INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 06 ISSUE: 06 | JUNE - 2022 IMPACT FACTOR: 7.185 ISSN: 2582-3930

A Two-Level Authentication Approach for Securing Data in Cloud

Dr.J.Vinothkumar [1], Logaiyan Parthasarathy[2]

[1]*Asst.Prof / Dept. of Computer Science, Rajiv Gandhi Arts and Science College, Puducherry, India.*
[2]*Post Graduate Teacher, PSBB Millennium School, Cuddalore, India.*

Abstract— **Security in Cloud Application has become a key concern in recent years since all industries are marching towards cloud technology. There are several concerns in providing a secure environment to various sectors such as finance, healthcare using a cloud-computing environment. The primary concern is to provide secure access to cloud-based applications. There are many existing solutions in use such as One Time Password (OTP) for secure access. But, in the present scenario, the two important issues that have to be addressed are the One Time Password (OTP) has to be encrypted before sending to the end-users and the authentication time for login should be reduced to keep the authentication process secure. This paper proposes an OTP generation mechanism based on the user credential for a Cloud-based electronic healthcare system for securing healthcare data. Hence, the proposed system addresses how to provide a secure OTP using the proposed secure algorithm to the end-user based on Short Message Service (SMS). This proposed system also provides a secure data sharing scheme for the dynamic group in a cloud environment. Any user in the cloud can share the data with other users by the use of a group signature. The group signature is generated with the help of end-user credentials for secure data sharing. A group member will send their credential to the group manager. After verifying the user credential, the group manager will provide the group signature to the group member for accessing and sharing data in the cloud. In the proposed system, the cost of computation is not dependent on the number of the revoked user.**

Keywords— **Cloud computing security, Authentication, OTP, Dynamic Password, Time Synchronization, Information and communication security, Trust.**

I. INTRODUCTION

Computing plays an important role in the day-to-day activities of an individual such as email, usage of a debit, credit card, and online transaction for booking the ticket and other purposes. Also, computing has the power to improve the speed of financial transactions in banks. The different types of computing are:

Parallel Computing – The method by which a single problem is solved using two or more processes is termed parallel computing.

Distributed Computing – The computational process that is carried out within a group of the computing system. This system can be located anywhere in the world. This type of computing is called a distributed system.

Grid Computing – The process of handling the distributed information or tasks among a group of networked computers with the aid of a single computer is termed grid computing.

Cloud Computing –The technology which maintains data and its applications through the internet and the central remote server are termed cloud computing. The vital characteristic of cloud computing is the mechanism through which consumers or business people can use an application or can access their data across the globe. The only criteria are the need for an internet connection. The services of storage, memory, processing are centralized due to these technology provides efficient computing and this emerges to be a recent advancement of computer technology

Cloud Computing can also be a specialized form of Distributed Computing. It differs from Grid Computing in the following ways:

- Scalability: It is scalable to a higher extent
- Virtualization: It can be abstracted as an entity and delivers services to customers present anywhere around the globe
- Services: It can be dynamically configured and delivery was done on demand.

Advantages of Cloud Computing

Cloud computing or the Cloud server offers several services to the client. The only thing that client needs to have is a PC or a smartphone and an internet to access the cloud server.

The cloud has the added advantage of having a mechanism to manage the resources that it has, balance the workload, and manage if there is any change of request. It is not just a collection of computer resources.

There is a rapid decrease in hardware cost and a great increase in computing power and storage capacity.

Elasticity is another enormous advantage of the cloud, whereby it can add an application etc., dynamically at the time of the client's request.

DOI: 10.55041/IJSREM15098

The cost that would be incurred by downloading and installing the needed software is eliminated in the cloud.

Cloud Service Models

- Cloud Software as a Service (SaaS) - Use provider's applications over a network
- Cloud Platform as a Service (PaaS) - Deploy customer-created applications to a cloud.
- Cloud Infrastructure as a Service (IaaS) - Rent processing, storage, network capacity,and other fundamental computing resources.

One Time Passwords

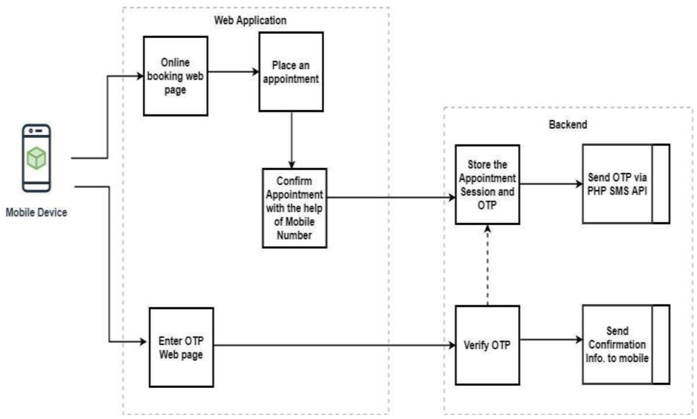


Figure 1: One-Time Password

A one-time secret key (OTP) is exactly what the names suggest, a secret phrase that is just legitimate for one login. The advantage of OTPs is that it offers a lot higher security than static passwords, in the cost of ease of use and arrangement issues. OTPs are insusceptible against secret word sniffing assaults, assuming an aggressor use programming to gather your information traffic, video records you when you type on your console, or utilize social designing, it doesn't make any difference since the secret phrase that the assailant gets hold of won't be legitimate to utilize. An OTP can be produced utilizing various strategies, and is frequently utilized related to a gadget that is synchronized with a validation server

Time sensitive OTPs: In the time sensitive strategy, a gadget with an interior clock creates passwords that are relying upon the current time. For instance, consistently another secret word is created in the gadget, and a similar secret phrase is produced at the verification server. At the point when the client needs to sign in to an assistance or framework, the current OTP that is shown on the gadget is utilized.

Data Security

Cloud computing is answerable for overseeing touchy information in a colossal volume. It permits different clients to share the information using explicit access privileges which shift from one client to another. Yet, since information proprietors and cloud storage are not situated in a similar believed space, it has become obligatory to encode the information prior to transferring it onto the cloud. Encryption algorithms assume a significant part in giving information security. The significant assignment of encryption algorithms is to ensure protection and security. The encryption calculations are named

- Symmetric Key Algorithms
- Asymmetric key algorithms

In symmetric encryption, a similar key is utilized for encryption just as unscrambling though in unbalanced encryption public key is utilized for encryption and a private key is utilized for decoding.

