of Kirubakaramoorthi *et al. (*2015). These data were plotted in line graphs for observation and inference. It was observed that cryptography techniques combined with audio steganography of the proposed system reduce time of downloading and uploading files more than existing system, and ensure data integrity and confidentiality in cloud computing environment.

INTRODUCTION

There is expanding consideration given to processing in cloud in the scholarly world and business conditions as of late. Numerous specialists, have perceived the possibility of capacity of information in cloud information, which characterizes Capacity as a Service (DaaS) idea. Be that as it may, the colossal development of data, have also increment desire for many institutions and associations to put into thought where to safeguarded, oversee and get to information instantly, and how these information could be secured legitimately. Registering in cloud is late paradigm resulting from years of logical research on conveyed Figuring, virtualization, systems administration, and web programming administrations. It is regular development of the across the board selection of virtualization, benefit arranged engineering, autonomic and utility calculation (Nikita and Toshi, 2014). This zone of registering is in help of making new level of applications running on blame resistant hardware gadgets that include: keen phones; mobile gadgets and tablets or Personal Digital Assistants (PDAs); utilizing distributed storage innovation in information storability. This new innovation is required in our establishments as instruction request is continually expanding because of advances and positive difference in e-grounds arrangements.

Besides, it is basic for e-grounds frameworks to meet the current pattern in innovation. Training establishments are excited at the capability of organizations to take their striking information from administration and physical framework, and offer consideration regarding center abilities of the advancement of storability of information in the cloud. The readiness gave by processing in cloud energizes establishments the most. However, various establishments of learning, associations, and people, managing cosmic information are concerned more on the Figuring in cloud, is related security dangers, especially away of information, as disgracefully secured information may influence them to encounter fractional loss of control of framework that usually they ought to be very responsible for. Among the quickly developing zones of data innovation is cloud (Boroujerdi and Nazem 2012).

Processing in cloud innovation offers a definitive blend of facilitating stage and web stockpiling administrations (Abhinay et al., 2013). Processing in cloud gives adaptable and modest Figuring framework, which conveys subjective administrations when required, and helps in actualizing on the web applications forquality yield. At last, registering in cloud objective is the arrangement of versatile and shabby Figuring foundation when required that likewise conveys abnormal state quality administrations (Harjit and Gurdev 2012).It accompanied web, which has given simple access to processing destinations that are remote. This much of the time utilizes web-arranged applications or devices, which clients have full access to through web programs which gives the inclination that they have the program introduced on remote hosts frameworks.

The National Foundations of Principles and Innovation (NIST) gave more destinations and rational meaning of processing in cloud, as a model that empowers helpful, availability to conFigureurable pool of

registering assets shared on systems comprehensively, web servers, stockpiling applications that are promptly given and endeavored of administration or connections of suppliers of web administrations. Run of the mill suppliers of Figuring in cloud conveys applications for business that are normal on the web, and that could be gotten to by means of Web programs, while putting away the product and the information on the server. Numerous individuals see Figuring in cloud as administration that is required in various ways and one in each three people uses it. Numerous individuals are constantly moving information into cloud for its adaptability. It is decreed to be an application to effectively use in associations for its application, which assign space for expansive information stockpiling and simple availability to the put away information when required. Because of the expanding level of individuals putting away their imperative and individual information in cloud, putting away the information securely is likewise turning into a genuine concern (Ramaporkalai, 2017). Information security under capacity is anticipating numerous associations, multinationals and foundations from exchanging their information that are delicate to cloud.A Salient concept of data storability is encryption in trusted environment before using cloud storage resource. There are range of encryption algorithms, which have proven secure, which can perform encryption/decryption operations e.g. AES, Serpent and blowfish. Theoretically, algorithms for symmetric key cryptography and asymmetric key cryptography are used for secure data storing in cloud but the latter is slower than the former. However, for performance measurement, symmetric algorithms are preferred. Encryption guarantees confidentiality of stored data and detects any corruption in data.

Major issue of secure storage is management of keys for encryption, because once data is encrypted, keys become the true bits to secure, and if keys are deposited in environment not trusted with data, an intruder can access data and keys to decrypt confidential data. The cryptography method for protecting information is called encryption.

The major debacle to encryption is that data is not hidden, because data encrypted although unreadable still exists, and if hacker is given enough room, he may eventually cryptanalyze the encrypted data. A way out of this debacle, is steganography. Steganography is science and art concealing information into obscure channels to code the information and prevent the anyone from understanding the concealed message.

MATERIALS AND METHODS

We embraced the Advanced Encryption Principles (AES) cryptography, and steganographic systems for our proposed show. AES cryptographic system, for classification of put away operational information and steganographic method called LSB sound steganography is utilized to keep up information trustworthiness. Furthermore, Microsoft Purplish blue is cloud stage of our execution.

Jasleen and Sushil (2016) says, cloud information insurance may utilize half and half of algorithms

and their exploration concentrated on presenting novel algorithmic structure made of two calculations: RSA as computerized mark and blowfish calculation, give assurance to put away information in cloud as they transfer or download from cloud. The disadvantage here, is that, to give clear security confirm while transferring and downloading information in multi-cloud.

Parsi and Sudha (2012), proposed Information Security in registering in cloud utilizing RSA Algorithm and they repeated that Figuring in cloud is a rising innovation and is quick turning into the most sizzling territory of research. To secure information in cloud, RSA calculation has been executed to give the required security. Their examination work and process includes encryption of information in cloud, and when the information is required for decoding then the mists cloud suppliers confirm client and information been unscrambled. The downside is that a pernicious cloud-administrations supplier can spy or take customers information

Rashmi and Deepali (2015) developed Design for security of information in Multi-cloud utilizing AES-256 Encryption Calculation portrayed for putting away of information in multi-cloud. Their work utilize two components information encryption and document part. At the point when clients transfer document, encryptions are finished with AES encryptions calculations, the scrambled record, is afterword separated into two as indicated by mists and kept in multi-cloud. This model, secured information in multi-cloud effectively. The downside of the model is that 256-word length of AES encryptions is to short and could be broken after time of industriousness of programmers.

