ESP IJSHMS
ESP International Journal of Science, Humanities and Management Studies
ISSN: 2583-9756 / Volume 1 Issue 1 July 2023 / Page No: 9-13
Paper Id: IJSHMS-V1I1P102 / Doi: 10.56472/25839756/IJSHMS-V1I1P102

Original Article

Advanced Secure Model for Data Protection via Cloud Computing

Samina H. Khan[1], Deepali N.Kende[2], J. Jadhav[3], Priyanka Bonde[4]

[1,2,3,4]*Assistant Professor in International Centre of Excellence in Engineering and Management(ICEEM), Maharastra, India.*

Received Date: 12 June 2023 Revised Date: 20 June 2023 Accepted Date: 02 July 2023

Abstract: *Any cloud-based information hoarding model's main goal is to make it simple to access information without compromising its security. Any cloud information capacity model should consider security as a key aspect to ensure efficiency and well-being. In this research, we suggest a secure approach for cloud-based information security. The recommended method provides a remedy for a number of cloud security issues, including insurance of data from any infringement and insurance from a phoney approved character client, both of which have a negative impact on cloud security. The distributed computing issues and difficulties listed in this document compromise information security and protection. It explains the dangers and assaults affecting cloud-stored data. Better cloud-based information encryption is only one of the benefits and flexibility provided by our proposed paradigm for distributed computing security. On the distributed computing platform, it offers customers protection and flexibility when sharing information. Our architecture successfully implements distributed computing security features as encryption, identification and verification, and approval. This design also protects the system from any bogus information owner who can enter harmful data and undermine the main purpose of cloud services. We support the one-time secret key (OTP) as a logging method and transfer technique to safeguard clients and information owners from any fraudulent, unauthorised access to the cloud. Utilising a simulation of the model known as Cutting edge Secure Cloud Server (NG-Cloud), we run our model. These findings strengthen the security assurance measures for end users and information owners against fake users and fake information owners in the cloud.*

Keywords: *Cloud Computing(CC), One time password (OTP), Next Generation Cloud(NG-Cloud), Cloud Server(CS), Public Key(PK)*

I. INTRODUCTION

The method of communicating computing administrations has been dramatically changed by distributed computing [1]. A growing number of defenceless devices (clients) rely on distant servers (hubs) for data storage and computations in rethinking calculating models [2]. An enormous amount of force is being used by the growing number of cloud server farms throughout the world [3]. Distributed computing is emerging as a brand-new approach to fully distributed processing. With the aid of using prohibitively large amounts of capital speculations, it has pushed the calculation away from indigenous computers and small businesses to huge scope in-line offices and made it wonderful for clients and IT organisations. Numerous problems and challenges that are related to the limitations of distributed computing have been the subject of much research [4]. Data communities, which are essentially predicated entirely on virtualization advancements, are a supplier that adds distributed computing (CC). During the Corona virus emergency, distributed computing functions with collaboration, communication, and basic internet-based administrations [5]. Such assessments are carried out by scientific collaborations that pursue a variety of goals and make clear attempts to develop the processing systems [6]. A significant capability of the cloud information distribution centre is to protect the security of sensitive data, which may be accomplished via steganography and cryptography techniques [7]. Numerous little files may contain large amounts of data. Concerns about safety exist, including data loss, dependability, and the outrageous hazards that botnets provide to organisations' data and code.

II. RELATED WORK

Model consists of four organisational gatherings:
(1) The owner of the information who utilises the cloud for information support and has information stored there,
(2) Data owners might be businesses or individual clients.

(3) When the information client accesses the information supplied by the information owner, he downloads relevant information and decrypts it with his secret codes.
(4) The confidential key generator (PKG), which creates and sends users' comparing private keys and sends the information owner's public keys.

When an authorised client discloses client name and secret word to an unapproved client, the framework is unable to determine whether that client is an approved client or not. As a result, only the approved clients were able to access and reestablish files accurately. This problem is a crucial requirement for cloud security because it makes it impossible to identify security violations in the event that an unauthorised client gains access to the system. This system also has the drawback of enabling toxic information owners to transfer files or information on the cloud server. False information owners have the ability to upload harmful data to the cloud and spread destructive diseases that can completely destroy the data stored there.
OTP is described as an erratic code generated by a cloud server, which is then sent to clients or information owners through email address before being sent, independently, to a mobile device for logging and transferring. In our suggested model, we address the concerns from the past by employing the one-time secret word (OTP) technique in two steps. On a distributed computing environment, the two steps are the client login process and the file transmission procedure.

