International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 8, Issue 9, September-2023, http://ijmec.com/, ISSN: 2456-4265

A SECURITY MODEL OF THE ENHANCEMENT OF DATA PRIVACY IN CLOUD COMPUTING

Zoha Fatima[1], T.Anita[2], Dr. Akhil Khare[3]
[1]PG Scholar, Department of CSE, ISL Engineering College
[2]Assistant Professor, Department of CSE, ISL Engineering College";
[3]Professor CSE Dept; MVSR Engg College ;

Abstract: Any cloud-based data storage strategy should make it simple to retrieve data without compromising its safety. Any model for storing data in the cloud must take security into account if it is to guarantee the safety and efficacy of the system. In this work, we advocate for a cloud-based data protection approach that is both robust and flexible. The suggested approach provides a remedy for a number of cloud security problems, including the inability to verify the identity of users and the disclosure of sensitive information. This study details a variety of problems and difficulties associated with cloud computing that endanger users' personal information and professional secrets. The risks and dangers associated with cloud storage are outlined. Improvements to cloud data encryption are only one example of how our suggested paradigm makes cloud computing safer. Users may feel safe exchanging data on the cloud because of its security measures and scalability. Achieving identity and authentication, authorisation, and encryption in the cloud is possible with our methodology. In addition, this architecture safeguards the system from any fictitious data owner who may submit harmful data with the intent of undermining cloud services' fundamental premise. To prevent users and data owners from falling victim to spoofed attempts to gain illegal access to the cloud, we create the one-time password (OTP) as a logging approach and uploading technique.

1. Introduction

With cloud computing, IT service delivery has changed drastically [1]. A rising number of susceptible devices (customers) store and calculate data on faraway servers (nodes) in outsourced computing models [2]. The expansion of cloud data centers globally has increased energy usage dramatically [3]. A new kind of decentralized computing called "the cloud" is developing. Blocking considerable financial investment has moved computing from individual PCs and small enterprises to big data centers, where it may benefit end users and IT service providers. Cloud computing literature has focused on challenges and difficulties arising from its concepts [4]. Cloud computing (CC) is a virtualization-heavy data center service. In the face of COVID-19, cloud computing simplifies collaboration, communication, and internet access [5].

Scientific research teams have several demands and techniques to designing computer frameworks [6]. The cloud data warehouse protects critical data contained in many apparently harmless files using steganographic and cryptographic methods [7]. Security challenges include data loss, compromised data integrity, and botnets threaten enterprises' data and software [8]. Data security is crucial in contemporary communication, particularly cloud-based [9, 10]. More people are using cloud computing every day, and enormous quantities of data are

DOI: https://doi-ds.org/doilink/09.2023-66483628

stored there. Cloud computing enables massive remote storage, mobility, information sharing, hardware and software cost savings, and more [11].

Attackers constantly exploit cloud security flaws, resulting in an annual rise in data spillage. To protect sensitive data in cloud computing settings, engineers and researchers are detecting cloud dangers and attacks [12]. Many data-secure cloud computing methods have been developed recently [13–17].

Migrating programs to the cloud and realizing the advantages starts with comparing record safety problems to cloud security challenges. The switch from on-premise to cloud-based software offers problems for companies, including data residency, organizational compliance, privacy, and third parties' responsibility for sensitive data. Corporate policies or national laws affect where sensitive data is held, what data may be gathered and stored, and who can access it. These challenges will effect firms' cloud computing valuation.

A centralized database stores user login information, and files posted and downloaded are encrypted and decrypted using an AES-based mostly architecture before being saved in the cloud. Admins may validate, lock, and retrieve IP addresses to create a more secure client identity framework. This authentication is sensitive to password guessing since users seldom reveal their password. Thus, cloud computing safety is essential nowadays. Overall, paintings increase cloud computing security and offer comprehensive cloud-based system protection [18].

The cloud lets everyone exchange data. When data is moved to an off-website online garage community managed by a third party (cloud carrier provider), data owners face new privacy risks, such as the carrier provider accidentally disclosing sensitive data, questions about the data's veracity and accuracy of data stored outside the carrier, etc. Cloud storage requires complete control over who may access data. Encryption was normal before the cloud conveyed this sensitive data. The user encrypts and saves his file on the cloud server in a conventional public key architecture with the decryption key only known to the authorized user. This method protects privacy but involves extensive control and distribution systems. The growing variety of software users renders this strategy useless.