Izevbizua (2015) proposed security for information in cloud utilizing serpents encryption and disseminated steganography as effectively existing path for concealing information. Izevbizua (2015) utilized a component to guarantee security for information by vital utilization of serpent cryptographic calculation and dispersed steganography. The combined approach is pointed at gathering the quality of these two demonstrated procedures to accomplish a strong system for guaranteeing privacy and respectability of information in mists. The main inconvenience of this structure, is the utilization of serpents encryption

Santosh et al. (2015) proposed effective Figuring with Secure Information Stockpiling utilizing AES. They noticed that a significant number of the security plots in cloud condition had not tended to the protection saving among outsider inspector and information in cloud. They proposed utilizing AES encryption calculation that no practicable assault against AES exists. The disadvantage is that AES encoded back rub can be broken with time.

Awadh and Hashim (2017) developed an Improving Information Stockpiling Security in registering in cloud through Steganography. They proposed the utilization of picture steganography in improving honesty of information in cloud. They gave a practical strategy to keep up information respectability. Pictures are utilized to secure information sent to server in this structure. Consequently, unapproved use would never

see concealed information in steganographic record. The composed model utilize pictures steganography for securing information uprightness. Be that as it may, the security of information amid transmission isn't dealt with in their work

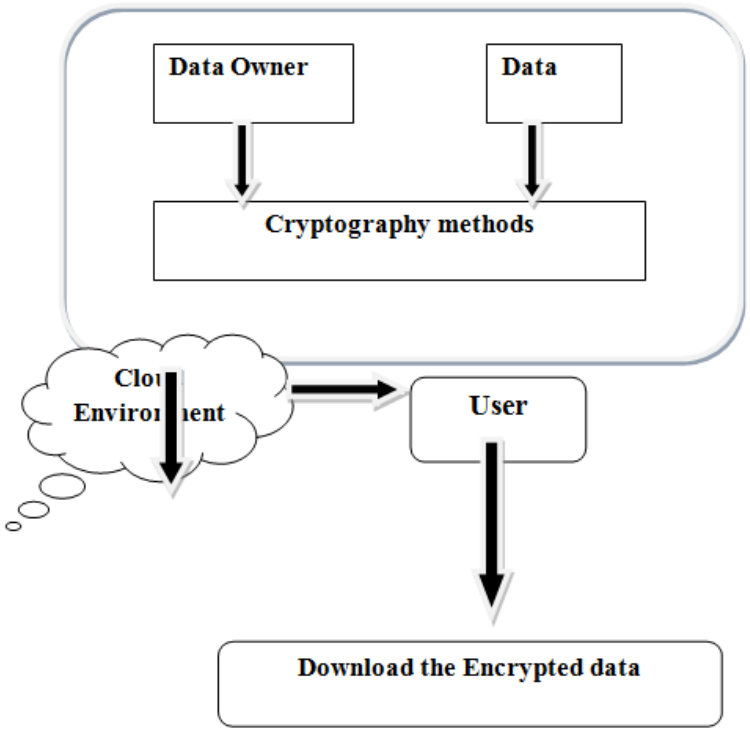
Prasanth and Gowtham (2014) developed the AES and DES utilizing a Protected and Dynamic Information Storage in Cloud. They suggested that information in cloud are liable to security assaults in this way, to secure information in cloud, Computerized Mark Calculation (DSA) was applied to keep up uprightness of documents, while Advanced Encryptions Standard (AES) calculation encodes and decodes records in cloud. Actualizing open review by open key made amid record creation or procedure of altering.

(Deepanchakaravarthi and Sunitha (2012) emphasised the strategy of securing information in cloud. Their plan utilize conveyed security of information in cloud. Their work was accomplished with token homomorphism and conveying check of information diddled. Their plan could permit stockpiling of information and recognize any altering. Their work claimeda system that justified arrangement assaults of server alteration by malevolent clients evasion.

The Existing System Architecture:

The current design of Kirubakaramoorthi; Arivazhagan and Helen (2015) is made out of two modules, i.e. the customer module and the server module. The whole world concern has been aroused due to the emergence of computing in cloud, an information technology with rapid development. Companies rising demand from IT firms for large data storage and processing is further making computing in cloud more promising especially in usage IT infrastructure renting usually shortly. This rapidly developing IT technology has given recognition to computing in cloud model, which provides users resources online of general utilities. The model is given in Figure 3.1.

Data owners uses element that approves or denies access to information and in charge of precision, respectability, and convenience. Fundamental of information administration is that undertaking information doesnt "have a place" to people. It is a benefit that has a place with the undertaking. All things considered, it should be overseen. A few associations dole out "proprietors" to information, by the idea of information possession. The data are impounded using cryptographic methods (Cryptography is fundamental innovations utilized as a part of building a safe cloud information stockpiling Distinctive uses of a similar essential calculations can give both encryption that keeps information mystery and validation that guarantees that information is protected from meddling clients) to launch into the cloud for proper storage.Despite the cryptographic method used, it still has major drawbacks which are listed as follows:



Drawback of Existing Framework:

a) Unathourized clients assault through hacking the IP deliver of servers to gain admittance to information.
b) Users can download, adjust and see records without appropriate validation system
c) Congestion in System: An excessive number of solicitations from the customers cause clog or workload. Over-burden causes servers separate.
d) No control over proprietors information because of not knowing the area and security system of the capacity suppliers.
e) Data respectability check and untrustworthiness from the customer (information privacy).
f) Users pantomime with private keys.

