International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 02, February 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Enhancing Visual Image Protection in Cloud Using Hashing Algorithm with QR Code Encryption

Hemalatha.R [1],Dr. Selvi.S [2], Gowthami.S [3],Panthalarajan.M.S[4]

[1] *Assistant Professor,Department of Computer Science,PSG College of Arts & Science*

[2] *Associate Professor,Department of Computer Science,PSG College of Arts & Science*

[3] *Student, Department of Computer Science,PSG College of Arts & Science*

[4] *Student, Department of Computer Science,PSG College of Arts & Science*

ABSTRACT

Images have become an inevitable part of knowledge within the modern-day society. As data is growing at a fast rate, prices concerned in storing and maintaining data are additionally raising rapidly. Security of information in the cloud may be a challenge and is important as several issues and faults are nevertheless to be categorized. As data is keep in the cloud, the user is unaware of wherever it's being stored and who are privileged to access the info. Eventually, the data owners are fazed regarding the confidentiality and integrity of the data. to confirm this, a security technique has to be provided to the info even before it's kept on the cloud. Such technique ought to be straightforward and easy and at a similar time should be less complex. In this paper to confirm confidentiality and integrity of the data, a security technique has to be provided to the data even before it is stored on the cloud using Visual Cryptography with QR code generation with a hash algorithm.

Keywords: *Hashing Algorithm, QR code, Secure Image, Visual Cryptography.*

I. INTRODUCTION

Cloud computing could be a reproduction that has immense computation ability and vast memory houses at a low price. It permits users to get prospect services regardless of time and placement on diagonally varied platforms and therefore brings nice ease to cloud users. In today's world important security and accuracy of image is a huge challenge. Totally different sensitive knowledge equivalent to medical pictures, biometric images, space and geographical images that are taken from the satellite and business important documents are transferred over the web and held in remote locations. The large development in internet technology is a real challenge for the sender to send non-public images from one system Associate in Nursing to a different system. there's no assurance between sender and receiver that there is nobody intercepting those private images. Cloud computing is a rising technology that provides facilities for storage, computations, and database-driven services for varied industrial, financial, healthcare, academic and governmental sectors. The common security issues are:

• Securing data each during transmission and through storage,

• Securing package interfaces,

• User access management and

• information separation

The info within the cloud computing is placed in the hands of third parties, making certain the info security each during storage and through transmission is of nice importance. As data is held within the cloud, the user is unaware of wherever it's being stored and who is privileged to access the data. To make sure confidentially, a security technique needs to be provided to the data even before it is stored on the cloud. Such techniques ought to be straightforward and easy and at a similar time should be less complex. encoding techniques are used on a bigger scale with success providing security to the data both during transmission and storage. Cryptography encodes an understandable text to a cipher text and decodes the cipher text back to the plain text. Visual cryptography (VC) could be an encoding technique on pictures during which a secret image is regenerate into 2 or additional meaningless, non-identical shares, while not using any encryption keys. The hidden secret is discovered only if the shares are stacked together. The magnificence of VC lies within the facts that the hidden secret will ne'er be recovered simply by possessing one among the shares, and additionally that the key can be revealed with none pc intervention. this permits VC to be used by anyone with none deep understanding of cryptography, and without any exhausting computations.

II. LITERATURE SURVEY

In this paper, B.Li and H.Li, B.wang, given by public auditing for shared image with economical user revocation within the cloud. Sharing services in the cloud and with image storage, users will merely modify. dissimilar blocks in shared image are usually signed by totally different users thanks to image modifications performed by different users. To create certain shared image consistency is verified publicly, users in the cluster got to figure signatures on all the blocks in the shared image. For security reasons, once a user is revoked from the group, the blocks that were before signed by this revoked user should be re-signed by associate degree gettable user[1].

In this paper Sahai and Waters, “Fuzzy Identity-Based Encryption” is given a replacement form of identity-based coding that is referred to as fuzzy IBE. In fuzzy IBE, it observes an identity as a set of descriptive attributes. This technique permits for a secret key for an identity, p, to rewrite a ciphertext encrypted with an identity, alphabetic character, if and providing the identities p and q are on the point of each other. Therefore, this theme allows a definite quantity of fault-tolerance within the identities. Fuzzy-IBE [4] produces 2 new applications. The first is the associate degree IBE system that uses biometric identities. that will show a user’s identity corresponding to iris scan, finger print[2].