Here are our contributions:(1) Our method verifies authorized users' identities without needing passwords. We also used OTP tracking and registration to prevent fraudulent registrations. Combining the secret key and private key strengthens encryption for users and data owners when they access cloud data.We innovate to protect cloud services and their consumers from cloud computing risks. Any cloud-based system design should consider certain considerations. We also discuss model security measures to protect a system, its users, and cloud data.Finally, (3) our method prevents replay, insider, and man-in-the-middle attacks. The work also has these advantages: Our method permits mutual authentication between the user and the authentication cloud server, anonymity, and safe password storage with the service provider. This decreases resources required to verify the sensitive data table's integrity.(4) The proposed solution overcomes the challenge of balancing security and usability to meet user demands.We use NG-Cloud simulation to install the recommended paradigm to avoid cloud computing security risks including authentication, authorization, and privacy.

DOI: https://doi-ds.org/doilink/09.2023-66483628

2. RELATED WORK

Cloud storage and other favorable developments led Xin Dong et al. [13] (Dong's plan) to promote data sharing in 2014. Dong's approach combines CP-ABE [19] and IBE [20]. Dong's design supports and protects dynamic operations like file creation and user access. Dong's network model has four nodes:Any cloud-based data exchange involves three parties: the data owner, who stores data in the cloud and relies on the cloud for data maintenance; the data user, who downloads data of interest and decrypts it using his secret keys; and the cloud provider, who hosts the data.(4) The private key generator (PKG), which gives users private keys and the data owner public keys.

Xin Since Dong's plan is safe and reliable, customers may access their cloud data on demand. The concept suggests using CP-ABE and IBE to offer privacy-maintaining information coverage with semantic protection.

After an authorized user gives an unauthorized user the user name and password, the system cannot detect whether the user is an authorized client. Dong's approach permitted only authorized users to access and recover data properly, but it did not address phony identities. For cloud trust, unauthorized client access to the system is a big security concern. Another problem is that a false data owner might upload dangerous material to cloud storage. Hackers may compromise a cloud service by submitting harmful data or uploading dangerous software as genuine users.

A cloud server generates a random code and texts it to clients or data owners' phones during logging and uploading. The two-stage one-time password (OTP) technique in our proposed solution addresses the above concerns. User login and cloud data transmission are the two stages.

Getaneh Berie Tarekegn et al. expanded their understanding of cloud computing by examining privacy and security challenges and describing solutions. Thus, IT leaders' main worry regarding cloud adoption has always been security. Each cloud computing component—approaches, OSes, storage, networking, and virtualization—has security problems. Cloud computing uses "pay per utilize" to share resources and cut prices. More features increase IT costs and privacy and security risks.

A privacy steering group to guide policy choices is also suggested. This group will prepare your organization to fulfill consumer and regulatory data privacy regulations. The increased use of cloud storage raises concerns about data accessibility, privacy, and territory. Cloud companies who disclose sensitive data face legal ramifications for their customers, who may violate equivalent government laws. Software developers must design cloud services to reduce privacy threats and ensure legal compliance. Cloud computing adoption is delayed owing to security and privacy issues. This article describes features, security-architecture, dangers, threats, and remedies. [21].

Eesa Alsolami listed many cloud computing vulnerabilities that threaten data privacy and security. This work proposes many mitigation strategies for these threats and raises some unsolved problems that must be addressed if we want a genuinely secure cloud computing environment [22].

DOI: https://doi-ds.org/doilink/09.2023-66483628

This report examined cloud computing's data security and privacy vulnerabilities, including these.(1) Unrestricted privileged access: Cloud service providers typically have free access to user data, making this a huge security risk.Two, because cloud service providers typically provide privileged individuals unfettered access to user data, some sensitive data may be compromised.Due to the complexity of the cloud, customers must depend on the cloud provider business for defensive surveillance, which may feel like an invasion of privacy.Fourth, many data centers backup consumers' data, which might cause discrepancies and leaks. This allocated storage increases information leakage, and synchronization problems cause data inconsistencies.International rules must mediate all customers' right of access and meet all consumer needs. Multidomain acquires the authority to govern cloud platform and presents security threats to client data stored in cloud due to interoperation on shared resources.Sixth, encrypting data at rest, in transit, and at rest is the most essential cloud computing information privacy technique. The decryption keys are needed to access sensitive information encrypted by encryption techniques.(7) Trust management: smooth and tough agree with control may solve cloud computing safety and privacy difficulties. Soft agree with control defines a date among the occurrences that may occur in any activity. Hard agree with control is a future trend for privacy and records integrity issues since it uses user-supplied digital infrastructure, which is typically constructed on unstable technology.