The proposed system:

The proposed framework will utilize steganography and Advanced Encryption Plan (AES) calculation to include an extra layer of security of information on cloud server. Steganography is concerned concealing messages: writings, sound, or pictures in document. The commonest technique is minimum noteworthy bits for putting away information. For instance, in high resolution graphics record, each pixels are spoke to by 24 bits.

Utilizing slightest huge (i.e. last 1 or 2 bits) to store other information, the picture isn't traded off and

information covered up in picture. It is worried about fracture of message to conceal it in cover-files to make message greatly hard to identify. The message is dispersed over various carrier signals/sources to conceal the message further. For instance, a solitary instant message would deteriorate into obstructs, each piece covered up in various picture. Another part of this procedure is that the piece size can differ and the squares are not really put away. This is an ordinary system in cryptographic calculations whereby changes and substitution are joined to scramble information. The strategy utilized as a part of this proposed framework is plot as takes after:

i. The customer chooses an information for transfer and the transferred information is scrambled with AES calculation.
ii. The scrambled information is hidden with LSB of sound file where information is to be put away. The bit position in 0th, first or second position.
iii. The strategy for concealing the information is sound steganography.

The shrouded information goes through server utilizing the split calculation where the information will be part first utilizing the split calculation. The information is gotten in plaintext organize. The split calculation separate the information into "even" and "odd" bits of data and afterward the consolidation calculation turn around the procedure. From here, alternate modules clarified in the current framework follows through to its logical end.

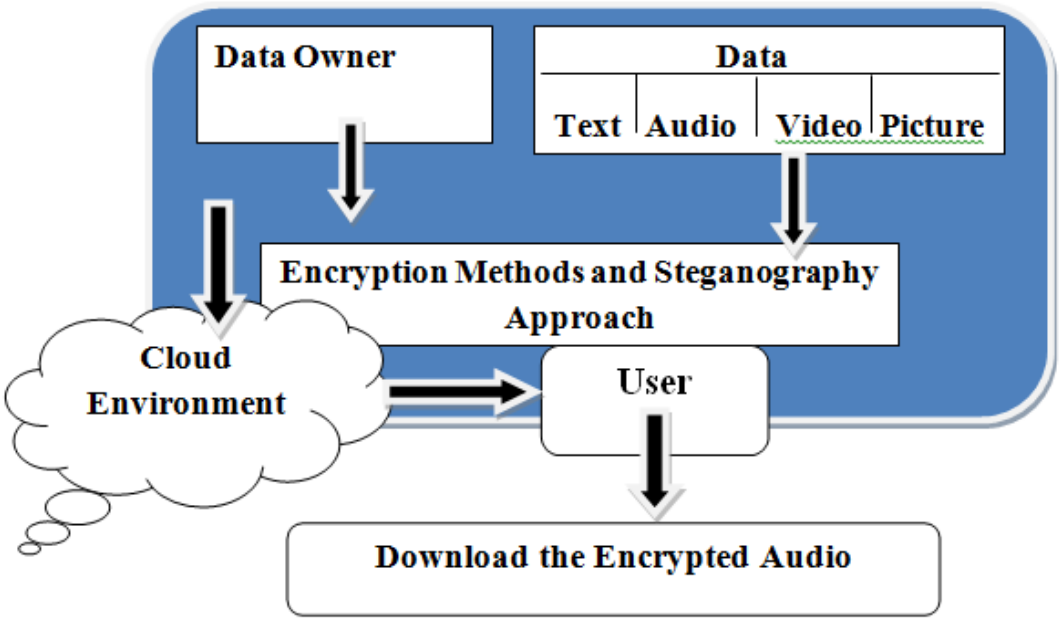


Figure 3.2: Proposed security system architecture

The proposed security framework utilizes Advanced Encryption Standard (AES) calculations and sound Steganography for security to data in cloud servers in existing engineering. We likewise include a layer of cryptosystem calculation that compliments the security endeavors of DH and RSA. This guarantees clients data are legitimately checked and enabled access to any information or data put away in the cloud.

At last, steganography layer is added to additionally secure information. Along these lines the framework utilizes a three layers security design like 3DES. Altogether, we utilized the encryption systems: mystery key cryptography plan and steganography plans. We consolidated these plans for an assailant to think that its ungainly to get to unapproved information and data from the cloud. The key cryptography utilized is the AES. Besides, the steganography was utilized to additionally sustain our method.

Advanced Encryption Measures (AES) Algorithm:

The advanced encryption standard (AES) calculation likewise called Rijndaels calculation was proposed-by Rijman and Daeman in 1978. It utilizes substitution, transportation, and the move, selective OR, and expansion activities to give abnormal state security for information. AES is unpredictable speculation of the exemplary substitution and transport Figures and can perform sensible and expansion tasks on information with the end goal that the information encoded under this plan are secure.

The AESs calculation utilizes a move rehash cycle. It performs 9, 11, or 16 cycles for keys of 128, 192, and 256-bits, separately. Each cycle has four stages:

i. Byte substitution,
ii. ii) Move push
iii. iii) Blend segment
iv. iv)Add subkey

Along these lines, the AES utilizes a decoding key to register from the encryption key. Along these lines this calculation is the symmetric key cryptography. The suggestion is that auser can without much of a stretch the unscrambling key once he knows the encryption key or access to the encryption calculation. This is the reason we utilize different calculations to frame a multilayer security that aggressors can't sidestep these security levels effortlessly.

