Secure File Storage in Cloud Using Hybrid Encryption

Kiran Kurian
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala
kirankurian18@gmail.com

Lekshmi S Nair
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala
lekshminair434@gmail.com

Dr. Joby P P
Professor
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala
jobypp@sjcetpalai.ac.in

Rinu Maria Jose
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala
rinu.mariajose@gmail.com

Rosa Mariam John
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology
Palai,Kottayam,Kerala
rosamariamjohn18@gmail.com

***Abstract*—In the present scenario, we come across millions and trillions of data in our daily lives which can be handled by a data centre. Cloud is the data centre that enables users to access files and applications from almost any device and geographical location. Computing and storage take place on servers in the data centre instead of the user device locally. It facilitates users with services like Software, Applications promptly without any hazard. Though the cloud has mesmerized the world with its advanced capabilities, safety is still involved in it because the cloud is shareable. All security components must ensure data security for every user. In this project, a new security model using Hybrid Cryptography is designed as data in the cloud is vulnerable to issues like unauthorized data access, integrity violation, identity management, etc. Due to the RSA Algorithm's benefits in terms of CPU usage, encryption time, and key size, we will be implementing it in our project for the secure transfer of data since the application is placed on the cloud. This project will investigate the deployment of applications on the cloud while enhancing security by using the RSA algorithm and the AES algorithm for encrypted file management.**

***Index Terms*—RSA, AES, Hybrid Cryptography**

I. INTRODUCTION

Cloud computing is a model for delivering IT resources over the internet on an as-needed basis. Instead of purchasing and maintaining physical hardware, organizations can access a range of technology services from a cloud provider, such as computing power, storage, and databases. These services are typically paid for on a pay-as-you-go basis, with organizations only paying for the resources they actually use. Cloud computing has many benefits, including cost savings, scalability, and flexibility. It allows organizations to access the resources they need without having to make large upfront investments in hardware and infrastructure. It also makes it easy to scale up or down as needed, without the need to purchase additional hardware. In addition, the cloud allows organizations to access a wide range of specialized services and tools, such as big data analytics and machine learning, that they might not have the expertise or resources to develop in-house. Overall, cloud computing is a powerful tool that is being used by organizations of all sizes and in many different industries to drive innovation and improve efficiency. Cloud computing is based on five key attributes: shared resources, scalability, pay-as-you-use pricing, elasticity, and self-provisioning of resources. These attributes allow organizations to access and use IT resources on an as-needed basis, without the need to purchase and maintain physical hardware. Many organizations are moving their applications to the cloud to take advantage of the speed of implementation and deployment, improved customer experience, scalability, and cost control. There are three main types of cloud computing services: Software as a Service (SaaS), Platform as a Service (PaaS),and Infrastructure as a Service (IaaS). PaaS and IaaS services exhibit five essential characteristics: rapid elasticity, resource pooling, on-demand self-service, broad network access, and measured service. Together, these characteristics allow organizations to access and use cloud resources in a flexible and scalable way, while only paying for the resources they actually use. Data is being transmitted between two clouds so in order to secure the data most of the systems use a combination of techniques,

including:
• Encryption- It is used to encode the data in such a way that a third party will not be able to hack that data.
• Authentication- It is used to create a separate user ID and Password so that only authorized users will able to access the data.
• Separation of duties- In which access is provided to all the users according to their priority.