Cloud service providers should be held more accountable for security and privacy to protect consumer data. Compromised software interfaces, which may interact with cloud goods, provide a substantial security risk and need more examination into platform security integration. Separating sensitive data is another cloud computing difficulty that involves more research and less dependable data storage. Consistent user access, hacking, data leakage, and slow recovery procedures need more research [22].

Srijita Basu et al.'s study considers cloud security, but it must now include virtual machine (VM) security. This paper's major emphasis is identifying cloud security domain names and finding cautious remedies. This article discusses current cloud security holes and patching requirements. The need of understanding cloud computing security issues and developing solutions was stressed by offering a wide overview. Consequently, various cloud security models were created. The research's main goal is to accurately depict existing circumstances and future cloud protection options [23].

Feras Awaysheh et al. found that data security concerns drive cloud architecture adoption. A thorough safety diagram is impossible to develop without a preliminary evaluation that assures a realistic impermeable assembly and addresses local risks. It enabled a cutting-edge, security-by-design cloud BD framework architecture. It needs a completely automated security assessment mechanism and a systematic protection evaluation. It illustrated the multiple levels of cloud-specific security needs. This methodology links large data cloud security details to optimum planning [24].

DOI: https://doi-ds.org/doilink/09.2023-66483628

3. PROPOSED MODEL

3.1. The Methodology of the Proposed Model

False information plagues cloud computing. Using phony data may reduce real-world difficulties. The agents are hospitals and the data objects are patient medical records. In this case, changing patient data may be troublesome. Since no patient would be treated mainly on false data, inserting a bogus clinical data set may be allowed. firm A provides firm B a one-time mailing list. Address data from A is presented as hint data. Thus, business B always utilizes the bought mailing list and company A always gets the letter. These data are fake objects to discover data processing errors. Cloud computing allows internet users to access a range of services independent of device size or capabilities.

Encryption key management is the hardest security issue. Key control prevents encryption keys from being stolen or compromised. Key control is typically the main reason firms don't encrypt completely. Passwords and other safe entries are key. If a user forgets their password during encryption, cloud data cannot be recovered. Clients who use apparent passwords like email or spouse names pose additional security concern. The simpler the security key to guess, the lower the breach risk.

A user set (US), cloud server (CS), and data owner (DO) comprise our paradigm. OTP logging prevents users from being tricked into assuming they have cloud access. Cloud services seek users for authorization to send one-time-password (OTP) codes to their personal email and/or mobile phones. Each user must properly enter the cloud-provided OTP code to verify authorization. We used OTP login between users and cloud computing to prevent thieves from hacking into our system. OTP protects users' accounts and sensitive data during login in the recommended design. Figure 1(a) shows the user's cloud file download OTP method.

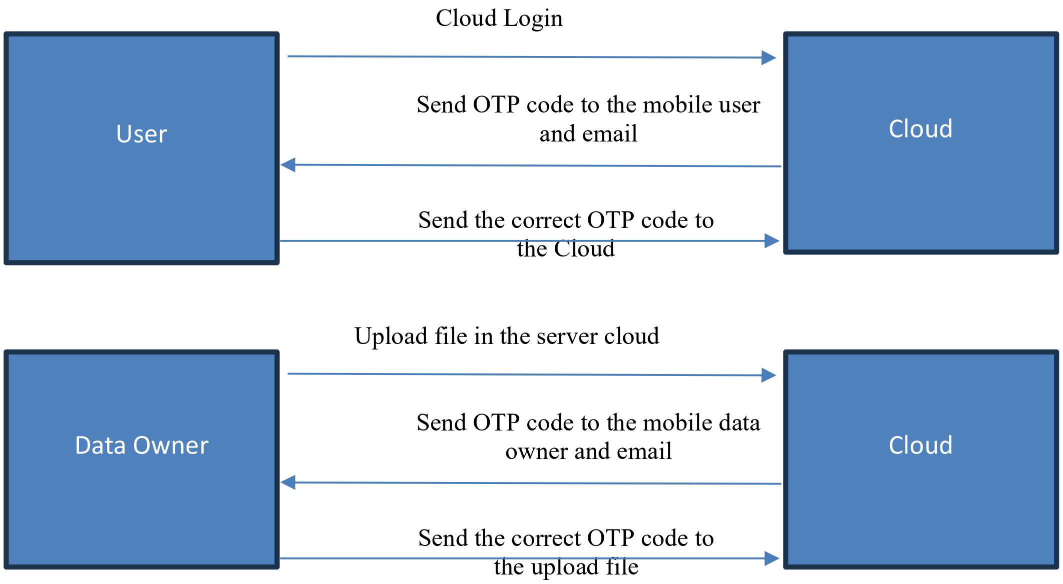
Cloud Login
User
Send OTP code to the mobile user and email
Cloud
Send the correct OTP code to the Cloud
Upload file in the server cloud
Data Owner
Send OTP code to the mobile data owner and email
Cloud
Send the correct OTP code to the upload file