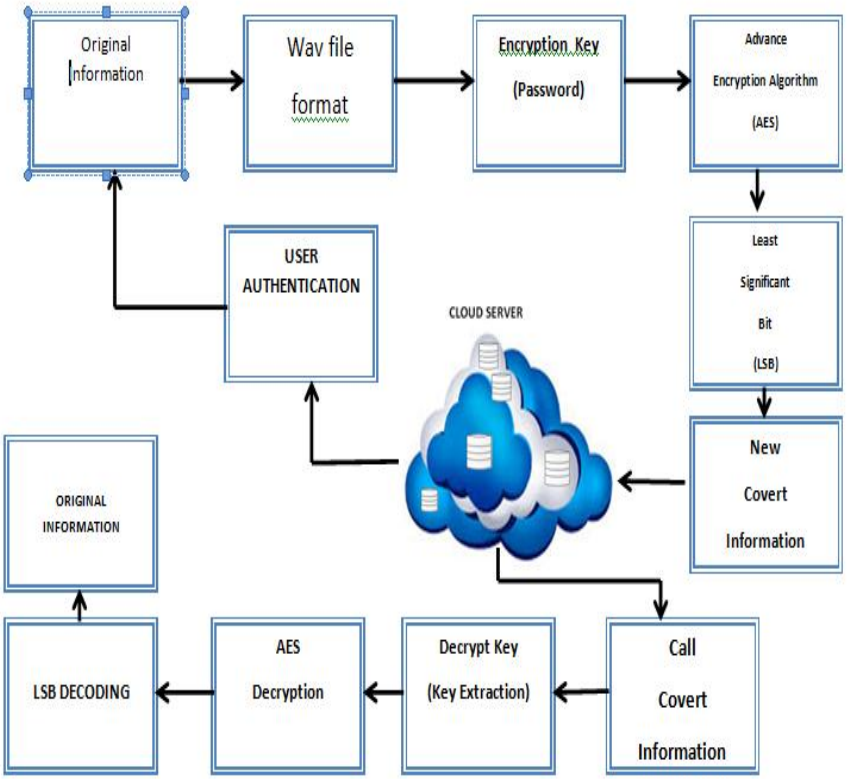
Wave File:

Waveform Sound Document Configuration (WAVE) is applicationof Asset Exchange Record Arrangement (RIFF), which stores sound piece streams" (Rahul, 2013) in lumps. WAVE codes sound in LPCM designs i.e. Straight Heartbeat Code Balance. Sound is wave of weight or mechanical vitality with weight change in flexible medium. The change engendered s packed and rare facted, yet when weight is higher than

including weight, pressure happens" (Rahul, 2013)and rarefaction occurs when the weight of proliferated wave is lesser than surrounding weight. A Wave document is sound record design, made by Microsoft, now standard PC sound document organize for framework amusements, sounds, and Disc quality sound. Wave record is distinguished by document expansion of (.wav). Utilized as a part of PCs, Wave record arrange is acknowledged as suitable trade medium for PC platforms like Mac.

This allows developers to move sound records unreservedly on stages for processing."In expansion to uncompressed crude sound information, the Wave document arrange stores data about tracks (mono or stereo), example rate, and bit profundity" (http://whatis.techtarget.com/definition/Wave-record). Documents with WAV or .WAVE record expansion is a Waveform Sound record. This is standard soundconfiguration seen essentially on Windows PCs. WAV records are generally uncompressed however pressure is upheld (http://resorterogon.weebly.com/ home/ files/05-2017/2. Uncompressed WAV documents are bigger contrasted with other sound arrangements, as MP3, so they are not utilized as favored soundconfiguration when sharing on the web, rather sound altering virtual products, working framework capacities, and video gamesare executed. WAV; an augmentation on bit stream design Asset Trade Documentconfiguration (RIFF). WAV is like AIFF and 8SVX organization documents.