Cloud computing has its roots in earlier distributed computing technologies. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, such as networks, storage, applications, and services. These resources can be quickly provisioned and released with minimal management effort or service provider interaction. One of the key benefits of cloud computing is that it allows organizations to access and use computing resources on an as-needed basis, without the need to purchase and maintain physical hardware. This can be more cost-effective and flexible than traditional IT models, which often require upfront investments in hardware and infrastructure. In addition, cloud computing allows organizations to scale up or down as needed, without the need to purchase additional hardware. Overall, cloud computing is a powerful tool that is being used by organizations of all sizes and in many different industries to drive innovation and improve efficiency. Data security is a major concern in cloud computing, as all data is transferred over the internet and is stored on servers that are managed by a third party. There are several key mechanisms that can be used to protect data in the cloud, including access control, auditing, authentication, and authorization. Access control refers to the process of restricting access to data and resources based on user privileges and permissions. This can be used to prevent unauthorized users from accessing sensitive data. Auditing involves tracking and recording user activity in the system, which can help to identify and prevent security breaches. Authentication is the process of verifying the identity of a user or device, and authorization is the process of granting or denying access to specific resources based on the user's privileges. To further protect data, it is important to store it in encrypted form. Encryption helps to protect data from being compromised, both when it is being transferred and when it is stored in the cloud. This can help to prevent unauthorized users from accessing the data and protect it from being compromised in case of a security breach.

II. OBJECTIVE AND SCOPE

The ultimate objective of the project is to develop low-power versions of the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms. The web application is deployed on the cloud, and the project aims to use the RSA algorithm for secure data transmission due to its advantages in terms of CPU utilization. The project aims to achieve high-throughput, real-time, reliable, and extremely secure cryptography algorithms for secure file storage on the cloud using hybrid cryptography. In conclusion, the basic objective of the project is to securely store and retrieve data on the cloud using hybrid cryptography, which combines both symmetric and asymmetric algorithms, in a way that allows only the owner of the data to control it. This can help to protect the data from unauthorized access and ensure that it remains secure even when it is stored on the cloud.

III. LITERATURE SURVEY

In the paper Secure File Storage on Cloud using Hybrid Cryptography Vivek Sharma et al [2021][1], Triple DES (3DES) is a symmetric-key block cypher, which applies the Data Encryption Standard (DES) cypher algorithm three times to each data block. 3DES provides a relatively simple and inexpensive way to increase the security of data compared to DES. Blowfish is another symmetric-key block cypher that uses a variable-length key, typically between 32 and 448 bits. It is fast and simple, making it a popular choice for use in certain applications. By using both 3DES and Blowfish in the proposed system, the authors aim to provide multiple layers of security for the data being stored in the cloud. By dividing the encryption process into three parts and using different algorithms and keys for each part, it is more difficult for an attacker to break the encryption and access the data.

Hybrid cryptography for cloud computing Heena Kausar Khan et al [2021] [2] In this paper, hybrid cryptography is a method of encrypting data that combines both symmetric and asymmetric algorithms. Symmetric-key encryption is a type of encryption where the same key is used for both encrypting and decrypting the data. This can be faster than asymmetric encryption, but it requires that the key be shared between the sender and the receiver. Asymmetric-key encryption, on the other hand, uses a pair of keys: a public key that is used to encrypt the data, and a private key that is used to decrypt it. This allows for secure communication without the need to share a secret key, but it can be slower than symmetric-key encryption. In the proposed system, the RSA algorithm is used for authentication, the Blowfish algorithm is used for confidentiality, and the Secure Hash Algorithm 2 (SHA-2) is used for data integrity. By using a combination of these different algorithms, the system aims to provide strong security for data in the cloud and protect against various threats such as unauthorized access, integrity violations, and identity management issues.

Secure File Storage using Hybrid Cryptography Putta Bharathi et al [2021] [4], hybrid cryptography is used in this project, combining multiple encryption techniques can increase the security of data stored in the cloud. In the proposed system, the data is divided into three sections and encrypted using three different algorithms: Advanced Encryption Standard (AES), Data Encryption Standard (DES), and the Rivest-ShamirAdleman (RSA) algorithm. AES is a widely-used symmetric-key encryption algorithm that is

considered to be very secure. DES is another symmetric-key algorithm that was widely used in the past, but it is now considered to be less secure than AES. RSA is an asymmetric-key algorithm that is often used for secure communication and data exchange. The keys used to encrypt the data are then hidden using steganography, a technique for hiding data within other data such as an image. This makes it more difficult for an attacker to obtain the keys and access the encrypted data. When a user wants to access the data, they must first recover the keys from the image and use them to decrypt the data using the appropriate algorithms. This multiple-layer approach to encryption and key management can provide strong security for the data stored in the cloud.

Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption Yusfrizal Yusfrizal1 et al [2018] [3], combining the Diffie-Hellman key exchange with the Advanced Encryption Standard (AES) algorithm can provide a secure method for exchanging and encrypting data. The Diffie-Hellman key exchange is a method for securely exchanging keys over an unsecured channel. It allows two parties to generate a shared secret key without either of them ever sending the key in plaintext over the communication channel. In the proposed application, the Diffie-Hellman key exchange is used to generate a shared secret key, which is then used to encrypt the data using the AES algorithm. The security of the system depends on the size of the keys used in the DiffieHellman key exchange. Larger keys provide stronger security, but they also require more

computational power and can be slower to use. According to the results you described, using a 1024-bit key in the Diffie-Hellman key exchange provides security equivalent to the 3DES 2-key algorithm, while using a 7680-bit key provides security equivalent to the AES-182 algorithm.

privateDH: An Enhanced Diffie-Hellman Key-Exchange Protocol using RSA and AES Algorithms Ripon Patgiri [2020] [5] This Literature search suggests that there is an issue of cryptanalysis attacks in symmetric-key cryptography and a shared secret key is required for such cryptography; for instance, AES cryptography. The most famous key exchange protocol is Diffie-Hellman; however, it has an issue with the number field sieve discrete log algorithm attacks. Moreover, recent research suggests that Diffie-Hellman is less secure than widely perceived. In addition, there is another issue of the Logjam attack that allows a man-in-middle attack in Diffie-Hellman. To address the above-raised issues, we combine RSA, AES, and Diffie-Hellman algorithms to mitigate the potential attacks on the key exchange protocol, called privateDH. Our key objective is to provide guaranteed security to the Diffie-Hellman Algorithm. Therefore, privateDH does not share the data publicly with the intended party. Instead, privateDH encrypts all shareable data using the AES algorithm at the time of key exchange protocol. privateDH uses the RSA algorithm and retrieves the public key to avoid a man-in-the-middle attack. Thus, we demonstrate how to provide security to the Diffie-Hellman algorithm to defeat various kinds of possible future attacks.Lack of authentication procedure. It's also worth noting that the DiffieHellman key exchange is just one of many key exchange protocols that can be used to establish a shared secret between two parties. Other popular key exchange protocols include the Elliptic Curve Diffie-Hellman (ECDH) key exchange, which is more efficient than the traditional Diffie-Hellman key exchange and is resistant to the number field sieve attack, and the RSA key exchange, which is based on the difficulty of factoring large composite numbers. The algorithm can be used only for symmetric key exchange.

A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With a Four-Layered Authentication Stack XIAOFENG ZHONG et al [2019] [6] the Secure Hybrid RSA (SHRSA) messaging scheme is a method for securely exchanging messages that combines the RSA algorithm with a four-layered authentication stack. RSA is an asymmetric-key algorithm that is commonly used for secure communication and data exchange. The Chinese Remainder Theorem (CRT) can be used to speed up the RSA algorithm by reducing the number of modular exponentiations that are required. According to the results you described, the SHRSA messaging scheme has similar encryption throughput to RSA and CRT-RSA, but it has faster decryption throughput. This makes it an efficient choice for certain applications. The authors of the study suggest that the SHRSA messaging scheme could be integrated into blockchain architectures, cyberphysical systems, and the Internet of Everything. However, it should be noted that the SHRSA scheme works over the Transmission Control Protocol (TCP), which means that the IP address of the sender and receiver are identified and the peer is disclosed. In addition, the text size for messaging is limited to between 1 and 255 bytes.