Data Security on cloud

Cloud security is a bunch of organization made rules to impede any conceivable type of information misfortune, breech, or inaccessibility. Cloud security is additionally a specific, add-on cloud administration that guarantees cloud conditions and the information put away in them are secure.

Cloud suppliers and security organizations wouldn't endure long assuming that they couldn't ensure their clients' information well. In any case, associations should choose for themselves which security highlights they require, and these may not be a one-size-fits-all suggestion.

For instance, fundamental cloud administrations will more often than exclude essential security highlights; be that as it may, ventures require undertaking grade security choices.

When moving to the cloud, security and IT experts are astute to comprehend their organization's danger craving and security pose so they realize what cloud-based controls will be essential. For instance:

Administrative consistence might be fundamental. Provided that this is true, the association will need consistence controls.

The viability of the information security required ought to be undeniable.

Cloud-based controls ought to be basically just about as powerful as on-premises controls. The cloud supplier ought to have actual security set up to guarantee that troublemakers don't approach gear.

To reassure customers, cloud suppliers offer administration consoles IT and security experts can use to guarantee that:

Their information and the cloud climate that has it are secure.

They have regularly updated knowledge into the present status of safety.

They get convenient notices of outside the allotted boundaries conditions and essential occasions.

They can recognize the underlying driver of issues and remediate them.

Given the quick development of information volumes, the speeding up speed of innovation advancement, and continually arising dark cap strategies, depending on the security of your cloud is a sensible choice. This is on the grounds that – whenever oversaw appropriately – it can give more noteworthy strength and security than in-house server farms. To understand that, notwithstanding, cloud security the executives and security the board ought to be adjusted and reliable.

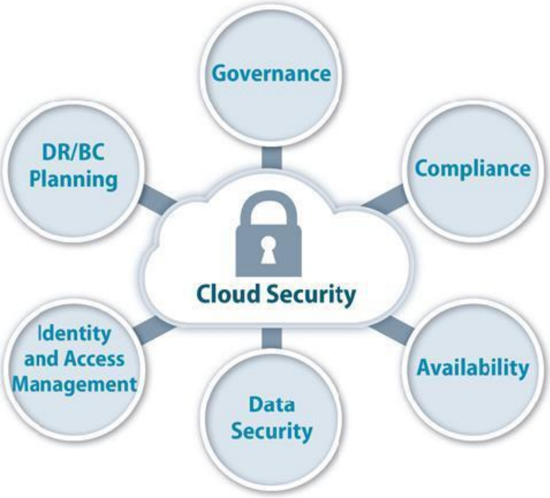


Figure 2: Cloud Security

Cloud Security Architecture

Cloud security design impacts the viability of cloud security. Coming up next are a couple of significant security the board tips you can use to sustain user's cloud environment.

Prevent The "best" sort of cyberattacks are those that fizzle from the start. The most ideal way to forestall an assault is to constantly:

Recognize weaknesses.

Focus on them dependent on their seriousness, danger insight, and the resources that would be impacted by the assault.

Remediate the focused on weaknesses by fixing them.

Tragically, most associations are not overseeing security weaknesses as consistently as they ought to. All things being equal, they're overseeing weaknesses intermittently, like Patch Tuesday, month to month, and so forth most associations likewise battle to focus on weaknesses since they can be so various.

Detect The association ought to have discovery controls set up that recognize issues and ready security work force when vital. Identification controls will quite often work couple with remedy controls that might be programmed, manual, or a mix of the two, contingent upon whether the circumstance is brought about by a minor mistake, a cyberattack, or one more kind of episode.

Correct Security episodes happen regardless security controls are set up. Before they occur, there ought to be remedy controls set up that limit the measure of harm an agitator can cause. For instance, assuming a programmer accesses an information base or delicate document, what occurs straightaway? In the event that the information are annihilated, are there calamity recuperation choices set up

Cloud Security Software and Services

Coming up next are a portion of the cloud security programming and administration choices organizations ought to consider:

IaaS or PaaS cloud security choices – these are add-on administrations that give endeavours more broad security choices than are accessible with fundamental cloud choices.

Character and Access Management (IAM) – these instruments guarantee that main approved gatherings approach information and figuring assets.

Actual security – IaaS/PaaS suppliers ought to have actual security – locked entryway, designated spots – notwithstanding advanced security to guarantee their IT resources stay secure.

- Encryption – scrambles information very still and moving.
- Entrance testing – outside advisors are employed as "white caps" to break into an organization's framework to recognize shortcomings.
- Consistence controls – guarantee adherence to HIPPA, GDPR, and so forth

Password Authentication

The multilateral framework architecture is probably the furthest down the line idea to ensure information. In this system set of rules will be intended to access and handle the information. Presently the inquiry is the way to ensure this multilateral design which is securing the information. Secret phrase confirmation is one of the broadly utilized verification strategies. It is successful, straightforward, and precise, with no additional expense. The strength of a secret phrase relies upon how powerful a secret phrase is produced to secure the framework. The interest is extremely clear and basic. In this base paper, we foster a secret word age framework by utilizing a reasonable structure plan to get strategies created by multilateral framework. The security will be two level security approaches. At first the framework will be created to produce dynamic secret word utilizing set of rules and afterward same will be utilized to validate the client while handling the information. So the whole reasonable structure will be planned such a way that it gives greater security to the multilateral framework in the cloud.

II. RELATED WORKS

Raghavendran et.al (2016) surveyed that a lot of large-scale organizations have migrated to cloud computing and relocating their business and have their designated storage unit attached along with it. The author elaborates in detail about the advantages and security regarding matters over the cloud environment. Sheta Patel and Mayank Bhatt developed a proposed algorithm in cloud computing by introducing the concept of assigning various time slices to each cloud user processes depending on the priorities of their task. Such a system results better than the existing round robin method. Sujareet kaur and vinay Chopra(2015) adding an encryption algorithm to the existing cloud services .It possess the security enabled service by using small size dynamic private key which operates the encryption / decryption algorithm. Such algorithm is secure and put forward to help identifying the cloud users and hackers and immediately reject them from cloud service. Scarlin and K.Curran (2013) introduce two technologies namely Multi-tenancy and Virtualization offers dynamicity which cannot be tracked. Such system results better than the conventional system. Nirmal and Sanjeev Kumar (2018) list out the various cloud security issues that may be possible at the cloud data transmission at the hybrid cloud. The cloud computing data transmission policy ensures whether the issues specified by the author are sorted and rectified before the actual transmission begins.