RESULTS



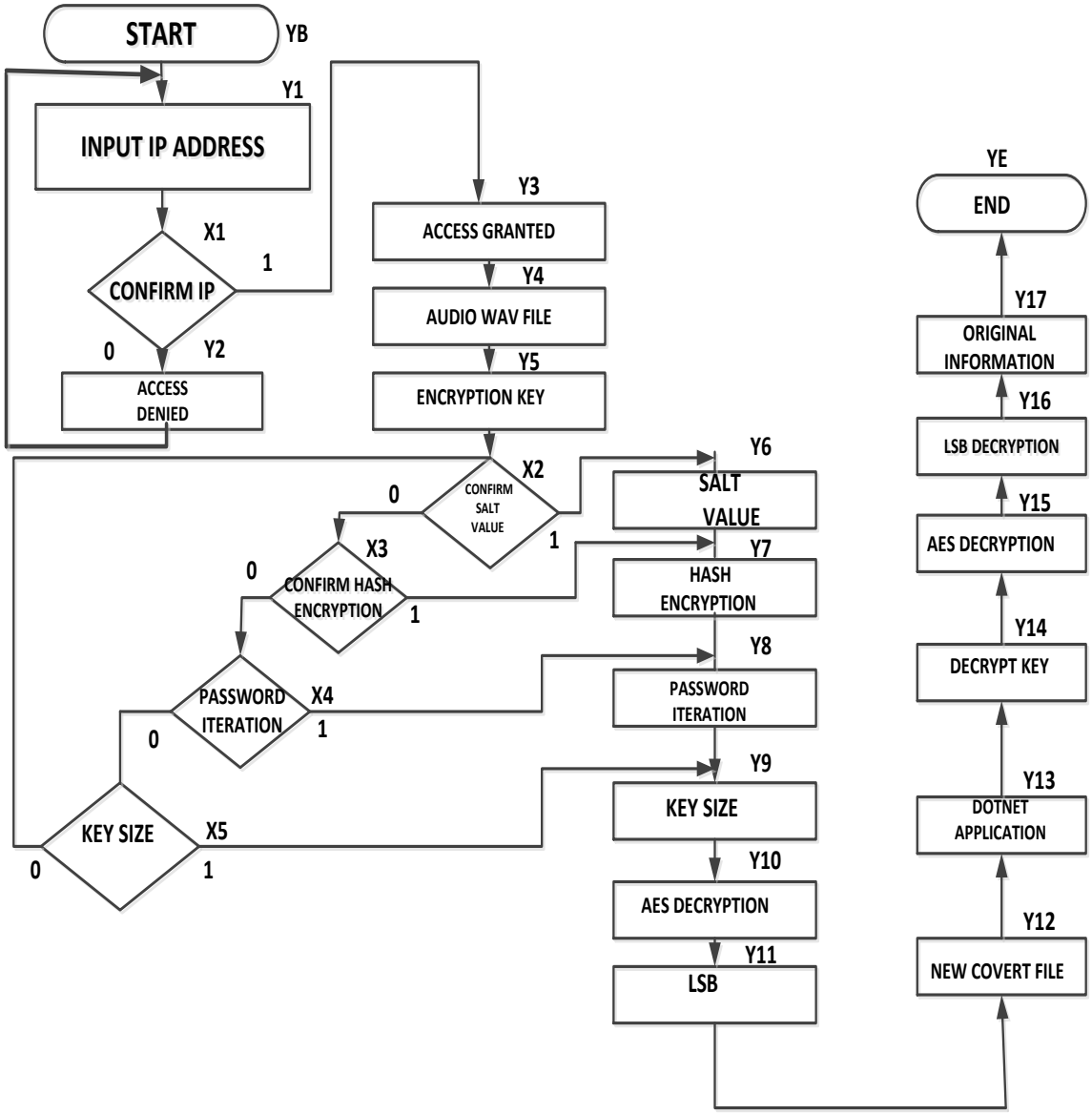
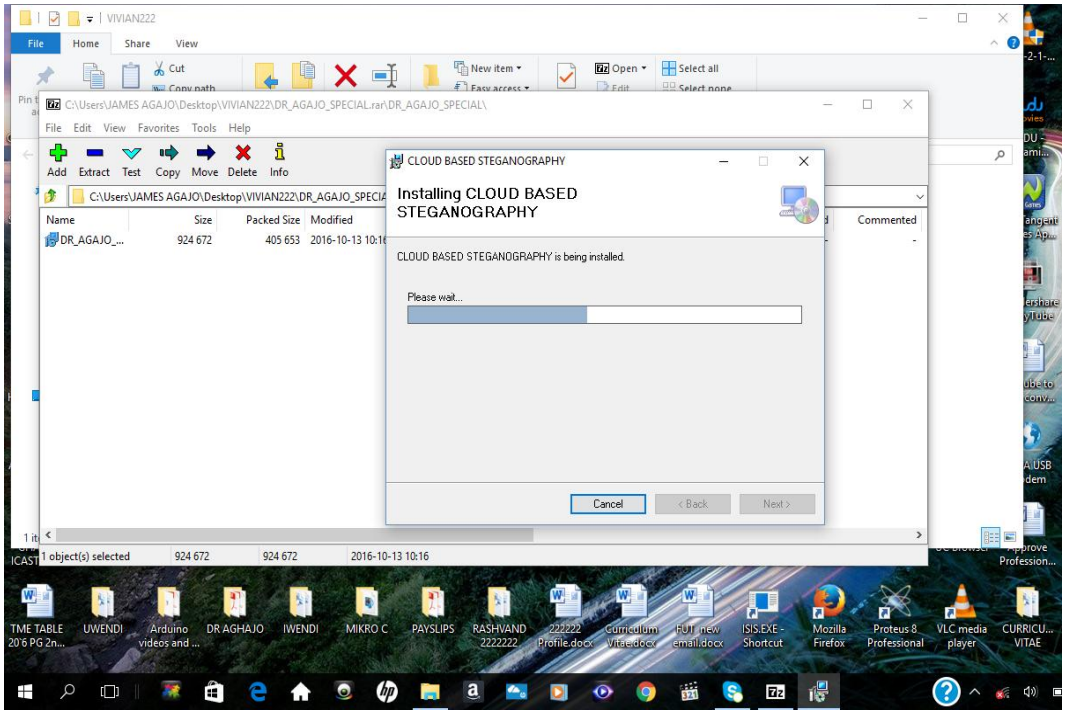
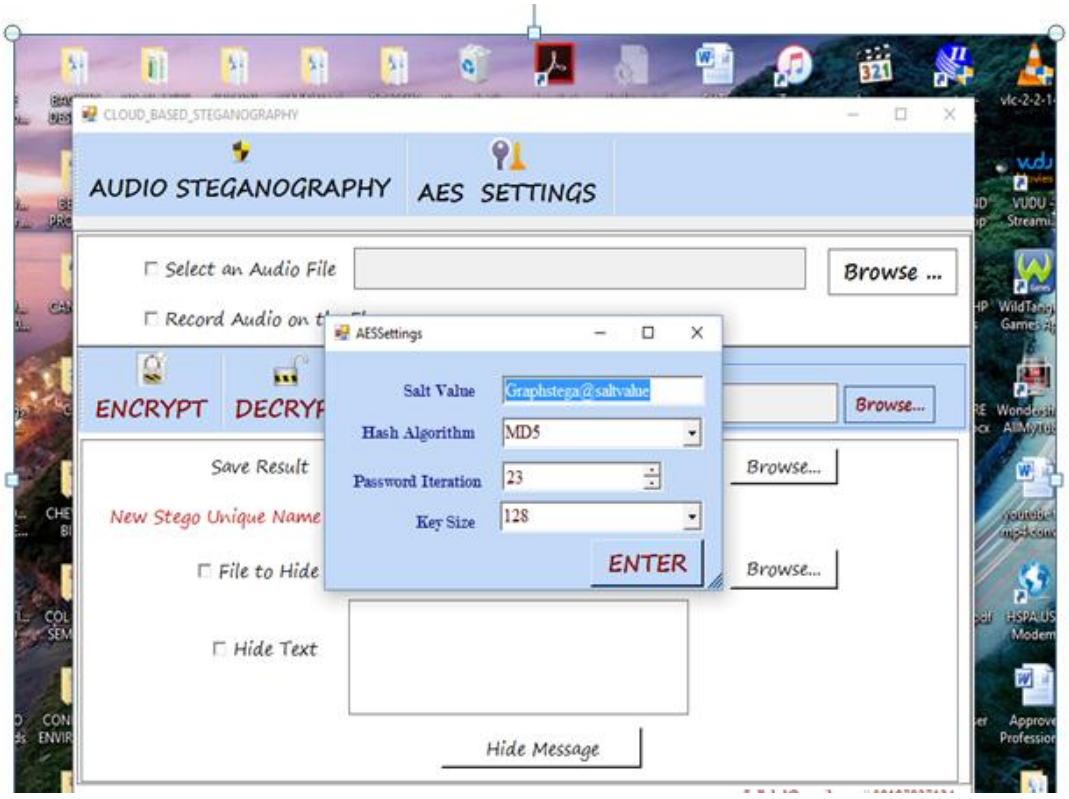