A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With a Four-Layered Authentication Stack XIAOFENG ZHONG et al [2019] [6] the Secure Hybrid RSA (SHRSA) messaging scheme is a method for securely exchanging messages that combines the RSA algorithm with a four-layered authentication stack. RSA is an asymmetric-key algorithm that is commonly used for secure communication and data exchange. The Chinese Remainder Theorem (CRT) can be used to speed up the RSA algorithm by reducing the number of modular exponentiations that are required. According to the results you described, the SHRSA messaging scheme has similar encryption throughput to RSA and CRT-RSA, but it has faster decryption throughput. This makes it an efficient choice for certain applications. The authors of the study suggest that the SHRSA messaging scheme could be integrated into blockchain architectures, cyberphysical systems, and the Internet of Everything. However, it should be noted that the SHRSA scheme works over the Transmission Control Protocol (TCP), which means

that the IP address of the sender and receiver are identified and the peer is disclosed. In addition, the text size for messaging is limited to between 1 and 255 bytes.

IV. PROPOSED SYSTEM

The application of many different cryptography techniques can provide a mechanism for the solution to more deficiencies that are happening in a secure cryptographic system which includes:

1. Key encryption management guarantees that all security objectives are met.
2. To develop a secure communication application that allows users to share information and data over the Internet.
3. Since people are transferring a lot of data, there should have been a cryptographic technique created that was examined, tested, and reliable.

In the proposed system, a secure method for storing files in the cloud using hybrid cryp- tography is suggested.

1. Initially, the user has to sign up and login into the web interface. The User can then upload the file which will be encrypted and stored directly in the private cloud.
2. If the user wishes to share the file, the file gets encrypted using the receiver's public key.
3. The receiver can decrypt the file using his private key.

The proposed system is using a combination of symmetric and asymmetric encryption to achieve both security and efficiency. The encryption process takes place within the application and the database stores the user's information, the key is obtained from the Key Distribution Centre. Using symmetric encryption, AES,for the actual data encryption and decryption allows for faster processing times since the same key is used for both encryption and decryption. However, key management can be a challenge with symmetric encryption as the key must be securely shared between the sender and receiver. On the other hand, asymmetric encryption, RSA can be used to securely exchange the symmetric key used for the actual data encryption and decryption. This allows for the benefits of both types of encryption to be utilized. The RSA key is used to encrypt the symmetric key, ensuring that it is only accessible to the intended recipient. This also provides data integrity, authentication, and non-repudiation, as the sender's identity can be verified using their public key. Overall, using the combination of both AES and RSA encryption provides both security and efficiency in the data transmission process.

The following are the steps in the proposed hybrid cryptography technique for secure file storage in Cloud:

Encryption:

1. Receive the file to be encrypted from the data owner.
2. Provide an AES key for data file encryption.
3. Data is encrypted using the AES key and stored in Cloud.
4. Provide the RSA public key of the data user to the data owner.
5. Encrypt the AES key using RSA public key of the data user.

Decryption:

1. Verify the RSA public key of the data user.
2. Fetch the file to be decrypted from the Cloud.
3. Decrypt the AES key using the RSA private key of the data user.
4. Decrypt data using the AES key.
5. Provide view access to the decrypted file for the data user within the application.

V. TECHNOLOGIES USED

A. ReactJS

The React.js framework is an open source JavaScript framework and library developed by Facebook. It is used to quickly and efficiently build interactive user interfaces and web applications with far less code than regular JavaScript.

React develops applications by creating reusable components that can be thought of as individual lego bricks. These components are the individual parts of the final user interface, which together form the overall user interface of the application. React allows developers to build large-scale web applications that can change data without reloading the page. The main goals of React are to be fast, scalable and simple. Works only in the application's user interface. This corresponds to the view in the MVC template. It can be used in conjunction with other JavaScript libraries or frameworks like Angular JS for MVC.

B. MongoDB

MongoDB is a source-enabled, cross-platform, document-centric database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents and optional schemas.

A record in MongoDB is a document, a data structure consisting of field-value pairs. A MongoDB document resembles a JSON object. Field values can contain other documents, arrays, and arrays of documents. Many computer languages provide native data types that correlate with documents (that is, objects). Using embedded documents and arrays alleviates the need for expensive joins. Flow polymorphism supported via dynamic schemes.

C. AWS S3

Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can store and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps. With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements.

