CLOUD-BASED MULTIMEDIA PROTECTION SYSTEM

Ms.Vidhya.A[1] , Sai Manish.K[2],Sanjay.J,Tharun.V[3]

[1]Assistant professor,Department of computer science and engineering , Jeppiaar engineering college,ch-119

[2]UG students, Department of computer science and engineering , Jeppiaar engineering college,ch-119

ABSTRACT - As the year passes by the personal data privacy of an individual user is getting less and less, more companies selling their user's data for giving them personalized advertisements. The paper proposes another outline for interactive media assurance frameworks. System can be used to protect various multimedia contents like videos, images, music or any large text files. The system can run on public or private cloud or any combination of public private clouds. By using encryption and decryption is the process of converting plaintext back to ciphertext vice versa. The encrypted files will be saved on our cloud database, which can be accessed anytime and anywhere.

Keywords: Multimedia, Encryption, Decryption, Hash Algorithm, Cloud Application

I. INTRODUCTION

We present a novel system for multimedia content protection on cloud infrastructures. The system can be used to protect various multimedia content types, including regular videos, images, songs, and music clips. The system can run on private clouds, public clouds, or any combination of public-private clouds. The design is cost effective because it uses the computing resources on demand. The design can be scaled up and down to support varying amounts of multimedia content being protected. . User can also download the encrypted file if the wants to decrypt the encrypted file user can use the decrypt option and upload the encrypted file to be decrypted. We have developed a complete running system of all components and tested it with more than 11,000 3D videos and 1 million images.

II. CLOUD COMPUTING

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based_storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing is the delivery of different services through the Internet, including data storage, servers, databases, networking, and software. Cloud-based storage makes it possible to save files to a remote database and retrieve them on demand. Services can be both public and private—public services are provided online for a fee while private services are hosted on a network to specific clients. Cloud computing can be both public and private. Public cloud services provide their services over the Internet for a fee. Private cloud services, on the other hand, only provide services to a certain number of people. These services are a system of networks that supply hosted services. There is also a hybrid option, which combines elements of both the public and private services. Cloud computing takes all the heavy lifting involved in crunching and processing data away from the device you carry around or sit and work at. It also moves all of that work to huge computer clusters far away in cyberspace. The Internet becomes the cloud, and voilà—your data, work, and applications are available from any device with which you can connect to the Internet, anywhere in the world.

Cloud computing is not a single piece of technology like a microchip or a cell phone. Rather, it's a system primarily comprised of three services: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

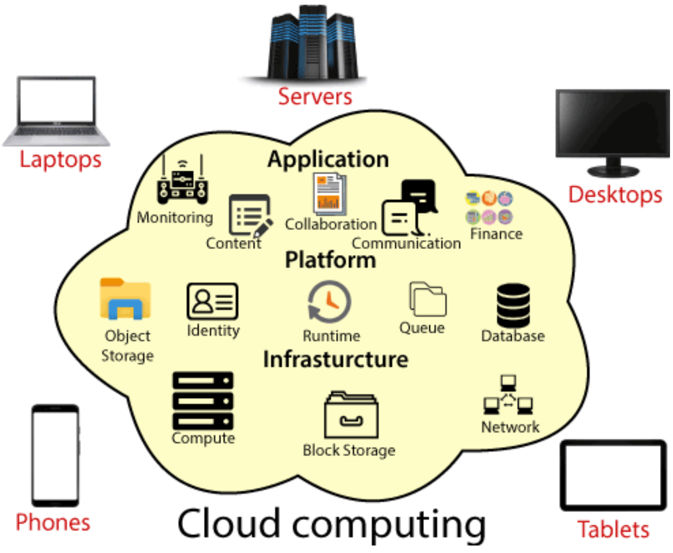


Figure1: Cloud computing

III. ENCRYPTION AND DECRYPTION

Encryption is the method by which information is converted into secret code that hides the information true meaning. The science of encrypting and decrypting information is called cryptography. In computing, unencrypted data is also known as plain text and encrypt data is called cipher text. The formulas used to encode and decode message are called encryption. To be effective, a cipher includes a variable as a part of the algorithm. The variable, which is called a key, is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt message as well as what key were used as variables

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption It decodes the encrypted file so that an authorized user can only decrypt the data because decryption requires a secret key or password. There are many methods of conventional cryptography, one of the most important and popular method is Hill cipher Encryption and Decryption, which generates the random Matrix and is essentially the power of security. Decryption requires inverse of the matrix in Hill cipher. Hence while decryption one problem arises that the Inverse of the matrix does not always exist. If the matrix is not invertible then the encrypted content cannot be decrypted. This drawback is completely eliminated in the modified Hill cipher algorithm. Also this method requires the cracker to find the inverse of many square matrices which is not computationally easy. So the modified Hill-Cipher method is both easy to implement and difficult to crack.