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

However, a data owner may still use the cloud to store encrypted information. Owners' data has to be safe from any fabricated information. The phony data owner may introduce harmful data that might undermine the value of cloud computing. The cloud requires the owner of the data to provide an OTP code in text format prior to file upload. Each data owner will get an OTP code through his personal e-mail and/or SMS to his personal phone number. Encrypted information should be safe throughout the upload procedure to the cloud. The OTP method protects the data owner during cloud storage synchronization. The OTP procedure for file upload from the data owner to the cloud is shown in Figure 1(b).

3.2. The Phases of Proposed Model

Our model's PKG is based on the concept of a trusted third party (TTP), which mediates interactions between data consumers and data owners. A data owner might be an individual or a company. All user and data owner interactions are subject to rigorous testing by PKG. Both the user and the data owner may utilize this trust to safeguard their communications inside this paradigm.

3.2.1. Phase 1: Data Owner vs User

Each user's public and private keys are created by PKG. The public key is the user ID that may be downloaded by each user. PKG provides the data owner with both a user public key (User ID) and a private key. User IDs may be anything from a user's actual ID number to their email address. The user ID (public key) may be obtained by attackers with little effort. Therefore, it is important to protect the lines of communication between end users and the cloud server (CS). Users may sign up for a cloud storage account with the data provider. This is done so that there is a higher degree of confidence between the user and the data owner. A user's private key is used to decode data that has been encrypted.

3.2.2. Phase 2: Data Owner vs Cloud Users

Uploading files to the server accurately represents their data. Uploading data to the cloud is vital to system security. Owners may restrict access to encrypted sensitive files. The data owner provides the encryption secret key. The data owner picks the user's public key and describes the file. The file is transmitted to the user encrypted using SK. We may safeguard information using the secret key (SK) and public key (PK). Data owners encrypt using symmetric keys (AES) using the same key for both processes. Users' data is secured in the cloud, making cloud computing secure. To keep data private, data owners should encrypt it before uploading it to a cloud server.

3.2.3. Phase 3: Cloud vs Data Owner

Before uploading files to the cloud, OTP should authenticate data owner. The cloud service must also meet the data owner's changing demands, such as modifying access permissions or erasing data. Posing as the data's owner, it may upload the files to the cloud. It may download malware or malicious items to breach cloud

DOI: https://doi-ds.org/doilink/09.2023-66483628

security. It emphasizes data owner identification while uploading to prevent a fraudulent data owner from accessing the cloud server. We'll discuss data ownership and how OTP may assist later.

3.2.4. Phase 4: Cloud vs User

Users should utilize OPT to verify cloud files before downloading. The data owner encrypts cloud-stored files using a private key. Cloud storage gives each user a private key from the data owner. The file's secret key is needed to decode it. The private key is needed to decode data, thus users will require both. The user retrieves encrypted data from the cloud server (CS). Decrypting the file requires each user's private key and the file's secret key. This is significant since it's when the user begins using the cloud service. An authorized user can decrypt data using a secret key, but anybody with the key may attack it. Thus, we utilize secret and private keys to protect our data since individual users cannot decrypt it. This technique secures our model, allowing users to safely access information.

Cloud computing safety issues may be addressed using the proposed strategy. The system's trusted data access control is protected against imposters by this strategy, one of its greatest successes. This problem was previously intractable. We propose a secure and scalable cloud data sharing architecture.