Figure 3.13: Flow diagram for the entire process


CLOUD BASED STEGANOGRAPHY
Installing CLOUD BASED STEGANOGRAPHY
CLOUD BASED STEGANOGRAPHY is being installed.
Please wait...
Cancel
< Back
Next >


CLOUD_BASED_STEGANOGRAPHY
AUDIO STEGANOGRAPHY
AES SETTINGS
Select an Audio File
Browse ...
Record Audio on
ENCRYPT
DECRYP
AESSettings
Salt Value
Graphstega@saltvalue
Hash Algorithm
MD5
Password Iteration
23
Key Size
128
ENTER
Browse...
Save Result
New Stego Unique Name
File to Hide
Hide Text
Hide Message

Discourse of Results:

The product created from our proposed display is appeared in Figure 4.1. Through experimentation with input information, yields were produced on program running. From the exploratory setup of the program interface, we introduce the cloud based AES and steganography to ensure information in cloud. This procedure is to guarantee that if aggressor can hack scrambled apparatus, for instance, the AES calculation key, which is the most effortless an assailant Figure, it is hard to Figure the safe layer of steganography that further ensure information in the cloud with the goal that any aggressor as yet endeavoring to hack the information in the cloud will think that its significantly harder.

Figure 4.2 shows yield of the encoded records in the product. The records are particularly scrambled utilizing the AES and Steganography with both sound message so aggressors when recognized are uncovered. Figure 4.3 demonstrates the recreation consequence of the scrambled wave record flag taking a scope of value sin x ordinate from 0 to 10 and 0 to 8 on the y ordinate. The subsequent reenactment diagram framed demonstrates that the document is defenceless against assault if no safety effort is set up to shield in from interlopers and programmers.

Figure 4.4, demonstrates the reproduction after effect of the scrambled sound wave flag when an assailant is endeavoring to hack the information from the cloud amid download a clueless approved clients. The reenactment result was tried with values. For instance, in the y facilitate, the scope of qualities is from 0 to 8 while in the x arrange, the qualities are from 0 to 10. The recreation after effect of the scrambled wave document flag demonstrates that the wave impact is relatively consistent regardless of clients or aggressors.

Figure 4.5 demonstrates the recreation result when the encryption calculation, Advanced encryption standard (AES) encoded wave flag. The recreation comes about, have same range for x and y coordinates depicted in Figure 4.4. In any case, the distinction is in the wave coming about because of the two reproductions. The wave shaped from the outcome in Figure 4.5 is considerably nearer than that framed from result in Figure 4.4 despite the fact that both have a similar scope of qualities. This demonstrates with the Advanced encryption standard (AES) calculation made information complex for aggressors to enter.

Figure 4.6, demonstrates the reenactment result drums wav wave record in its whole examining range. The after effect of the chart demonstrates that given a more extensive scope of qualities, the likelihood that aggressors will anticipate and Figure the secret key of the unscrambling key turns out to be much littler. Figure 4.7 demonstrates the reproduction result for variable D which id the variable that holds initial 2000000 position tests which ranges from 0 to +1. The chart demonstrates that the higher the scope of qualities chose and utilized, the more extreme it progresses toward becoming for the outcome and the suggestion is that the more troublesome it moves toward becoming for aggressor to Figure the correct key

utilized for decoding a scrambled information.

Figure 4.10 demonstrates the throughput for transfer. X pivot speaks to the throughput, Y hub speaks to document measure. Throughput is how much megabyte is computed in one moment. Information of existing framework, demonstrates that 16mb was transferred in 50s, and in proposed framework, it takes 25s to transfer a 16mb document. In Contrast with existing framework, execution of proposed framework is higher. This diagram plainly demonstrates the proposed framework lessens the throughput over the current framework by a normal of 15.5% and up to 55% for the transferring.