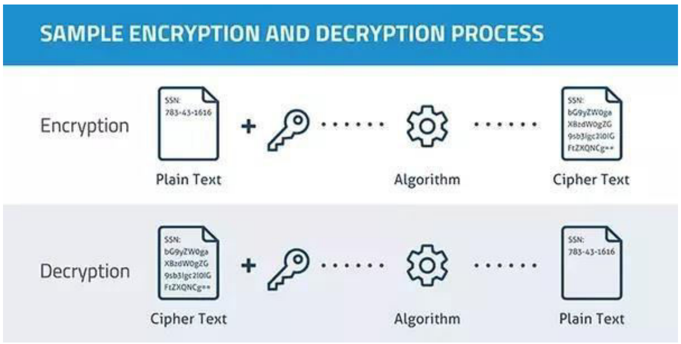


Figure2: Encryption and Decryption

IV. HASH FUNCTION

Hashing is the transformation of a string of characters into a usually fixed length value or key represents. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length. Values returned by a hash function are called message digest or simply hash values. The following picture illustrated hash function. Hash functions are extremely useful and appear in almost all information security applications. Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data. In general, the hash is much smaller than the input data; hence hash functions are sometimes called compression functions. Since a hash is a smaller representation of a larger data, it is also referred to as a digest. Hash function with n bit output is referred to as an n-bit hash function. Popular hash functions generate values between 160 and 512 bits. Since, the hash value of first message block becomes an input to the second hash operation, output of which alters the result of the third operation, and so on. This effect, known as an avalanche effect of hashing. Avalanche effect results in substantially different hash values for two messages that differ by even a single bit of data. Understand the difference between hash function and algorithm correctly. The hash function generates a hash code by operating on two blocks of fixed-length binary data.

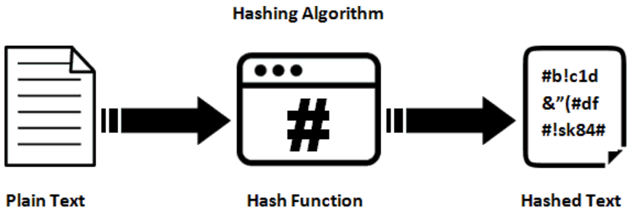


Figure3: Hash Function

V. LITERATURE SURVEY

This chapter deals with the survey done prior to the design and development of the system. The survey includes study of various technologies used to create this application as a whole. The multimedia content protection system can be used to protect different multimedia contents types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips. This system can be deployed on private or public cloud. We provide a holistic survey of multimedia content protection applications in which block chain technology is being used. The study of the literature reveals that there is currently no complete and systematic taxonomy dedicated to block chain-based copyright protection applications. The number of successfully developed block chain-based content protection systems is very low. Protection of the system is made using the simple concept. Without any calls it forms an interconnection with the database. One time password is used in the system which makes it simple. Without any of the system architecture it gives a algorithm with development. Legal distribution of multimedia contents is a recurrent topic of research. Broadband home Internet access has enabled the sustained growth of e-commerce, including direct downloads of multimedia contents. Fingerprinting emerged as a technological solution to avoid illegal content re-distribution. The copyright protection and information integrity assurance have gradually become an urgent issue that needs to be resolved. It is more convenient and effective in practical applications. The configuration use cloud frameworks to give cost effectiveness, fast sending, versatility, and flexibility to suit differing workloads

VI. EXISTING SYSTEM

There are many innovations and technologies in the world with the same multimedia content protection system. The existing system can save clients data on to the cloud, which makes it can be accessed anywhere anytime.

"Priyanka R", "Cloud Based Multimedia Protection System", NLPGPS - 2017 Conference, 2017. In this paper, they have gone through their system properties very well but the cost for the project is too high compared to the other papers we referred. Security is also less and it is too complex for the end user to execute.

PROPOSED SYSTEM

The client users are given provision to store their files in the cloud. We developed new system for multimedia content protection on cloud framework. The proposed framework can be utilized to encrypt media including 2-D recordings, 3-D recordings, pictures and music. The design is cost effective because it uses the computing resources on demand. The design can be scaled up and down to support varying amounts of multimedia content being protected. The proposed system is fairly complex with multiple components. The programming devices utilized as a part of this venture is Microsoft windows Virtual Studio and Google Firebase. The content of the multimedia can be uploaded and it will be encrypted and user can also assign a password for each and every file for second layer of protection. The file will be saved on to the cloud. User can also download the encrypted file if the wants to decrypt the encrypted file user can use the decrypt option and upload the encrypted file to be decrypted. We have developed a complete running system of all components and tested it with more than 11,000 3D videos and 1 million images. By minimizing the cost the system it will be more affordable for all the users

VII. ARCHITECTURE DIAGRAM

we have modules of 7 and the namely: Login user, Home page, Upload the file, Encryption, Decryption, Database storage, Logout or exit.