Choiet.al(2015) proposed a secure OTP algorithm which uses the IMSI number of registration of users and captcha images along with OTP to prevent from the various attack. Kysaw and Nay (2019) developed the OTP approach which is encrypted by RSA public-key encryption algorithm. Such type of encryption is more secure even for the third party user. Fazal et.al (2020) proposes the generation of OTP by using one of the hashing functions called the mid-square method. The encryption used in his system is the AES encryption algorithm. By this method, the generated OTP is used for many online transactions. Huiye and Yueqong (2013) developed a novel two-factor authentication scheme based on OTP which reduces the computation cost and also offers the secured transaction. OTP generator algorithm uses infinite and forward hash chaining methods to allocate memory for the hash keys. Dindayal Mahto and Dilip (2017) proposes the generation of OTP along with iris biometric for e-commerce transactions. Such type of OTP is shorter than RSA. This type of OTP is much secured and it is very difficult to hack by intruders. This proposed algorithm always uses dynamic keys which is very difficult to hack by the middleman because of confusing dynamic private keys. Krishna et.al (2015) developed ATM transaction security by generating and sending OTP through the GSM module to the client's registered mobile number. If the customer failed to register with the OTP, immediately ATM card will be blocked after the three successive wrong attempts. Abhskek et. al(2018) developed a framework that identifies the MAC address of the registered phone number's device which requires generating TOTP(Time-based OTP).TOTP is the offline secret hash code generated by the offline token generation mobile App. Sumathy and Ananthi Sheshaayee (2014) developed reliable m-banking authentication by introducing PIN along with the OTP. The PIN is mainly used to encrypt and decrypt the OTP which is known only to the client and the bank. Each time the PIN is verified and SMS is sent the client registered mobile number. Such a combination of PIN and OTP is more secured in case of any uncertainties arise due to any possible attacks such as middleman attacks or mobile theft.

Jaikumar V et.al (2021) proposed a cloud model which uses the cloud-based encryption algorithm and ring model along with fingerprint authentication on the cloud. Moganarangan et al (2017) developed a multilevel authentication system for the healthcare environment. In this paper, the author sectionalizes the fingerprint image into five divisions based on the fingerprint classification. The author suggested that the hacking of user fingerprint patterns is huge difficult when the sectionalized image is used for enrolment and matching. Ananya Bhattacharya et.al (2013) proposed an approach to speed up the matching process of fingerprint by classifying the fingerprint into different groups in enrolment which improves fingerprint matching. R.G.S.kumar et al (2017) developed Tri degree coalition which aims for dynamicity, user identity preserving, and privacy of user data. The author suggests the Virtual machine allocation policy to store the encrypted keys over the cloud environment

III. PROPOSED SYSTEM

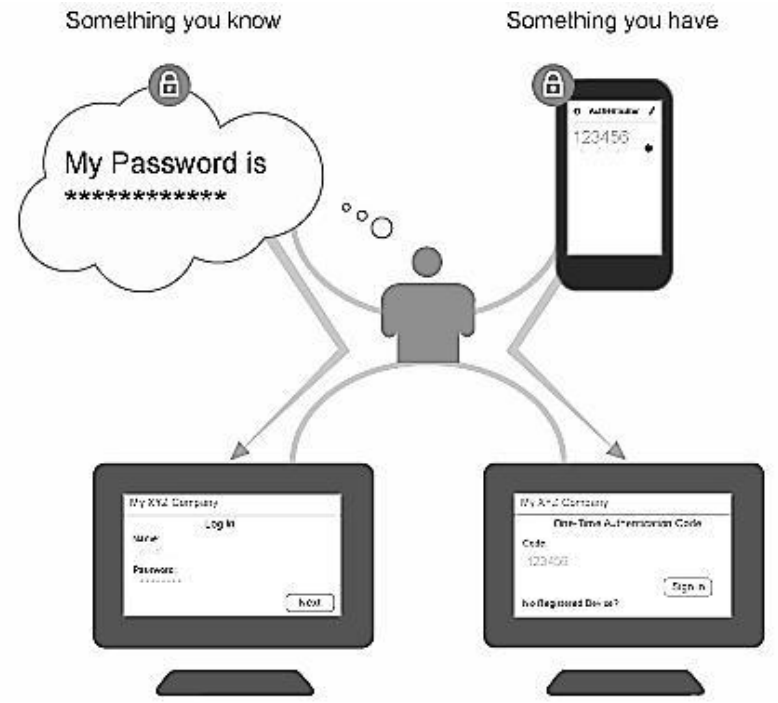


Figure 3: Two-factor OTP authentication

Authentication solutions

The previous section referenced the issues with static passwords and furthermore different issues related with various cloud suppliers' security arrangements, and how they can't be utilized acceptably in a cloud climate. There are ways of having a solid and simple to-utilize cloud administration that can fulfil these standards':

- Give a superior secret word answer for login strategies than the unreliable strategy for static passwords.
- Give a superior two-factor OTP verification arrangement than those talked about in the past part. 3. Have a straightforward enlistment framework, which simultaneously doesn't think twice about.
- Utilize an encryption calculation that is secure yet in addition quick, to have the option to serve the tremendous measure of cloud clients.
- Offer an answer that is for nothing to draw in more clients to the cloud administrations.

By and large, the security answer for cloud administrations should be not difficult to utilize yet in addition be extremely secure to ensure the clients' information and gain the trust of the clients.

Authentication with OTP: The authentication method utilized is two-factor validation with a one-time secret password with certain adjustments. The client's cell phone will function as the confirmation gadget, in which the client needs to enter a 6-digit PIN code to produce an OTP that can be utilized for login. The OTP that is created on the cell phone depends on three parts which will be hashed along with MD5:***6-digit PIN code that the client enters.***

A mysterious arbitrary number that was made during gadget introduction (Init-secret) that main exists on the client's cell phone.