In Result, Figure.4.11 demonstrates the throughput for download. X hub speaks to the throughput, Y hub speaks to the document measure. In existing framework, 16mb was downloaded in 50s, while in proposed framework it takes 18s to download] a 16mb record. Contrast with the current framework the execution of proposed framework is higher. It demonstrates that proposed framework decreases the throughput over existing framework by a normal of 18% for transferring and 50.75% for downloading. The Figures demonstrate the throughput comes about for the diverse plans. The throughput diminishes in light of the fact that transfer and download forms require considerably more CPU calculation and completing encryption and decoding forms in the proposed framework, contrasted and the current framework. Table2 demonstrates the execution assessment for transferring. In existing framework, 16mb was transferred in 50s, where as in proposed system it takes 20s to transfer a 16mb record. Contrast with the current frameworks the execution of proposed framework is higher.

FILE SIZE	EXISTING	PROPOSED
16MB	40s	20s
64MB	60s	30s
124MB	70s	40s
500MB	80s	50s
1GIG	90s	55s

Table 4.1: Performance Evaluation for Uploading of Existing and Proposed System

Execution Assessment:

The execution assessment of programming is estimated with the frameworks utilized. A few grids utilized as a part of assessment of programming going from speed, time, proficiency et cetera. In our proposed information security framework, the lattices utilized as a part of the assessment testing are the document measure, the ideal opportunity for transfer and download, we considered the latest Strategy like Information Encryption Standard (DES) calculation looked at to Advance Encryption Calculation (AES) and the throughput. This segment clarified in points of interest how the execution for the transfer time and download time for proposed framework is lesser than the current framework. Right off the bat the information which is to be transmitted from sender to collector in the system must be scrambled utilizing the encryption calculation in cryptography. The tables 4.1 and4.2 record the execution of existing and proposed framework as far as document measure (in MegaByte) and time (in seconds) for transferring file to cloud and downloading files from cloud, and are spoken to in the histograms in Figures 4.14 and 4.16 and line charts in Figures 4.15and 4.17 It can watched that our proposed framework execution as far as time spent for record emptying and downloading is lesser than that of the current framework.

FILE SIZE	EXISTING	PROPOSED
16MB	47s	25s
64MB	59s	35s
164MB	73s	45s
500MB	86s	55s
1GIG	96s	65s

Result Table 4.2: Performance evaluation for downloading

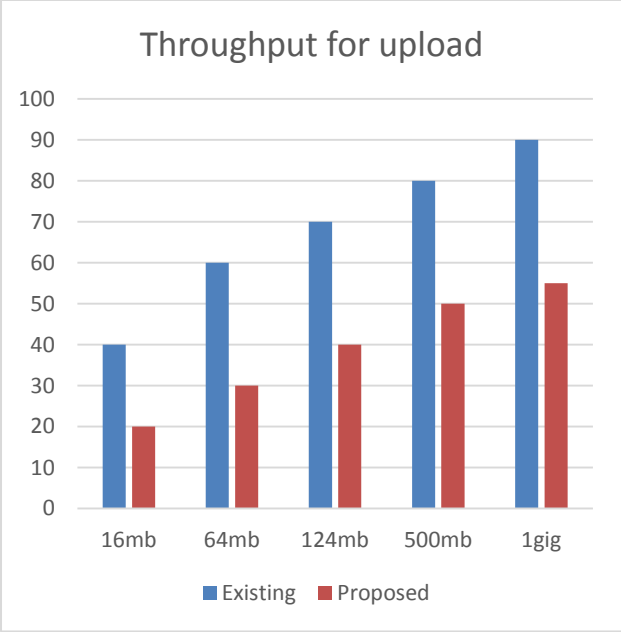


Figure 4.14: A Histogram of throughput for upload

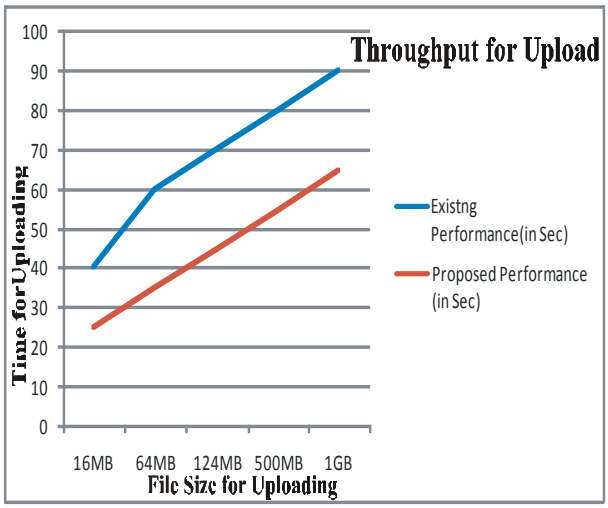


Figure 4.15: A graph of throughput for upload

Figure 4.10 shows throughput for upload. X axis represents the throughput, Y axis represents the file size. Throughput is how much megabyte is calculated in one second.

In existing system, 16mb was uploaded in 50s, where as in proposed system it takes 10s to upload a 16mb file. Compare to the existing system the performance of proposed system is higher. This graph clearly shows the proposed system reduces the throughput over the existing system by an average of 15.5% and up to 55% for the uploading.