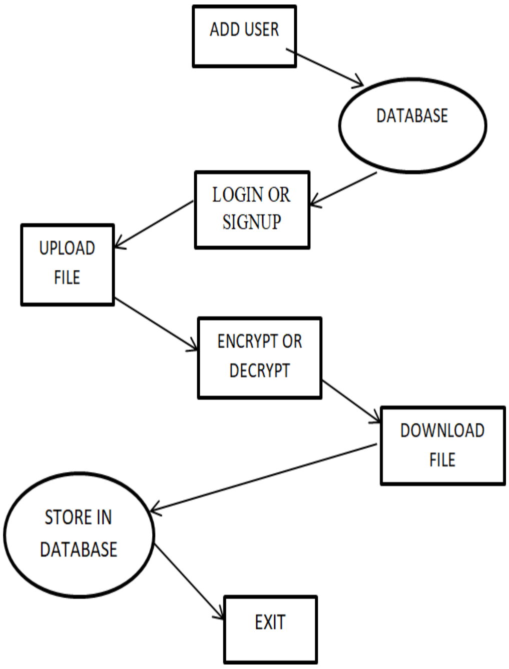


Figure4: Architecture of the multimedia protection system

A. *LOGIN USER*

User must login or can sign up using their email of Google email id to access the home for encrypt or to decrypt the files. When user logged in. it checks whether the user is in active or he/she is inactive so that it logout in a period of time. It checks in the database for the user details and presents it in the home page.

B. *HOME PAGE*

Home page is the page, where the user can access the system for encrypting or decrypting the file. Home page will be more attractive to user for accessing the items in the system. The home also contains database the user can see the files that the user uploaded. There is a bin feature; the deleted files will be automatically stored in the bin.

C. *UPLOAD FILE*

Uploading the file for encryption and for decryption adds a dynamic way of approach where uploaded file will be sent in the database and can be received wherever the use wants it is a get feature to access

D. *ENCRYPTION*

Encrypting the file applies a strong password for the file which makes it highly encrypted which cannot be accessed by anyone without the correct combination of passwords.

E. *DECRYPTION*

After the encryption the file must be decrypted to use and to access the file so the decryption section we decrypt the file by Appling the correct password for the file and receiving it from the database or from the system downloads. Every process is further encrypted and decrypted which cannot be accessed or use by any users from the system permission.

F. *DATABASE STORAGE*

The download file from the encryption and decryption process will be stored in the database so that it won't get lost or deleted. In firebase database it is stored in the system that gives a proper design to store the data and can be received by the easy accessible ways.

G. *LOGOUT OR EXIT*

User can logout the system whenever they want the files will be stored it the cloud which can be accessed with one or more number of ways where it will allow the user again to login at any time and at anywhere.