OTP Generation

The significant undertaking of the proposed framework is to make a one-time secret phrase based on the random sphere value space to verify the clients to stay away from different digital assaults like a phishing assaults. The one-time secret key age conspire should have the option to create a bigger space of interesting passwords so it very well may be utilized to validate various clients all at once with no deception. The OTP adds an additional a security layer to ensure the client login.

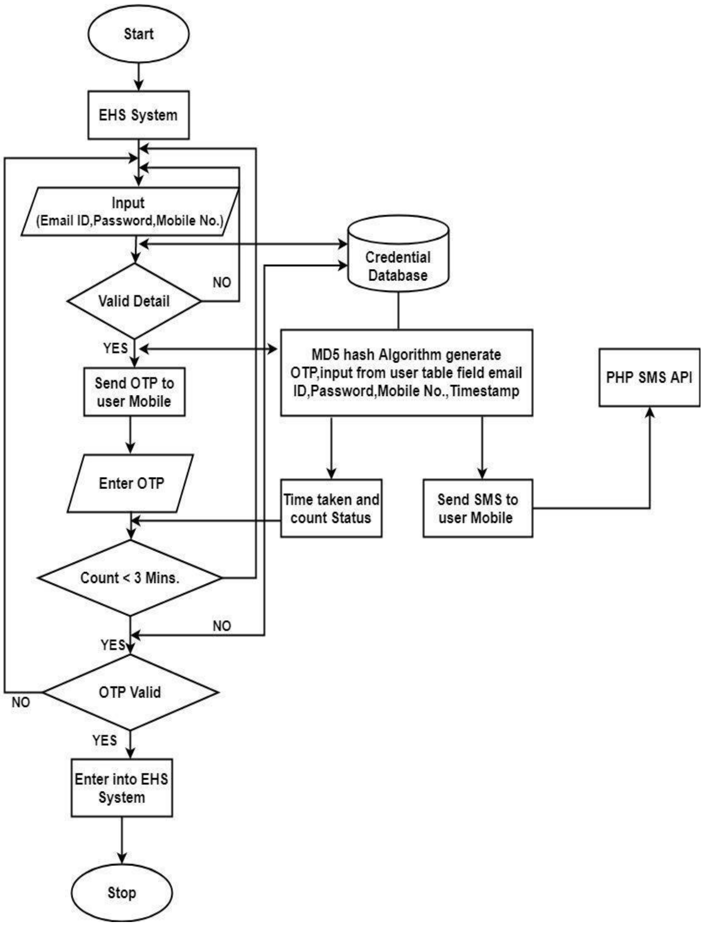


Figure 4: Flow Chart of OTP Login Security

OTPs are broadly utilized over the web for authentication. OTP age is utilizing values in the circle space-based irregular number age framework for enormous thickness clients on the double. The cubic irregular capacity gives the ability of a bigger number of arbitrary number mixes. The OTP age at first produces the network of million qualities. The various quantities of qualities are arbitrarily chosen among the million qualities created before and connect to make an OTP. Then, at that point, the perplexing number is changed over into a whole number based secret key is changed over into a picture utilizing visual encoding makes it safer and sends it by means of portable/SMS-based confirmation conditions.

Step1: Sphere Random Function to generate a random number

a) Initialization of the arbitrary number generator and work out the point of rise in the circle. The circle contains values in the open span, (- π/2, π/2) yet isn't consistently circulated.

b) Creation of the point of azimuth for every circle point dependent on consistently circulated in the open stretch, (0,2π)

c) Compute sweep an incentive for each point dependent on an open interval, (0, 6) not consistently circulated.

d) Rearrange and connect the arbitrary grid esteems and return OTP.

Step 2: encoding and decoding

We have created and carried out a symmetric key algorithm where OTP is encrypted at the customer side and transferred to an online distributed storage administration. Here we deal with the encryption cycle and encryption keys. At the point when the information is downloaded from the distributed storage administration we decode it utilizing the encryption keys.

The primary point of this calculation is to get the information while on the way, in spite of the fact that SSL(Secure Sockets Layer) is utilized to keep the information hidden by building up an encoded connect between a web server and a program while the information is on the way however by scrambling the information before it is sent gives an additional a layer of safety. Likewise, many specialist co-ops don't scramble information when it is moved between their own server farms which can prompt government interruptions, information misfortune and protection hazards, hazard of licensed innovation robbery, and spying endeavours, and furthermore many specialist co-ops don't have start to finish encryption. In this manner, encoding information at the customer side before it is transferred to a distributed storage administration can assist with managing such dangers.

Encryption algorithm

a) Extract each character from a record and get its comparing ASCII esteem.

b) Convert the ASCII worth to the relating parallel worth

c) Check in the event that the parallel worth is 8 pieces or not.

d) If not then add going before 0's to make it a 8-bit double worth.

e) Reverse the relating 8-digit paired worth.

f) Extract the initial 4 pieces from the switched 8-digit paired worth and opposite them.

g) Similarly, separate the last 4 pieces and converse them too.

h) Append the 4-cycle paired qualities acquired in stages 6 and 7.

i) The 8-cycle double worth acquired subsequent to attaching in sync 8 is the cipher text.

j) Convert this 8-cycle double worth to ASCII and compose the relating character to the encoded record.

k) The key is created by adding 10 to the ASCII esteem in sync 10, and the relating character is kept in touch with a different encryption key record.

Decryption Algorithm

a) Extract each character from the encoded document and get its comparing ASCII esteem.

b) Get the ASCII worth of each character from the encryption key record and take away 10 from it.

c) Check assuming that the qualities in stages 1 and 2 are something similar or not.

d) If they are not a similar then decoding won't be performed.

e) If they are a similar decoding will be performed by turning around the encryption calculation, i.e., by changing scrambled person over to comparing ASCII worth and afterward from ASCII worth to 8-bit twofold worth, breaking the parallel worth to 4 pieces, switching them independently, and attaching them and the switching the affixed paired worth.

f) The decoded character is kept in touch with a different unscrambling document which ought to be as old as content of the first record.

GROUP SIGNATURE

Any member of the group is allowed to sign the messages while the identity is kept secret from the verifiers. But when a dispute occurs the group manager might reveal the identity of the owner of the signature, and this is termed traceability.