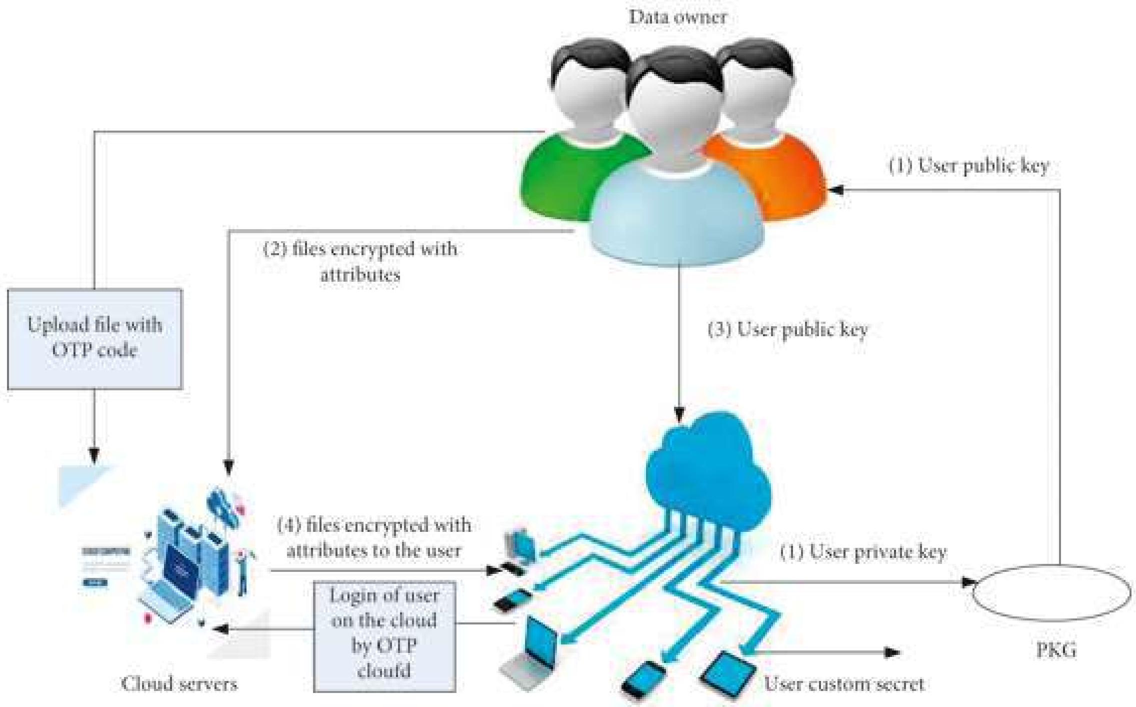
Data owner
(1) User public key
(2) files encrypted with attributes
Upload file with OTP code
(3) User public key
(4) files encrypted with attributes to the user
Login of user on the cloud by OTP cloufd
(1) User private key
Cloud servers
User custom secret
PKG

Figure 3: The proposed model.

DOI: https://doi-ds.org/doilink/09.2023-66483628

4. EXPERIMENTAL RESULTS

We implemented and made our idea accessible to cloud users to assure their safety at all times. This situation is possible with our NG-Cloud model simulation.

The Java-based discrete-event cloud simulation toolkit NG-Cloud provides application construction, resource identification, and interfaces for allocating application tasks to resources and controlling their execution. The NG-Cloud platform protects users and data the most. CAPTCHA login/registration employs numerous approaches. Signup and login are demonstrated in Figures 4(a) and 4(b). Users and data owners may create accounts in our system by providing their username, password, email address, phone number, and CAPTCHA. After registration, users and data owners may use the cloud; the cloud will offer an OTP code to type upon login.

The entered email and phone number will get an OTP code to verify system safety and validity. We incorporated the function Reset Password, which must be cleared to access cloud data, to safeguard the data in case a user or data owner loses or the data is in danger. After entering her email and CAPATCHA text to recover her account, the user may use her cloud storage space. The unlawful user will be let down even with the appropriate user ID and password. The attacker also requires the master key to decrypt cloud-stored encrypted data. Three people administer the system and provide high-quality cloud-based services in our manner. Our cloud-based data backup protects data from loss, theft, unintentional sharing, and other threats. Our application depends on keyword searches, thus we built a filter. The data owner grants authorization to each user to access the data at any time and from anywhere. The data owner may revoke access anytime.

NG-Cloud, our next-generation secure cloud storage technology, has 100 users. There are 90 authorized and 10 guest users. In our approach, unauthorized users cannot access the system, and d can identify them. Therefore, our system uses strong authentication to safeguard users from fraudulent attackers. We will upload files based on data owners for a smooth and customizable system. After 100 data owners, each may upload a file every 5 minutes, up from 30 seconds for two.