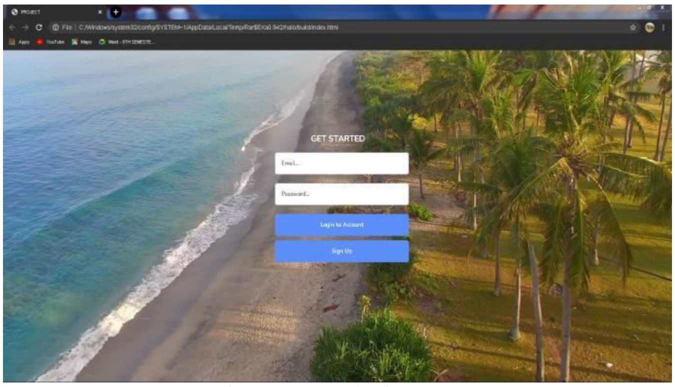


Figure5: User login screen

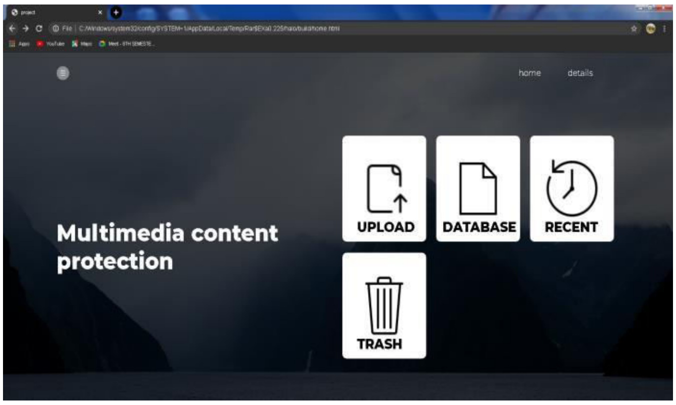


Figure6: Home page

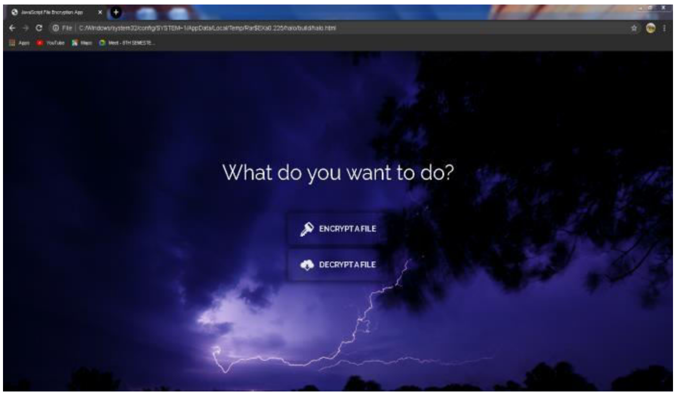


Figure7: Upload file screen

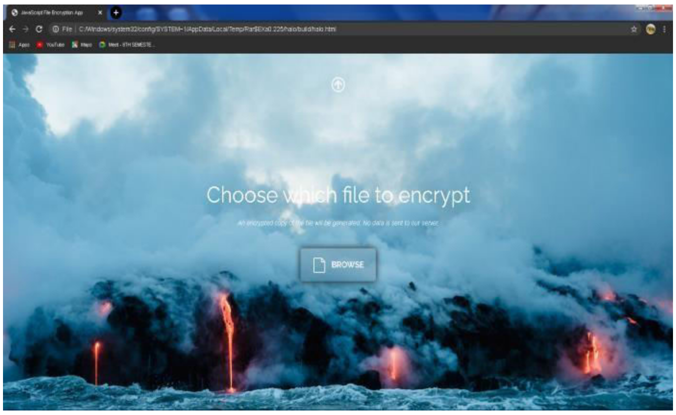


Figure8: Encryption screen

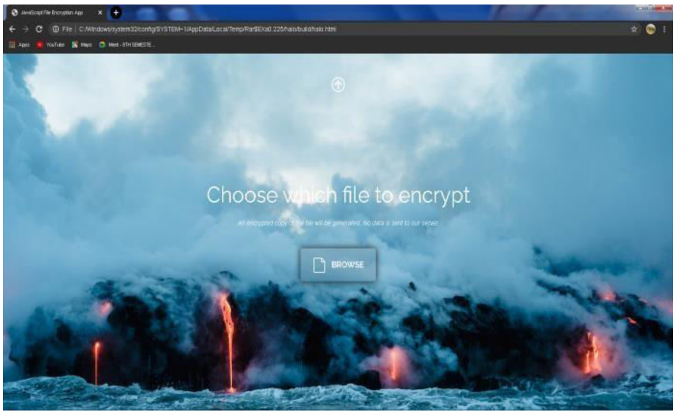
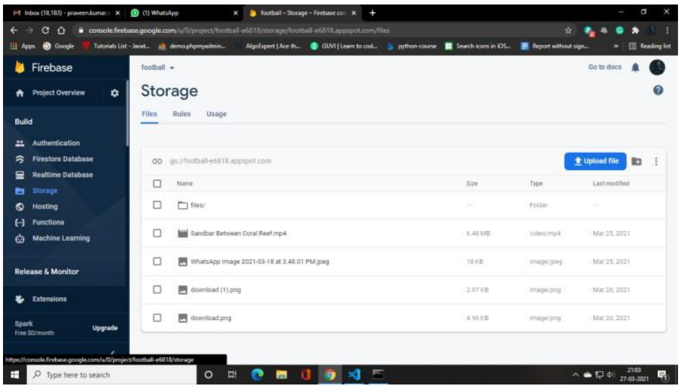


Figure9: Decryption screen



Name	Size	Type	Last modified
files/	—	Folder	—
Sandbar Between Coral Reef.mp4	6.48 MB	video/mp4	Mar 25, 2021
WhatsApp Image 2021-03-18 at 3.48.01 PM.jpeg	18 KB	image/jpeg	Mar 25, 2021
download (1).png	2.97 KB	image/png	Mar 26, 2021
download.png	4.96 KB	image/png	Mar 26, 2021