In this paper J.Liu, S.tang, X.Huang, Y.xiang, K.Liang, L.Xu and J.zhou ,proposed by associate degree correct analysis on the shared image provides anarray of advantages to each the society and people and Image sharing has ne'er been easier with the advances of cloud computing,. Image sharing with an enormous range of participants take into consideration several issues, as well as effectiveness, image dependability and privacy of image owner[3].

In this paper M. Stojmenovic, S. Ruj and A. Nayak, projected the secure image storage in clouds for a fresh suburbanized access. The cloud verifies the validity of the run while not knowing the user’s identity within the proposed scheme. Our feature is that solely valid users will be able to rewrite the keep information. It prevents the replay attack [4].

In this paper L.Rodero-Merino,L.M Vaquero, J.Caceres and M.Linder introduced Cloud computing to urge a whole definition of what a Cloud is, victimising the most characteristics usually connected with this pattern in the literature. This paper pays a lot of attention to the Grid paradigm, because it is commonly confused with Cloud technologies. A varied definition has studied then only a few definitions containing the essential characteristics. We tend to additionally describe the associations and distinctions between the Grid and Cloud approaches[5].

In this paper M.Franklin and D.Boneh projected a totally purposeful identity-based coding theme (IBE). The scheme has explicit ciphertext security within the random oracle model assuming a distinction of the process Diffie dramatist problem. Our system relies on additive maps between groups. They proposed the correct definition for secure identitybased encryption schemes and provided totally different applications for such systems[6].

III. PROBLEM DEFINITION

Unease close by the outside control of safety primarily based totally on services. The troubles without the settlement of cloud computing are because of huge elements to the non-public & public sectors. It's the very nature of cloud computing primarily based totally on services, non-public or public, that help outside control of supplied services. The particular trouble addressed in thispaper is the way to assemble a essentially hashing set of rules device to obtain the above safety goals. We additionally be aware that there exist different safety troubles which are similarly essential for a nearly system of picture sharing, including the authenticity and availability of the shared picture.

IV. PROPOSED SOLUTION

In this paper, we tend to are realize the higher manner for the secure image. It looks that the idea of hashing algorithmic rule could be a promising approach that fulfils the said security requirements for image sharing. So we are consider the however secure the image in cloud computing and that's why we are mistreatment the OR code for security. Hashing algorithm options a mechanism that permits a sender to append to the write in code image specified the receiver will scanning the QR code and decode the image. The QR code is first scanner that protects you, your Image, and your identity from on-line threats by checking the security of internet sites coupled to QR codes before they get load on your mobile device. As indicated in figure, A hashing algorithm and QR code based mostly image sharing system work as follow: Step1: The sender uploads the image and shared with the receiver. Step2: once sender send the image to the receiver the QR code generate automatic for specific key. Step3: once receiver receive the image, he work the Id and scanning QR code. If receiver areauthorised person he will see the image otherwise cannot see the image.

V. METHODOLOGY

When it involves the hash time period withinside the virtual world, it generally refers to a cryptographic hash. This is essentially the "fingerprint" of a few facts. A hash is a random-searching string of characters that in my view identifies the facts in question, simply because it identifies your fingerprint. You can reproduce any

facts, both a file (consisting of a tune MP3 or spreadsheet) or only a string of characters (consisting of a password). Find the hash whilst you are jogging facts the usage of a hash generator. Whenever you've got the equal facts, you'll get the precise equal hash price as a result.

A. VISUAL CRYPTOGRAPHY

Visual cryptography (VC) is an encryption procedure on pictures (or text) during which decoding is finished by human tactile framework. During this strategy, an image is scrambled into a number of pieces (known as offers). At the point when the printed shares are superimposed together, the pictures are regularly decoded with human vision. In visual cryptography a seed is divided into shares which is distributed between a user and stored in the cloud. When all the shares overlap, a seed image or also known as secret image is revealed to the user. This report gives exhaustive comparative study of visual cryptography techniques based on cloud computing and MD5 algorithm. It also presents similarities between the systems, differences in approaches used in the systems, algorithms used and pros and cons of each technology.

B. ENCRYPTION

In cryptography, encryption is the manner of encoding a message or facts in this sort of manner that most effective legal events can get entry to and unauthorized events can't get entry to it.

C. DECRYPTION

Decrypting is the manner of taking encoded or encrypted textual content or different facts and converting it lower back into textual content which you or the laptop can study and understand. This time period might be used to describe a way for interpreting facts manually or without decrypting facts the usage of the precise codes or keys. In this report, we're using the hash set of rules and the QR code for overall facts security.