5. ANALYSIS OF THE PROPOSED MODEL

An good cloud data protection architecture should be robust to new threats. To help cloud computing progress as intended, we wish to give its benefits as seamlessly as feasible. A safer and more efficient cloud architecture can secure the owner's data against cloud dangers. In [25], we identified the following cloud computing security vulnerabilities that the proposed approach would mitigate:(1) PKG must be involved in identification and authentication for robustness. A fundamental issue in cloud computing is authentication [26]. Data owners should have a user ID for each user, therefore PKG gives them user public keys. PKG gives each system user a private key to decrypt encrypted data. PKG protects authenticated users from attacks even if a third party steals their ID and password since data decryption requires the owner's private key. PKG authenticates user-data owner interactions.User identities and permissions in the cloud are a common issue [27]. Our technique avoids authorization by letting data owners determine access permissions. The data owner may provide modify and delete rights to users using the tools. The data owner may revoke access anytime. Data owners offer access to those who need it. The cloud platform will not allow users without these credentials. To prevent permission

DOI: https://doi-ds.org/doilink/09.2023-66483628

issues, the data owner will manage the procedure.Thirdly, its design protects user data. Cloud data should only be accessible to authorized users to safeguard privacy. Thus, data privacy is controlled by the data owner, who permits access to approved users. The data owner alone may give or cancel access. When a user quits cloud access, the data owner imposes strict constraints so they can never use it again.We employ nonrepudiation to increase system safety. We protect upload and download procedures so no user may block others. A file is encrypted using a private key and stored in the cloud by the data owner, who then distributes it with the data user. The data owner gives each file access, which is recorded and not prohibited.Five) Integrity Data changes by unauthorized parties cause issues. We may handle data integrity by restricting access to authorized users with data owner rights. Only the authorized user may decrypt the encrypted data using the private key, preventing unauthorized alterations.Data encryption's main purpose is to make message deciphering harder than encryption [28]. The cloud gives the user a "User Secret Key" to decrypt data encrypted by the owner. The asymmetric RSA technique generates unique public and private key pairs for each user. Our method requires both the user secret key and the private key to decode a file. Without these two pieces of information, an attacker cannot access user data. Secure encryption protects sensitive data.(7) Confirming the storage provider: Businesses and individuals buy digital data storage space. The storage supplier's verification determines their reliability. Most individuals pick a service provider based on this alone. To solve the storage provider verification problem, the model requires customers to be honest, dependable, loyal, and have a conscience before choosing a service. If the supply is unreliable, we may not rent space to him.(8) Safe even if you forget your password or login info: our system protects your data if you forget your username or password. Users may utilize our "forget password" link to access the system if they forget their password or user ID.(9) Data indexing: cloud infrastructures are being pressured by the rapid expansion of data from numerous sources. Transmitted data is not adequately protected against transmission-related attacks [29]. Limiting the number of people that may access a data owner's cloud-stored data can reduce the amount of data transferred. Indexing makes database back-end applications easier to deploy on private and public clouds.(10) Keyword search: finding documents that match a user-specified keyword or set. Some academics tried to solve the problem by making it simpler for customers to find their publications. We invented search by adding parameters to queries. Table-based data may be rapidly searched using filtering methods. Each user may search the stored data for papers using the supplied keywords. We seek a simple data storage system for user-driven document searches.(11) Scalable data sharing: Cloud computing infrastructures allow users to share data, which offers several benefits. IT teams are being encouraged to share more information.(12) When re-encrypting the data, we must disseminate the new key to the final customers in the organization, which is computationally wasteful and burdens the data owner when the organization has hundreds of thousands of users. This approach cannot be utilized in the real world for critical data like that used in business, government, or medicine.Recently, cloud-based, scalable data-sharing has attracted attention (13). Scalable Data sharing will enable several people to access the same cloud data at once.Privacy is important since consumers' personal information is involved [30]. It protects users' personal data from illegal access. Data are encrypted and kept in the cloud by the owner. Data providers will provide users access to their supplied data. The data owner gives each file's user secret key to the user, who decodes it using their private key. Since each user can only access its own data, we implement privacy in the system.(15)Fake ID: cloud computing prioritizes security [11]. Authorized users may exchange passwords with non-authorized users. Customers and companies only like cloud computing provided their data is secured. This is difficult since

DOI: https://doi-ds.org/doilink/09.2023-66483628

a fake user's login would seem and feel normal to the system. Authenticating the user's identity will solve this difficult problem. Sending a one-time password to the real user's email and mobile phone simultaneously secures the false identity process against bots and other automated applications. The approved user receives an SMS and OTP to their private phone and email addresses to authenticate their identification.Balance security and usability. (16)Making the system more helpful increases the risk of exploitation. Proper setup balances system security and usability. Setting the right configuration balances safety and ease. Selecting Disable OTP upon login results in System Disable OTP (No OTP Secrecy). Entering Disable OTP during file upload results in System Disable OTP (No OTP Secrecy). Since compromising usability for security doesn't prevent the system from providing excellent user services, we will.