III. PROPOSED MODEL

The Proposed Model's Approach. False information is one of the challenging difficulties in distributed computing. False information may suggest fewer problems that might annoy genuine goods. For instance, clinical records are transmitted information objects and experts are emergency clinics. According to evidence from actual patients, even mild drugs might be harmful in this situation. Because no patient fits such facts, the accumulation of false clinical information may be acceptable because no persistent condition could ever be addressed only on the basis of false information. In the scenario presented here, association A gives association B access to a mailing list that can only be used once. Association A provides suggestions that include addresses that are claimed through the association A approach. In this method, organisation B uses the purchased mailing list for each event, while association A receives duplicate mailings. This information comes from fake articles that aid in spotting inaccurate information use. Distributed computing allows in registering gadgets, with considerably less respect to their abilities and sizes, to keep up with gaining admittance to managing data encryption, The most complicated problem facing any insurance system or organisation is key control. Key control is a method for protecting encryption keys from bad luck, unauthorised access, and tampering. OTP is a logging method to protect clients against phoney authorization for access to the distributed computing environment. In the event that a client registers with the distributed computing environment, the cloud will then be required to send an OTP code message to both his private email address and private phone number. To validate his way of life as an authorised client, they successfully entered his OTP code into the cloud. This should be done by every client. To prevent any unauthorised client from accessing our framework inadvertently in our model, we included the OTP login between the clients and the distributed computing. In the suggested paradigm, OTP secures the login cycle to protect clients and their private data from any infringement. The OTP interaction is depicted in Figure 1(a) as a client downloads files from the cloud. While moving data to the cloud, the OTP process protects the information owner. When moving files from the owner of the information to the cloud, the OTP interaction is shown in Figure 1(b).

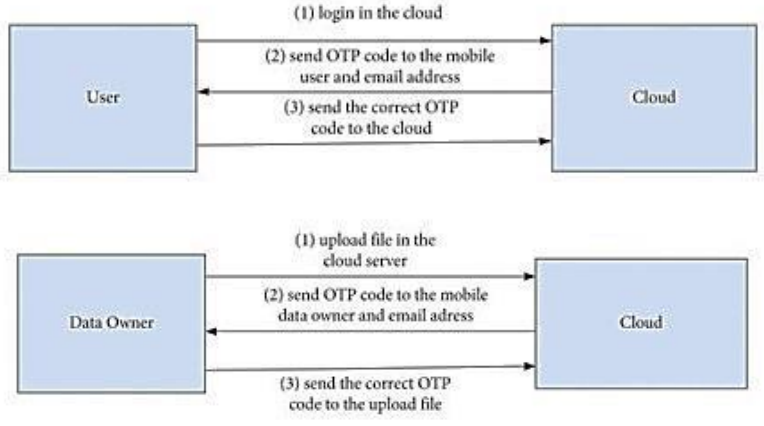

Figure 1: (a) The process of logging user on the cloud (b) The process of uploading file on the cloud OTP

The Proposed Model's Periods. Our model's PKG is a confided-in-outsider (TTP) structure, which functions with client- and information-owner interactions when both parties trust the outsider. Owners of information might be either individuals or organisations. PKG genuinely examines all basic method communications between the client and the information owner. The dependent parties (client and information owner) in this model make use of this trust to secure their own cooperation.

The suggested model's steps are depicted in detail in Figure 2, from the process of enrollment and logging in through the preferred method of receiving services. These are the four stages as they are listed.

Stage 1:

Client vs. Information Proprietor. Every client's public key and associated private key are generated by PKG. Every client has access to a public/private key pair, with the public key serving as the client ID. The information owner receives a client public key (Client ID) from PKG together with his corresponding private key. The client ID could be something like an email address, client personality card number, etc.

Stage 2:

Cloud clients versus data proprietors. In order to aid clients in understanding file content, the server's completion of information transmission includes a suitable description of the sort of information it contains. Information will be encoded using public key (PK) and SK.

Stage 3:

Information proprietor vs. the cloud. Prior to transmitting files, cloud should use the OTP interface to verify the information owner. Additionally, the cloud should support dynamic requests from information owners (such as granting or denying clients access privileges and enabling them to edit or delete their information).

Stage 4:

Client versus the cloud. Before clients download files, the cloud should provide them with a guarantee through the OPT process. By using a secret key, the information owner keeps the encrypted files in the cloud. Through the cloud, the owner of the information distributes a secret key to each client. A client should obtain the file's secret key when he needs to decode it. The mystery key alone is insufficient to decrypt the files, but clients can do so using both the mystery key and the private key together. From the cloud server (CS), the client will receive the encrypted files.