In this proposed work we apply a group signature, which has the following properties:

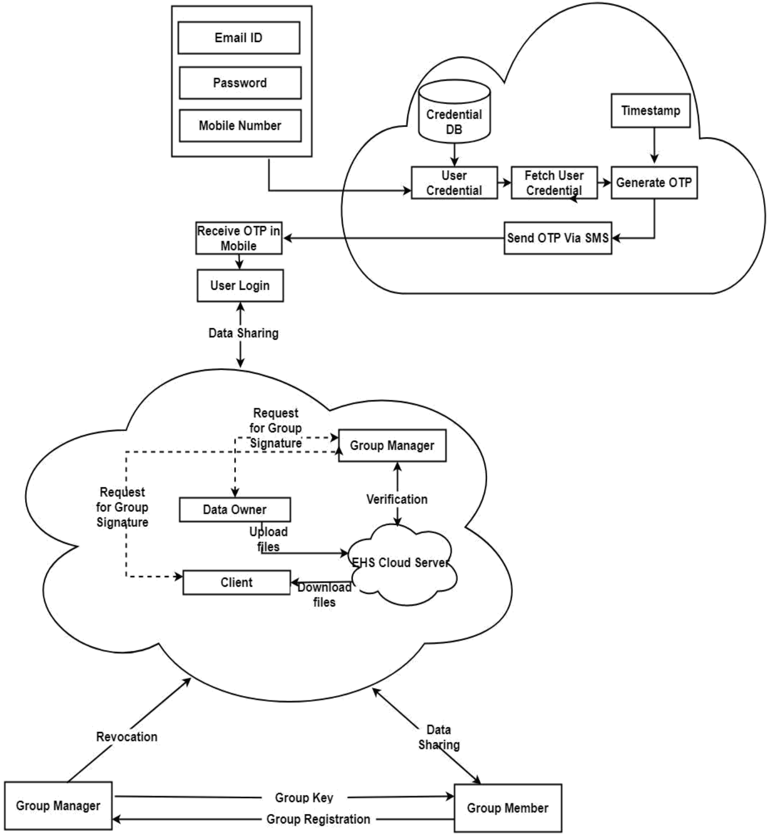
Only members of the group can sign messages;

a) The group signature can be verified by the member but the member who made this signature cannot be discovered.

b) These group signatures are a simplification of the credentials authentication schemes, in that every person has to prove that they belong to a certain group.

We consider a cloud computing architecture by combining with a healthcare example that a health care uses a cloud to allow its staff member in a similar group or division to share data. The cloud, group manager who is the administrator, and several group members who constitute the staff are the entities that comprise the system model. This model is illustrated in Figure

Figure 5: Proposed System Architecture



The CSP operates the cloud which provides the storage services with a price associated with the service. As the CSPs are outside the user's trusted areas the CSPs are not relied upon fully. The cloud server is honest and at the same time curious and hence tries to learn about the data content and the identity of the cloud users. But the cloud server does not delete or modify the data due to the presence of the auditing scheme.

The group manager has a responsibility to generate the parameter for the system, registration of the user, revocation of the user, and during the dispute, it has to reveal the real identity of the data owner. In the given health application, the group manager is acted by the administrator of the hospital/ health care. Therefore, we assumed that the other parties having full trust in the group manager.

A set of registered users are the group members who store their private data in the cloud server and share them with other members of the group. In the health care application which we use, the group member's role is played by the staff members. The group is dynamic as the staff members resign and new staff members join the company.

IV. EXPERIMENTAL SETUP &RESULTS

The results obtained and the experimental setup of implementation of two-level authentication using the concept of Mobile OTP to access the private cloud.

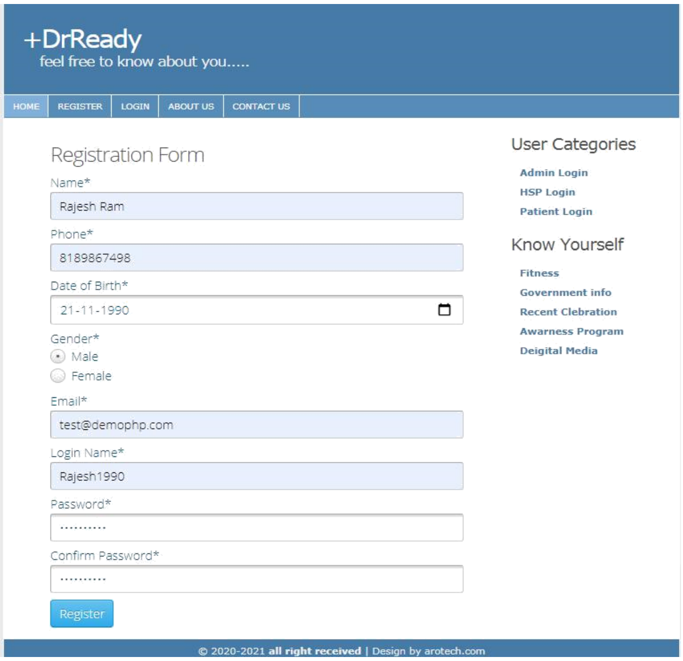
Server	Localhost
	Intel® Core™2 Duo processor
	4 GB hard Disk
	4 GB RAM
Operating System	Windows operating system(Windows 7 and above)
	Wamp Server
	(Apache, MySQL Server, PHP)
	FasttoSms API,
	CURL
	PhpSecurelib

Table 1: Software Requirements

WAMP Server is a collection of open-source software used to create a web server. The collection consists of Linux – the operating system, Apache server – the server, MySQL– the database system, PHP – the programming language

FasttoSMS API is used to send OTP from a PHP application. The user need to register and subscribe to the SMS service

PHPSecurelib is a Machine Learning API that is used to encrypt the uploaded medical report and it gets decrypted when the doctor download file