Cloud computing vulnerabilities are eliminated by our approach. If we can avoid these threats, any system will be safer. Data loss/leakage, account/service/traffic hijacking, insecure APIs, criminal Cloud computing use, and dangerous insiders may threaten any system. Defending the cloud against these attacks ensures cloud users' safety and security so they may enjoy its numerous benefits.

6. CONCLUSION

The delivery of IT services has been revolutionized by cloud computing. The suggested paradigm offered a workaround for a number of cloud computing's safety concerns. One of the major advancements of this paradigm is that it protects the legitimate user against impersonation. In addition, the suggested architecture safeguards the system against any fictitious data owner who inputs harmful material with the intent of undermining cloud computing's primary value proposition. The advantages and efficacy of cloud computing security were made available by our suggested paradigm. The suggested paradigm addresses the need for a middle ground between safety and convenience. The suggested methodology also ensured the safety and scalability of cloud-based data exchange between users. The next step is to apply the suggested model to existing medical records. Because of its significance and sensitivity, new approaches to countering assaults and threats may be developed. There is room for improvement in the speed and effectiveness of cloud computing. In order to construct a thorough policy-based management framework in cloud computing settings, it is necessary to present a secure service composition.

REFERENCES

[1] H. A. Jadad, A. Touzene, K. Day, N. Alziedi, and B. Arafeh, “Context-aware prediction model for offloading mobile application tasks to mobile cloud environments,” *International Journal of Cloud Applications and Computing*, vol. 9, no. 3, pp. 58–74, 2019.

[2] O. O. Olakanmi and A. Dada, “An efficient privacy-preserving approach for secure verifiable outsourced computing on untrusted platforms,” *International Journal of Cloud Applications and Computing*, 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 cloud computing an algorithmic approach for energy minimization in cloud data centers,” *International Journal of Cloud Applications and Computing*, vol. 9, no. 1, pp. 59–81, 2019.

DOI: https://doi-ds.org/doilink/09.2023-66483628

[4] K. Hossain, M. Rahman, and S. Roy, "IoT data compression and optimization techniques in cloud storage," *International Journal of Cloud Applications and Computing*, vol. 9, no. 2, pp. 43–59, 2019.

[5] R. P. Singh, A. Haleem, M. Javaid, and R. Kataria, "Cloud computing in solving problems of COVID-19 pandemic," *Journal of Industrial Integration and Management*, 2021.

[6] B. Demin, S. Parlati, P. F. Spinnato, and S. Stalio, "U-LITE, A private cloud approach for particle physics computing," *International Journal of Cloud Applications and Computing*, vol. 9, no. 1, pp. 1–15, 2019.

[7] P. M. ElKafrawy, A. M. Sauber, and A. M. Hafez, "HDFSX: big data distributed file system with small files support," in *Proceedings of the 2016 12th International Computer Engineering Conference (ICENCO)*, Cairo, Egypt, December 2016.

[8] S. O. Kuyoro, F. Ibikunle, and O. Awodele, "Cloud computing security issues and challenges," *International Journal of Computer Networks*, vol. 3, no. 5, pp. 247–255, 2011.

[9] P. M. El Kafrawy, A. M. Sauber, M. M. Hafez, and A. F. Shawish, "HDFSx: an enhanced model to handle small files in hadoop with a simulating toolkit," in *Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, April 2018.

[10] Mohammed Nadeem Shareef, Junaid Hussain, Mohammed Khaja Adnan Ali Khan,, Dr. Mohammed Abdul Bari ." Crypto Jacking", Mathematical Statistician and Engineering Applications, ISSN: 2094-0343, 2326-9865, Vol 72 No. 1 (2023), Page Number: 1581 – 1586

[11] Mohammed Fahad, Asma Akbar, Saniya Fathima, Dr. Mohammed Abdul Bari ," Windows Based AI-Voice Assistant System using GTTS", Mathematical Statistician and Engineering Applications, ISSN: 2094-0343, 2326-9865, Vol 72 No. 1 (2023), Page Number: 1572 - 1580

[12] Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022

[13] Hafsa Fatima, Shayesta Nazneen, Maryam Banu, Dr. Mohammed Abdul Bar," Tensorflow-Based Automatic Personality Recognition Used in Asynchronous Video Interviews", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022

[14] Mohammed Shoeb, Mohammed Akram Ali, Mohammed Shadeel, Dr. Mohammed Abdul Bari, "Self-Driving Car: Using Opencv2 and Machine Learning", The International journal of analytical and experimental modal analysis (IJAEMA), ISSN NO: 0886-9367, Volume XIV, Issue V, May/2022

[15] M. Mehrtak, S. SeyedAlinaghi, M. MohsseniPour et al., "Security challenges and solutions using healthcare cloud computing," *Journal of Medicine and Life*, vol. 14, no. 4, 2021.