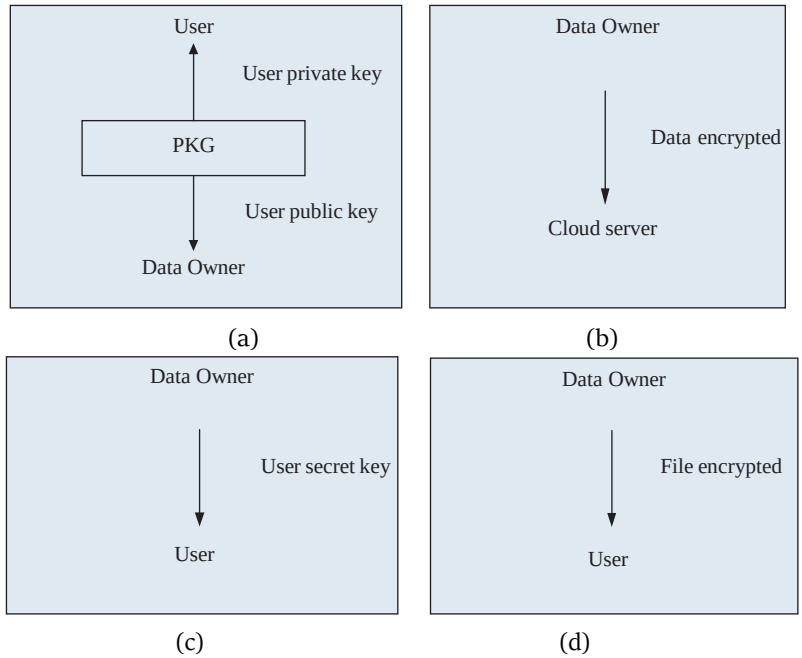

Figure 2: Phases for our model (a) Phase 1. (b) Phase 2 (c) Phase 3. (d) Phase 4

IV. EXPERIMENTAL RESULTS

We put our suggested strategy into practise in order to achieve cloud computing security and give consumers of the cloud top-notch services at any time and location. We run this model using our simulation of the NG- Cloud model.

The NG-Cloud toolkit, a Java-based toolkit for discrete-event cloud simulation, provides tools for creating applications, interfaces for assigning tasks to resources and overseeing their execution, as well as information services for locating resources. The NG-Cloud website offers the highest levels of end user and data owner security protection. These methods are used in the CAPTCHA-based login and registration processes. The registration and login procedures are shown in Figures 4(a) and 4(b). At this time, each user or data owner can sign up for our system by supplying their user name, password, email address, phone number, and CAPTCHA. After the registration process is over, each user and data owner can log in to the cloud. The cloud will provide the user or data owner an OTP number, which they must enter correctly to gain access to the system. To provide system authentication and security, OTP codes will be issued to the provided email address and phone number. Figure 5 is an example of an OTP code provided to a user or data owner through email. In the cloud computing security hierarchy shown in Figure 6, authentication is necessary in order to prevent unauthorised access. Therefore, we introduced the function Reset Password, which is a necessity to clear in order to access the data in the cloud, to secure the data in case any user or data owner loses or by the data can be in danger.

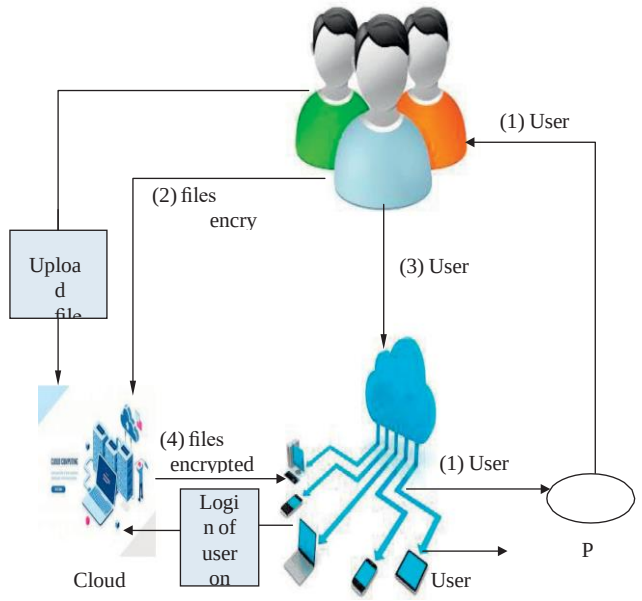

Figure 3: The proposed Model

(a) (b)