D. HASHING ALGORITHM

A hashing set of rules is a cryptographic hash feature. It is a mathematical set of rules that maps facts of arbitrary length to a hash of a hard and fast length. A hash feature set of rules is designed to be a one-manner feature, infeasible to invert. However, in current years numerous hashing algorithms were compromised. This befell to MD5, for instance — a widely recognized hash feature designed to be a cryptographic hash feature, that's now so clean to reverse — that we should most effectively verify facts in opposition to unintended corruption. Its clean to parent out what the proper cryptographic hash feature have to be like:

1.It have to be rapid to compute the hash price for any sort of facts;
2.It have to be not possible to regenerate a message from its hash price (brute pressure assault because the most effective option);
3.It have to be infeasible to locate messages with the equal hash (a collision);
4.Every extrade to a message, even the smallest one, have to extrade the hash price. It has to be absolutely distinctive. It’s referred to as the avalanche effect.
Hashing is used for :

• Document Management
• Password storage
• Digital signatures
• File management

Cryptographic Hash Functions are,

1. MD5: - The Message Digest five set of rules produces 128-bit hashes in period, expressed as 32 hexadecimal characters. Introduced in 1991.

2. SHA: - The Secure Hashing Algorithm is to be had in distinctive formats. The maximum usually used for not unusual place functions for the time being are SHA1 and SHA-256, which produce a hundred and sixty and 256-bit hashes respectively.

VI. PROPOSED WORK

In this paper, we have a tendency to attempt to secure the info in the cloud. The matter is that the user will access cloud or net mistreatment of any browser. contemplate the user is using Gmail accounting for accessing its data and suddenly his browser finishes off however the user remains logged in. Next time another user or anyone opens the browser there's a choice to restore it. Once clicking on restore the browser can open all tabs that were previously open and during this case the Gmail account is open therefore another user can access its data.

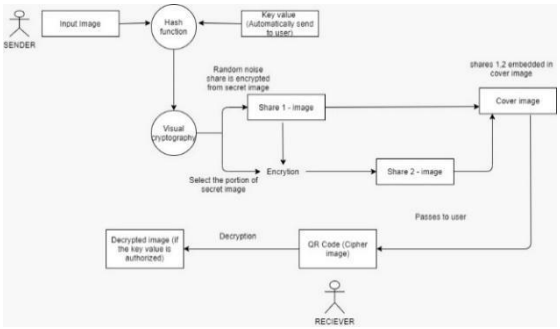
The planned system involves various steps in the method of storing and retrieving the info secured in a very cloud computing environment. 1st achieving initial authentication by the secure random range generation used for making a novel key for every user. Then the uploaded file is encrypted by homomorphic authentication combined with QR code. This mixture of cryptography code is keep in 3 totally different servers. A secret is given to the user at time of download. The info is downloaded from servers if the key is correct. The info is united and decrypted before showing it to the user. In our project, Forward secrecy is employed for advanced security. Revoke users will access the previous or subsequent knowledge so a rescindable identity primarily based cryptography technique is used. One factor is that if a user produces a key for shared data this key mechanically mails to a particular user.

Users can create key or parole for shared data also. we have a tendency to are reaching to offer 2 choices for making keys :

1. User can create key per data means that if user shared a specific file, doc etc to quiet one user then all shared data users can have the same key to access the shared data.

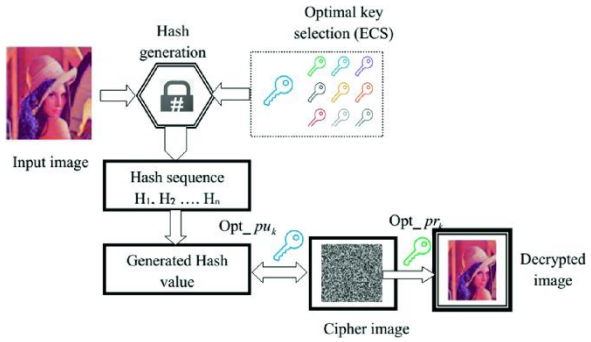
2. User will produce key per user means that if user shared a specific file, doc, etc to quiet one user then all shared user have totally different keys to access the same shared data.