[16] P. Chaudhary, B. B. Gupta, X. Changd, N. Nedjah, and K. TaiChui, "Enhancing big data security through integrating XSS scanner into fog nodes for smes gain," *Technological Forecasting and Social Change*, vol. 168, Article ID 120754, 2021.

[17] T.-S. Chou, "Security threats on cloud computing vulnerabilities," *International Journal of Computer Science and Information Technology*, vol. 5, no. 3, pp. 79–88, 2013.

DOI: https://doi-ds.org/doilink/09.2023-66483628

[18] X. Dong, J. Yu, Y. Luo, Y. Chen, Guangtaoxue, and M. Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," *Journal of Computer & Security*, vol. 42, no. I-14, pp. 321–334, 2013.

[19] S. K. Sood, "A combined approach to ensure data security in cloud computing," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1831–1838, 2012.

[20] C. Wang, Q. Wang, K. Ren, and W Lou, "Ensuring data storage security in cloud Computing in quality of service," in *Proceedings of the WQOS IEEE 17th international workshop*, vol. 1–9, Charleston, SC, USA, July 2009.

[21] Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46

[22] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021

[23] Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct

[24] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6

[25] S. Kumar, S. A. Abbas Jafri, N. A. Nigam, N. Gupta, G. Gupta, and S. K. Singh, "A new user identity based authentication, using security and distributed for cloud computing," in *Proceedings of the International Conference on Mechanical and Energy Technologies (ICMET 2019)*, vol. 748, Galgotias College of Engineering and Technology, Greater Noida, UP, India, November 2019.

[26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphert ext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, pp. 321–334, Oakland, California, USA, May 2007.

[27] Dr. M.A.Bari, "EffectiveIDS To Mitigate The Packet Dropping Nodes From Manet ", JACE, Vol -6,Issue -6,June 2019

[28] M.A.Bari & Shahanawaj Ahamad," Process of Reverse Engineering of Enterprise InformationSystem Architecture" in International Journal of Computer Science Issues (IJCSI), Vol 8, Issue 5, ISSN: 1694-0814, pp:359-365,Mahebourg ,Republic of Mauritius , September 2011

[29] M.A.Bari & Shahanawaj Ahamad, "Code Cloning: The Analysis, Detection and Removal", in International Journal of Computer Applications(IJCA),ISSN:0975-887, ISBN:978-93-80749-18-3,Vol:20,No:7,pp:34-38,NewYork,U.S.A.,April 2011

[30] Ijteba Sultana, Mohd Abdul Bari and Sanjay," Impact of Intermediate Bottleneck Nodes on the QoS Provision in Wireless Infrastructure less Networks", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021

DOI: https://doi-ds.org/doilink/09.2023-66483628

[31] A. Shamir, “Identity-based crypto systems and signature schemes,” in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47–53, Santa Barbara, CA, USA, August 1985.

[32] G. B. Tarekegn, G. Abadi Maru, and H. Zelalem Liyew, “Privacy and security issues IN cloud computing,” *International Journal Of Current Research*, vol. 8, no. 7, pp. 34894–34898, 2016.

[33] E. Alsolami, “Security threats and legal issues related to cloud based solutions,” *IJCSNS International Journal Of Computer Science And Network Security*, vol. 18, no. 5, 2018.

[34] S. Basu, A. Bardhan, K. Gupta et al., “Cloud computing security challenges & solutions-A survey,” in *Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, January 2018.

[35] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, “Security by design for big data frameworks over cloud computing,” *IEEE Transactions On Engineering Management*, vol. 99, 2021.

[36] P. M. El-Kafrawy, A. A. Abdo, and A. F. Shawish, “Security issues over some cloud models,” *Procedia Computer Science*, vol. 65, pp. 853–858, 2015.

[37] Y. Harrath and R. Bahlool, “Multi-objective genetic algorithm for tasks allocation in cloud computing,” *International Journal of Cloud Applications and Computing*, vol. 9, no. 3, pp. 37–57, 2019.

[38] C. Esposito, M. Ficco, and B. B. Gupta, “Blockchain-based authentication and authorization for smart city applications,” *Information Processing & Management*, vol. 58, no. 2, 2021.

DOI: https://doi-ds.org/doilink/09.2023-66483628