Figure10: Database Storage screen

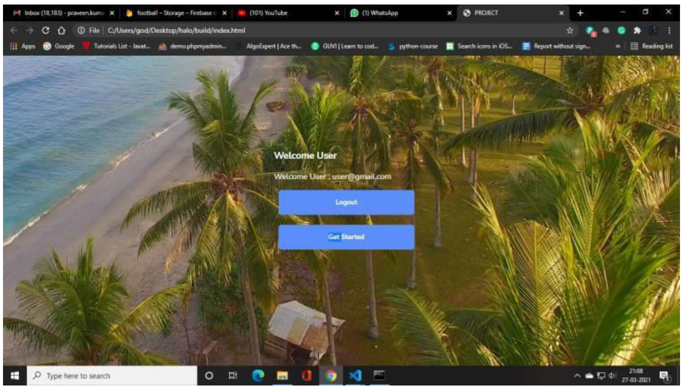


Figure10: Logout or Exit screen

VIII. CONCLUSION

Our project gives a detail progress of the user uploading a multimedia file online through our system. Our system encrypts the file and saves in our database. The main objectives of the project are to develop an algorithm that will be used to save the user information safely. To develop a database were all the related data will be stored and to develop a web interface. As it encrypts hash algorithm plays a keen role for the system. For future purpose the enhancements can be made to share the encrypted file in-between existing users through a safe and encrypted way in system. An Android/iOS can be developed in the future which will bring our existing system to hands of everyone. With this future implementation can be integrated with the help of firebase, Android Studio is a powerful platform for updating and recreating the web application in much easier way.

IX. REFERENCES

[1] Mohamed Hefeeda , Senior Member, IEEE, TarekElGamal , KianaCalagari, and Ahmed Abdelsadek ,"Cloud-Based Multimedia Content Protection System", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 17, NO. 3, MARCH 2015.

[2] Abdelsadek and M. Hefeeda. Dimo: Distributed index for matching multimedia objects using map reduce. In Proc. of ACM Multimedia Systems Conference (MMSys'14), pages 115–125, Singapore, March 2014.

[3]M. Aly, M. Munich, and P. Perona. Distributed Kd-Trees for Retrieval from Very Large Image Collections. In Proc. of British Machine Vision Conference (BMVC), Dundee, UK, August 2011.

[4] Khodabakhshi and M. Hefeeda. Spider: A system for finding 3d video copies. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 9(1):7:1–7:20, February 2013.

[5] H. Liao, J. Han, and J. Fang. Multi-dimensional index on hadoop distributed file system. In Proc. of IEEE Conference on Networking, Architecture and Storage (NAS'10), pages 240–249, Macau, China, July 2010.

[6] Z. Liu, T. Liu, D. Gibbon, and B. Shahraray. Effective and scalable video copy detection. In Proc. of ACM Conference on Multimedia Information Retrieval (MIR'10), pages 119–128, Philadelphia, PA, March 2010.

[7] P. Ram and A. Gray. Which space partitioning tree to use for search? In Proc. Of Advances in Neural Information Processing Systems (NIPS'13), pages 656–664, Lake Tahoe, NV, December 2013.

[8] Stupar, S. Michel, and R. Schenkel. Rankreduce - processing k-nearest neighbor queries on top of map reduce. In Proc. of Workshop on Large-Scale Distributed Systems for Information Retrieval (LSDS-IR'10), pages 13–18, Geneva, Switzerland, July 2010.

[9] M.Sudha, Dr.Bandaru Rama Krishna Rao, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment", International Journal of Computer Applications (0975 – 8887)
Volume 12– No.8, December 2012

[10] J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei, "Imagenet: A large-scale hierarchical image database," in Proc. IEEE Conf. Comput.Vis. Pattern Recog. (CVPR'09), Miami, FL, USA, Jun. 2009, pp. 248–255.

[11] Er. Mandeep Singh Sandhu and Er. Sunny Singla, An Approach to Enhanced Security of Multimedia Data Model Technology Based on Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013.

[12] Mani Malekesmaeili, MehrdadFatourechi, and Rabab K. Ward, Video Copy Detection Using Temporally Informative Representative Images, International Journal of Engineering Research and Applications 2014.

[13]R.Amirtharathna, Prevention Mechanism for Redistribution of Audio Contents in Cloud, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, and September 2015.

[14] Youjin Song, Yasheng Pang, An Approach of Risk Management for Multimedia Streaming Service in Cloud Computing, International Journal of Multimedia and Ubiquitous Engineering, Vol.9, No.4 , 2014.