International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 02, February 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

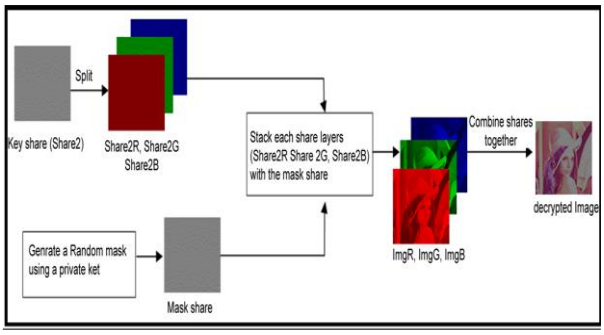


Fig(VI. 1).Data Transmission using Visual Cryptography and Hash Algorithm with QR Code Encryption

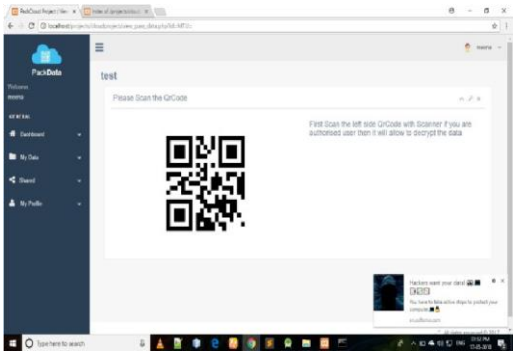
VII. IMPLEMENTED RESULTS



Fig(VII. 1).Secure image sharing using cryptographic hash function

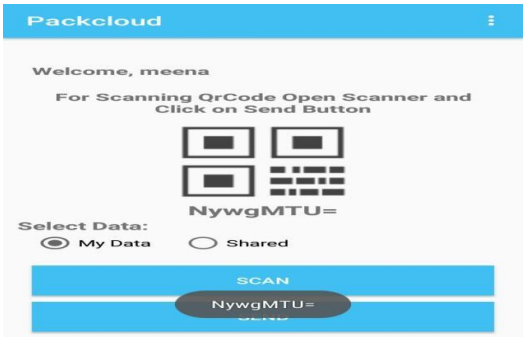


Fig(VII .2).Secure image sharing with Visual Cryptography Scheme using Private Key

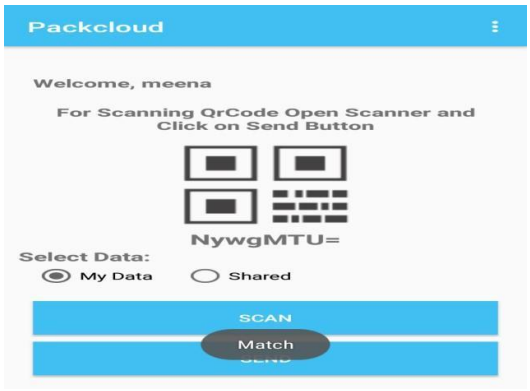


International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 02, February 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

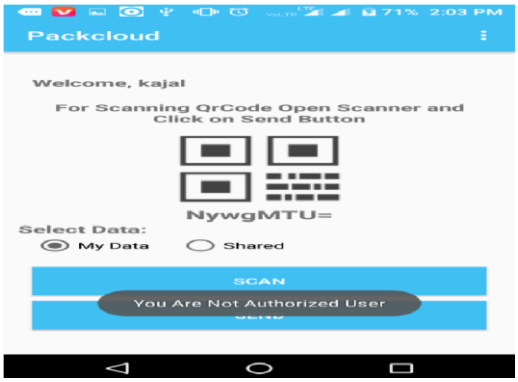
Fig(VII .3).Scanning QR Code



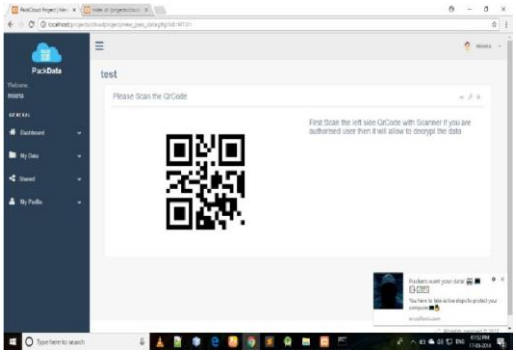
Fig(VII .4).After Scanning QR Code is key



Fig(VII .5).Key is matched



Fig(VII .6).After scanning the key, popup is send to the unauthorized user



Fig(VII .7).So the unauthorized user cannot see the actual image

VIII. CONCLUSION AND FUTURE SCOPE

In this system, we have presented a way to analyse information which is obtained from extraction of real time data. This proposed system will help user to have higher security while using cloud computing. In this paper, an efficient method for securely storing and retrieving images using Hash algorithm with QR code encryption and visual cryptography is proposed. The primary objective of image encryption is to transfer an image securely over a connected hostile network so that no unauthorized user should be able to decrypt the image. In relation, the quality of the reconstructed image should be maintained. The combined effect of the Hash algorithm with QR code encryption and visual cryptography makes the proposed algorithm much more secure and resistant to external attacks. As a future work, the time complexity taken for the completion of the entire process can be reduced.