Registration Form

Name*
Rajesh Ram

Phone*
8189867498

Date of Birth*
21-11-1990

Gender*
● Male
○ Female

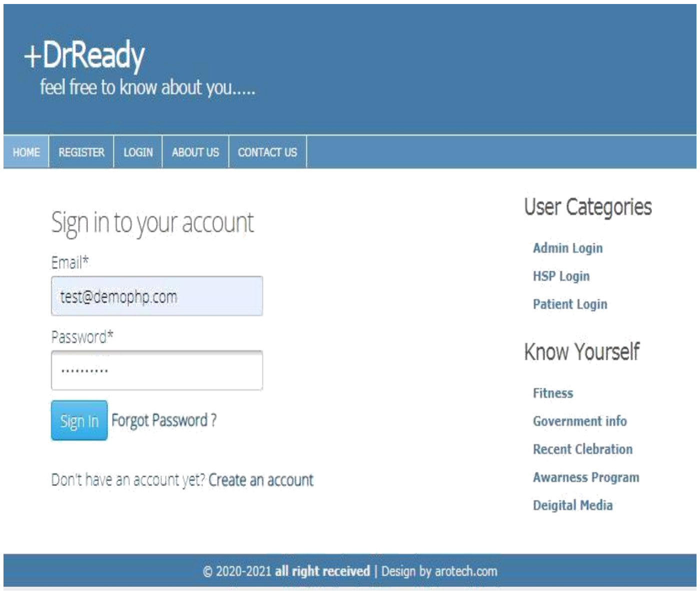
Email*
test@demophp.com

Login Name*
Rajesh1990

Password*
....

Confirm Password*
....

Figure 6: We have successfully registered and now we move to the Login page



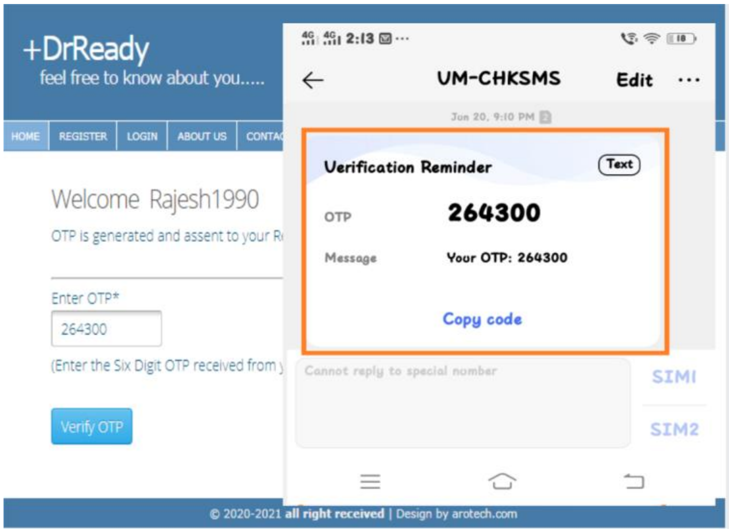
Sign in to your account

Email*
test@demophp.com

Password*
....

Don't have an account yet? Create an account

Figure 7: Level 1 Authentication (Username and Password Authentication)



Welcome Rajesh1990

OTP is generated and assent to your R

Enter OTP*
264300

(Enter the Six Digit OTP received from y

Jun 20, 9:10 PM

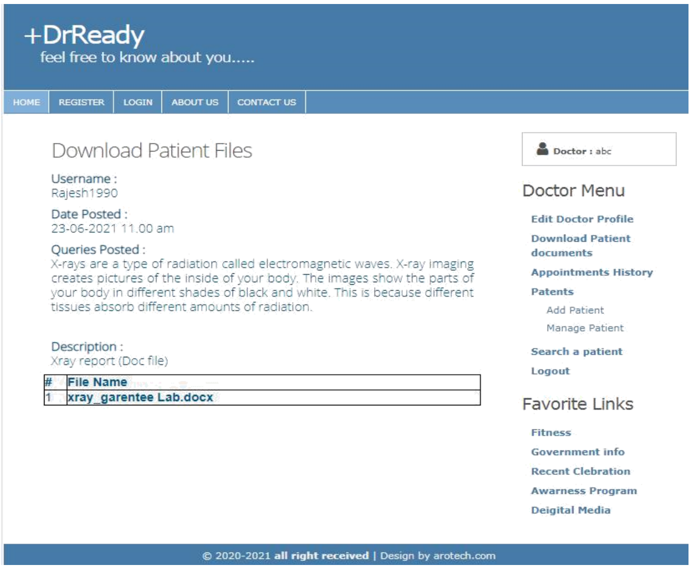
Verification Reminder

OTP 264300

Message Your OTP: 264300

Cannot reply to special number

Figure 8: Level 2 Authentication. OTP is only valid for 3 minutes. After that, the session expires and access is denied.



Download Patient Files

Username :
Rajesh1990

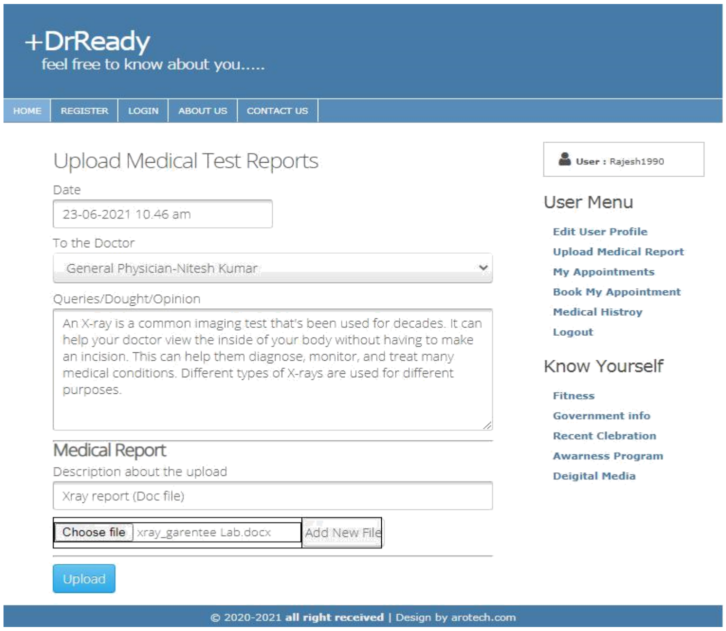
Date Posted :
23-06-2021 11.00 am

Queries Posted :
X-rays are a type of radiation called electromagnetic waves. X-ray imaging creates pictures of the inside of your body. The images show the parts of your body in different shades of black and white. This is because different tissues absorb different amounts of radiation.

Description :
Xray report (Doc file)

#	File Name
1	xray_garentee Lab.docx

Figure 9: After successful authentication, user-uploaded documents are encrypted and stored in cloud storage.