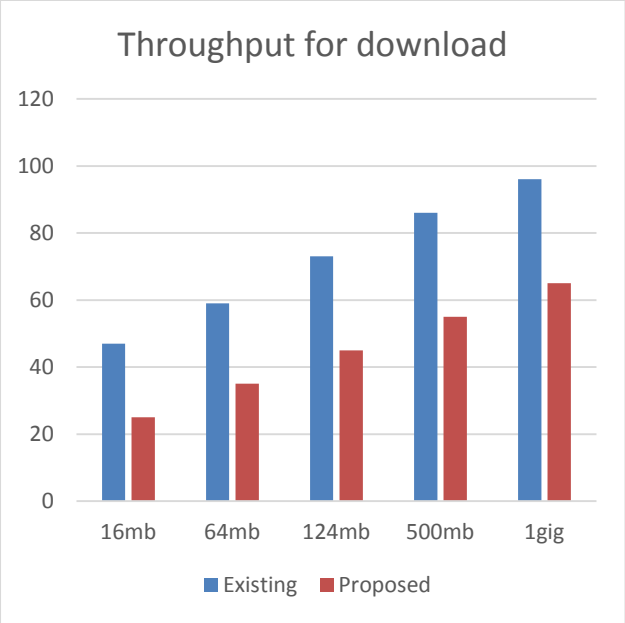


Figure 4.16: A Histogram of throughput for download

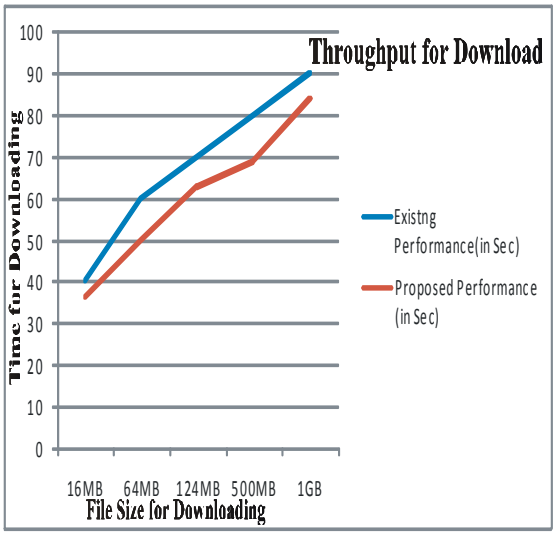


Figure 4.17: A graph of throughput for download

Figure 4.11, demonstrates the throughput for download. X-pivot stand for throughput, Y-hub remains for document estimate. 16mb was downloaded in 50s for existing framework, while in proposed framework it takes 18s to download a 16mb record. Contrast with the current framework there higher execution in proposed framework. It demonstrates that proposed framework lessens the throughput over existing framework by normal of 18% and 50.75% for the downloading. The Figures indicate throughput comes about for the two plans. There is diminish in throughput, in light of the fact that transfer and download forms

require more CPU calculation and completing encryption and unscrambling forms in the proposed framework, in examination with existing framework. Table2 demonstrates the execution assessment for transferring. 16mb was transferred in 50s for existing framework, while in proposed framework it takes 20s to transfer a 16mb document. Contrasting existing framework with proposed framework, execution of proposed framework is higher. Table 2 demonstrates the execution assessment for downloading. In existing framework, 16mb was transferred in 47s, where as in proposed framework it takes 25s to download a 16mb record. Contrast with the current framework the execution of proposed framework is higher.

Table2 demonstrates that the execution assessment for transferring. In existing framework, 16mb was transferred in 40s, while proposed framework takes 20s to upload16mb document. Contrast with the current framework, the execution of proposed framework is higher. Table 2 demonstrates the execution assessment for downloading. In existing framework, 16mb was transferred in 47s, where as in proposed framework it takes 25s to download a 16mb document. Contrast with the current framework the execution of proposed framework is higher.

REFERENCES

1. Abhinay B.A., Akshata B.A., and Karuna C.G. (2013). Security Issues with Possible Solutions in Clouds Computings-A Survey. International Journals of Advanced Research in Computer Engineering & Technology, 2(2), 652-661.
2. Awadh A. & Hashim A. (2017). Using Steganography for Secure Data Storage in Cloud Computing. International Research Journal of Engineering and Technology, 4(4),3668-3672.
3. Boroujerdi M. and Nazem S (2009) Cloud Computing: Changing Cogitation about Computing. World Academy of Science, Engineering and Technology. IJCSI International Journal of Computer Science Issues, 9(4), 177-182
4. Deepanchakaravarthi P. & Sunitha A (2012). An Approach for Data Storage Security in Cloud Computing. IJCSI International Journal of Computer Science Issues, 9(2), 100-105.
5. Harjit S. L.and Gurdev S. (2011). Cloud Computing-Future Framework for e-management of NGOs. International Journal of Advancements in Technology, 2(3), 400-407.
6. Izevbizua P. O (2015). Data security in the cloud using serpent encryption and distributed steganography. European Scientific Journal, 11(18), 347-359.
7. Kirubakaramoorthi,R.; Arivazhagan, D.; and Helen, D. (2015):Survey on Encryptions Techniques used to Secure Cloud Storage System. Indian Journal of Science and Technology, Vol 8(36) 3451-3557
8. Jasleen K. and Sushil G., (2016). Security in Cloud Computing Using Hybrid of Algorithms. International Journal of Engineering Research and General Science 4 (2), 465-472.
9. Nikita G. and Toshi S. (2014). Cloud computing – SPI Framework, Deployment Models, Challenges. Inetrnational Journal of Emerging Technology and Advanced Engineering, 4(1), 19-25.
10. Prasanth SP and Gowtham B (2014): AES and DES Using Secure and Dynamic Data Storage in Cloud, International Journal of Computer Science and Mobile Computing, 3(1), 401-407

11. Ramaporkalai, T.(2017): Security Algorithms in Cloud Computing:International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2. ISSN: 2347-8578 www.ijcstjournal.org Page 500
12. Rashmi S. G and Deepali M. K. (2015). Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm. International Journal on Recent and Innovation Trends in Computing and Communication, 3(5), 157-161.