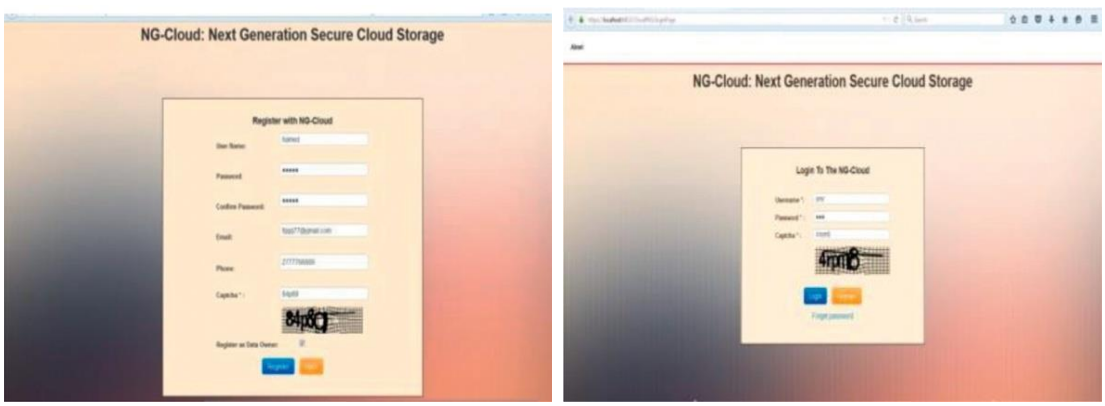

Figure 4: (a) Registration Process (b) Login Process

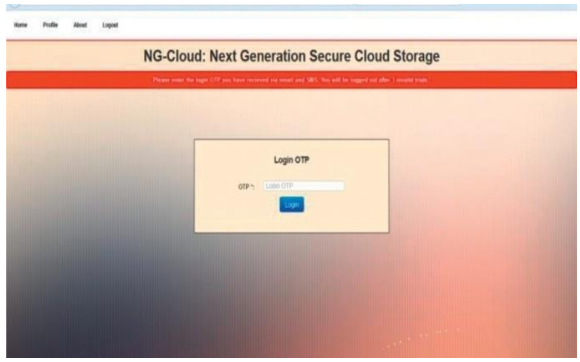

Figure 5: OTP Code

Figure 6: Reset Password

V. CONCLUSION

The way that computer services are delivered has changed as a result of distributed computing. The suggested model offered a solution to several distributed computing security concerns. One of the key pledges made to this model is the insurance of approved clients from any fake personalities. Additionally, the suggested approach guards against any fictitious information owner entering harmful information that could destroy the primary goal of distributed computing administrations. The advantages and effectiveness of safety in distributed computing were provided by our proposed paradigm. The proposed paradigm addresses the problem of striking a balance between convenience and security. The proposed paradigm also provided clients using distributed computing with security and flexibility while sharing information. The proposed model will be used with clinical information records in subsequent research. For its validity and importance, new configurations of various threats and attacks can be found. It is possible to improve the distributed computing environment's efficiency and appearance. It is anticipated that in the context of distributed computing, a safe help organisation will be suggested to create a broad strategy-based administration structure.

VI. REFERENCES

[1] H. A. Jadad, A. Touzene, K. Day, N. Alziedi, and B. Arafeh, "Setting mindful expectation model for offloading portable application assignments to versatile cloud conditions," Worldwide Diary of Cloud Applications and Figuring, vol. 9, no. 3, pp. 58-74, 2019.

[2] O. O. Olakanmi and A. Dada, "An efficient protection safeguarding approach for secure verifiable rethought registering on untrusted stages," Global Diary of Cloud Appli-cations and Figuring, vol. 9, no. 2, pp. 79-98, 2019.

[3] J. A. Jeba, S. Roy, M. O. Rashid, S. T. Atik, and M. Whaiduzzaman, "Towards green distributed computing an Algorithmic methodology for energy minimization in cloud server farms," Global Diary of Cloud Applications and Figuring, vol. 9, no. 1, pp. 59-81, 2019.

[4] K. Hossain, M. Rahman, and S. Roy, "IoT information pressure and enhancement procedures in distributed storage," Worldwide Diary

of Cloud Applications and Processing, vol. 9, no. 2, pp. 43-59, 2019.

[5] R. P. Singh, A. Haleem, M. Javaid, and R. Kataria, "Distributed computing in tackling issues of Corona virus pandemic," Diary of Modern Reconciliation and The board, 2021.

[6] B. Demin, S. Parlati, P. F. Spinnato, and S. Stalio, "U-Light, A confidential cloud approach for molecule material science figuring," International Diary of Cloud Applications and Registering, vol. 9, no. 1, pp. 1-15, 2019.

[7] P. M. ElKafrawy, A. M. Sauber, and A. M. Hafez, "HDFSX: large information dispersed file framework with little files support," in Procedures of the 2016 twelfth Worldwide PC Engi-neering Gathering (ICENCO), Cairo, Egypt, December 2016.