Upload Medical Test Reports

Date: 23-06-2021 10.46 am

To the Doctor: General Physician-Nitesh Kumar

Queries/Dought/Opinion: An X-ray is a common imaging test that's been used for decades. It can help your doctor view the inside of your body without having to make an incision. This can help them diagnose, monitor, and treat many medical conditions. Different types of X-rays are used for different purposes.

Medical Report

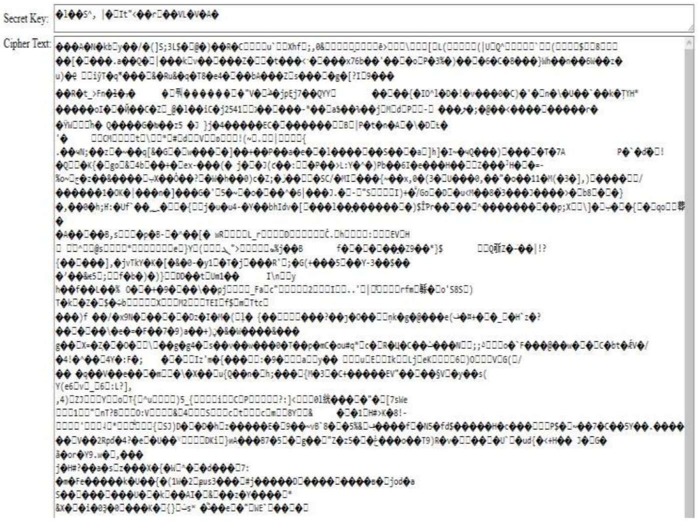
Description about the upload: Xray report (Doc file)

Choose file xray_garentee Lab.docx Add New File

Upload

© 2020-2021 **all right received** | Design by arotech.com

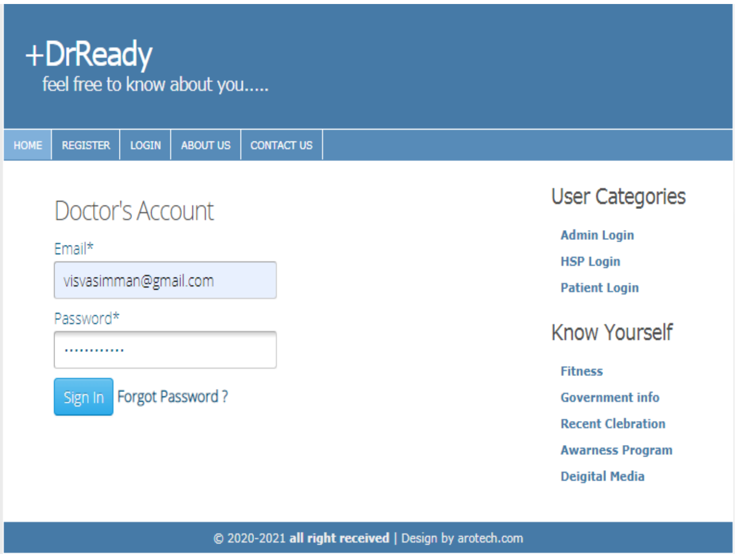
Figure 10: Files stored in remote cloud



Secret Key: �1��S^, |�It"<��r��VL�V�A�

Cipher Text: [illegible]

Figure 11: File gets encrypted in cloud server



Doctor's Account

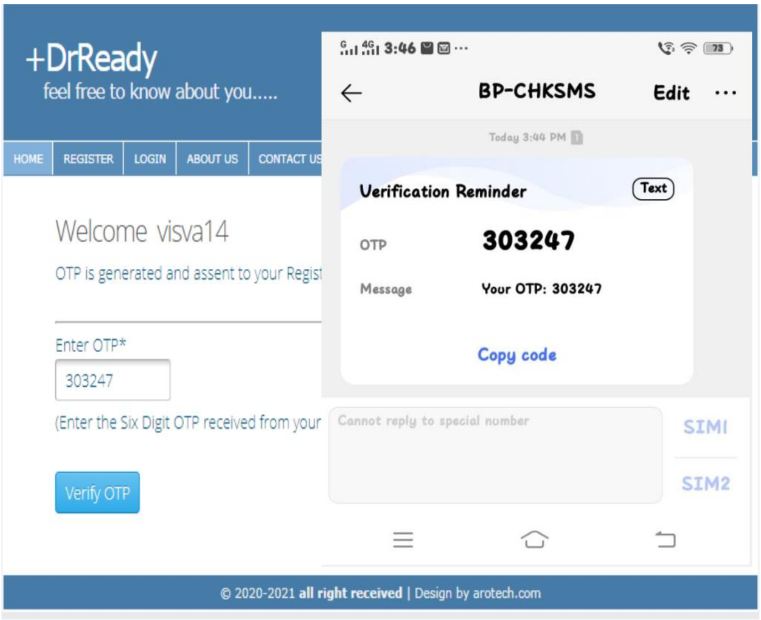
Email*: visvasimman@gmail.com

Password*: ....

Sign In Forgot Password ?

© 2020-2021 **all right received** | Design by arotech.com

Figure 12: Like the user, the doctor can also login into the system



Welcome visva14

OTP is generated and assent to your Regist

Enter OTP*: 303247

(Enter the Six Digit OTP received from your

Verify OTP

Today 3:44 PM

Verification Reminder

OTP 303247

Message Your OTP: 303247

Cannot reply to special number

© 2020-2021 **all right received** | Design by arotech.com

Figure 13: OTP for doctor's registered mobile number

V. CONCLUSION AND FUTURE WORK

Any verification framework's core strength relies upon the likelihood of progress for breaking that framework for getting to the administrations given by the cloud specialist co-ops. In our proposed authentication scheme, the core strength is certification based validation, an OTP generation mechanism dependent on the client accreditations and gathering mark for client verification. For gaining admittance to the requested service, the aggressor needs to break all the authentication layers. Security investigation says that increments as the quantity of validation techniques in the framework, the likelihood of accomplishment for breaking the OTP-based verification framework comes to approach zero. Subsequently, by seeing the investigation of safety, we can say that there is an exceptionally less likelihood of breaking the client accreditation based verification framework. The proposed method takes more space than the current verification strategy which is extremely less, and furthermore we can say that it is immaterial on account of a cloud environment where a lot of capacity and it's versatile.