REFERENCES

[1] L.Rodero-Merino, L.M.Vaquero, J. Caceres and M. Linder," A ruin withinside the clouds: toward a cloud defination", ACM SIGCOMM Comp.Communication Review pp. 50-55, , vol. 39, no. 1, 2008.

[2] M. Franklin and D.Boneh,"Identity-based encryption from the weil pairing" ,SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003. sharing with ahead security", IEEE Transactions on, DOI: 10.1109/TC.2014.2315619.

[3]Stojmenovic, S.Ruj and A.Nayak, "Decentralized get entry to manipulate with anonymous authentication of information saved in clouds, Parallel and Distributed Systems", IEEE Transactions on, 2014, no. 2, vol. 25, pp. 384-394.

[4]Asha,Yojita,Pranothi,Vuba,P.V.G.K.Jagannadh a Raju,"Secure information sharing in Cloud Computing Using Recocable-Storage Identity-Based Encryption",International Journal for Modern Trend in Science and Technology,Vol.3,2017.

[5] Rongmao Chen, Yi Mu, IEEE, Guiomin Yang, Member, Fuchun Guo and Xiaofen Wang,"DualServer Public-Key Encryption with Keyword Search for Secure Cloud Storage",1556- 6013(c)2015 IEEE.

[6] Kishor Babu V,R Amutha,"Secure Data Sharing in Cloud Computing Using RevocableStorage Identity Based Encription",IJSDR1706010.

[7] Prof. Jagruti Dange,Sheetal Y.Gaykwad,Gauri K.Khule,Linakshi N.Ahire,Mansi S. Bodhai,"Advanced Secure Data Sharing In Cloud Computing the usage of Revocable Storage Identity Based Encryption",Vol.4,ISSUE 4,APR-2017.

[8]Shashikumar,PuneethHegade,Siddarth Gopinath, Zabiulla, Mrs.Sridevi K N,"Secur information sharing in Cloud Computing Using Revocable Data Using CP-ABE Techniques",Issue 05,Vol.4,2017.

[9] Prof. Hitesh Patel, Prof. Parin Patel, Prof Kiran Patel," Achieving Data Integrity in Cloud Storage Using BLAKE Hash Function", IJEDR Volume 2, Issue 2 ISSN: 2321-9939,2014.

[10] Sheena Sathyan, Shaji R S Professor", a hybrid technique for the stable transmission of h.264/avc video streams",Vol.4,2015.

[11] chintha.guntla aparna,G Mounika Reddy,G.Naga Sujini, "Revocable-Storage IdentityBased Encryption in Cloud Computing",vol.4,Issue No.3,2017.

[12] Meenu Verma, Rahul Gedam, "Multilevel Data Security through encryption set of rules And QR Codes", IJRCEMAS extent 2, issue10 ISSN:2394- 5036.

[13] M. Bellare, S. Keelveedhi "DupLESS: Server aided hashing for deduplicated storage," in Proc. twenty second USENIX Conf. Secure., 2013, pp. 179–194.

[14] J. R. Douceur, A. Adya, D. Simon, and M. Theimer, "Reclaiming area from reproduction documents in a serverless dispensed record system," in Proc. IEEE Int. Conf. Distrib. Compute. Syst., 2002, pp. 617– 624, doi:10.1109/ICDCS.2002.

[15] G. Wallace, et al., "Characteristics of old workloads in manufacturing systems," in Proc. USENIX Conf. File Storage Technol., 2012, pp. 1– 16.

[16] Z. O. Wilcox, "Convergent hash reconsidered," 2011.

[17]G.Ateniese,K.Fu,M.Green, and S. Hohenberger, "cutting-edge proxy re-encryption schemes with packages to stable dispensed storage," ACM Trans. Inform. Syst. Secure., vol. 9, no. 1, pp. 1–30, 2006, doi:10.1145/1127345.

[18] D. T. Meyer and W. J Bolosky, "A take a look at of realistic cloning," ACM Trans. Storage, vol. 7, no. 4, pp. 1–20, 2012, doi:10.1145/2078861.