VI. REFERENCES

1. V. Jaikumar and K. Venkatachalapathy, "Integrative optimization with Qos using multi-level security in medical cloud," J. Ambient Intell. Humaniz. Comput., 2021.
2. J. Hamdard, N. Delhi, P. Agarwal, J. Hamdard, and N. Delhi, "Cryptography Based Security for Cloud Computing System," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 5, pp.2193–2197, 2017.
3. Journal, E. Engineering, and S. Kumar, "Security in Cloud Computing: A review," vol. 10, no. 2, pp. 927–936, 2018.
4. V. Paranjape and V. Pandey, "An Improved Authentication Technique with OTP in Cloud Computing," no. 3, pp. 22–26, 2013.
5. C. V. Raghavendran, G. N. Satish, P. S. Varma, and G. J. Moses, "A Study on Cloud Computing Services," Int. J. Eng. Res. Technol., vol. 4, no. 34, pp. 1–7, 2017.
6. S. Carlin and K. Curran, "Cloud computing security," Int. J. Ambient Comput. Intell., vol. 3, no. 1, pp. 14–19, 2011.
7. H. J. Kim et al., "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption," Int. J. Electr. Comput. Eng., vol. 8, no. 1, pp. 1–18, 2018.
8. M. Robinson Joel, V. Ebenezer, M. Navaneethakrishnan, and N. Karthik, "Encrypting and decrypting different files over different algorithm on cloud platform," Int. J. Emerg. Trends Eng. Res., vol. 8, no. 4, pp. 1379–1383, 2020.
9. N. Chandrakala and B. Thirumala Rao, "Migration of Virtual Machine to improve the Security in Cloud Computing," Int. J. Electr. Comput. Eng., vol. 8, no. 1, pp. 210–219, 2018.
10. Kyaw Swar Hlaing | Nay Aung Aung, "Secure One Time Password OTP Generation for user Authentication in Cloud Environment," Int. J. Trend Sci. Res. Dev. , vol. 3, no. 6,89–92, 2019.
11. H. Parmar, "Generation of Secure One-Time Password Based on Image Authentication," pp. 195–206, 2012.
12. H. Liu and Y. Zhang, "An improved one-time password authentication scheme," Int.Conf. Commun. Technol. Proceedings, ICCT, pp. 1–5, 2013.
13. E. Erdem and M. T. Sandikkaya, "OTPaaS-One time password as a service," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 3, pp. 743–756, 2018.
14. H. Choi, H. Kwon, and J. Hur, "A secure OTP algorithm using a smartphone application," Int. Conf. Ubiquitous Futur. Networks, ICUFN, vol. 2015-Augus, no. 2, 476–481, 2015.
15. J. V. Kumar, K. P. Kumar, K. Srinadh, and K. S. Kumar, "International Journal of Research Publication and Reviews Biometric Attendance System Over IOT," no. 2, pp.494–497, 2021.
16. K. N. Pandey, S. Kumari, and P. Dhiman, "ATM Transaction Security Using Fingerprint / OTP," vol. 2, no. 3, pp. 448–453, 2015.
17. M. A. Hassan, Z. Shukur, and M. K. Hasan, "An Improved Time-Based One Time Password Authentication Framework for Electronic Payments," Int. J. Adv. Comput.Sci. Appl., vol. 11, no. 11, pp. 359–366, 2020.
18. Karia, A. B. Patankar, and P. Tawde, "SMS-Based One Time Password Vulnerabilities and Safeguarding OTP Over Network," vol. 3, no. 5, pp. 1339–1343, 2014.
19. S. Zhao and W. Hu, "Improvement on OTP authentication and a possession-based authentication framework," 2018.
20. F. Noorbasha, C. R. Krishna, and S. Hafijullairshad, "FPGA Based OTP Generation System for Data Security," Int. J. Recent Technol. Eng., vol. 8, no. 5, pp. 1836–1839, 2020.
21. D. Mahto and D. K. Yadav, "One-Time Password Communication Security Improvement using Elliptic Curve Cryptography with Iris Biometric," vol. 12, no. 18, pp. 7105–7114, 2017.
22. N. Moganarangan, G. Sambasivam, N. Balaji, and R. G. Babukarthik, "Efficient multilevel authentication in an integrated pervasive healthcare environment," J. Adv.Res. Dyn. Control Syst., vol. 9, no. Special Issue 12, pp. 1661–1672, 2017.
23. Soe Moe Myint | Moe Moe Myint | Aye Aye Cho, "A Study of RSA Algorithm in Cryptography," Int. J. Trend Sci. Res. Dev. Int. J. Trend Sci. Res. Dev., vol. 3, no. 5, pp. 1670–1674, 2019.

24. Kaur, G. Narula, C. Science, and C. Science, "One Time Password Generation Using Mathematical Random Function In Sphere Space For Mid-Sized Applications", International Journal of Advance Engineering and Research Development, pp. 150–154, 2014.

25. Kulat, R. Kulkarni, N. Bhagwat, K. J. Desai, and P. Kulkarni, "Prevention of Online Transaction Frauds Using OTP Generation Based on Dual Layer Security Mechanism,"2016.

26. V. Gangwar, Ravishanker, and A. K. Luhach, "Mobile based secure authentication using TLS and offline OTP," Int. J. Control Theory Appl., vol. 9, no. Specialissue11, pp. 5253–5262, 2016.

27. M. A. Albahar, O. Olawumi, K. Haataja, and P. Toivanen, "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption," J. Inf. Secur., vol. 09, no. 02, pp. 168–176, 2018.

28. AnanthiShesashaayee and D. Sumathy, "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security", International Journal of Innovative Research in Computer and Communication Engineering, pp. 6192–6201, 2014.

29. H. J. Kim et al., "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint," Procedia Comput. Sci., vol. 5, no. 03, pp. 619–622, 2018.

30. R. G. S. Kumar, T. Nalini, and V. Saranya, "A COMPLETE PUBLIC AUDITING FOR DATA SHARING IN HYBRID CLOUD USING TRI DEGREE COALITION (TDC) ARCHITECTURE,", International Journal of Recent Technology and Engineering , vol. 117, no. 21, pp. 925–929, 2017.