D. FastAPI

FastAPI is a Web framework for developing RESTful APIs in Python. FastAPI is based on Pydantic and type hints to validate, serialize, and deserialize data, and automatically auto-generate OpenAPI documents.

It fully supports asynchronous programming and can run with Gunicorn and ASGI servers for production such as Uvicorn and Hypercorn. To improve developer-friendliness, editor support was considered since the earliest days of the project.

CONCLUSION

Given India's current low straightforwardness of charity , data security, trust issues among people, and issues related to the bogus foundation are problem areas that need to be addressed immediately. This paper provided a new approach to leveraging blockchain innovations to revolutionize this framework of this fundraising. The resolutions we proposed were put into action to create to create an end-to-end empowerment and platform for decentralized foundation. All transactions are recorded on the blockchain, enabling traceability of funds and increasing transparency for charities. The lack of transparency in philanthropy can be technically resolved with this blockchain fundraising system, which can increase public trust in charities. A complete fundraising system based on the blockchain is the future.

REFERENCES

[1] V. Sharma, A. Chauhan, H. Saxena, S. Mishra and S. Bansal, "Secure File Storage on Cloud using Hybrid Cryptography," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.9702323.

[2] H. K. Khan, R. Pradhan and B. R. Chandavarkar, "Hybrid Cryptography for Cloud Computing," 2021 2nd International Conference for Emerging Technology (INCET), 2021, pp. 1-5, doi: 10.1109/INCET51464.2021.9456210.

[3] Y. Yusfrizal, A. Meizar, H. Kurniawan and F. Agustin, "Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption," 2018 6th International Conference on Cyber and IT Service Management (CITSM), 2018, pp. 1-6, doi: 10.1109/CITSM.2018.8674278.

[4] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 1635-1638, doi: 10.1109/WiSPNET.2016.7566416.

[5] Patgiri, Ripon. (2021). privateDH: An Enhanced Diffie-Hellman Key-Exchange Protocol using RSA and AES Algorithm. 10.13140/RG.2.2.23938.40647.

[6] Bhattacharjya, Aniruddha Zhong, Xiaofeng Li, Xing. (2019). A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With Four-Layered Authentication Stack. IEEE Access. 7. 30487 - 30506. 10.1109/ACCESS.2019.2900300.

[7] I. Mustafa et al., "A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications," in IEEE Access, vol. 8, pp.99273-99285, 2020, doi: 10.1109/ACCESS.2020.2995801.

[8] Lee, Sangyub Cho, Sung Kim, Heeseok Hong, Seokhie. (2019). A Practical Collision-Based PowerAnalysis on RSA Prime Generation and Its Countermeasure. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2909113.

[9] Imam, Raza Areeb, Mohammad Alturki, Abdulrahman Anwer, Faisal. (2021). Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3129224.

[10] S. An and S. C. Seo, "Designing a New XTS-AES Parallel Optimization Implementation Technique for Fast File Encryption," in IEEE Access, vol. 10, pp. 25349-25357, 2022, doi: 10.1109/ACCESS.2022.3155810.

[11] E. Ochoa-Jiménez, L. Rivera-Zamarripa, N. Cruz-Cortés and F. Rodríguez-Henríquez, "Implementation of RSA Signatures on GPU and CPU Architectures," in IEEE Access, vol. 8, pp. 9928-9941, 2020, doi: 10.1109/ACCESS.2019.2963826.

[12] C. -H. Hsia, S. -J. Lou, H. -H. Chang and D. Xuan, "Novel Hybrid Public/Private Key Cryptography Based on Perfect Gaussian Integer Sequences," in IEEE Access, vol. 9, pp. 145045-145059, 2021, doi: 10.1109/ACCESS.2021.3121252.

[13] Yong PENG, Wei ZHAO, Feng XIE, Zhong-hua DAI, Yang GAO, Dong-qing CHEN, Secure cloud storage based on cryptographic techniques, The Journal of China Universities of Posts and Telecommunications, Volume 19, Supplement 2, 2012.

[14] W. N. A. Ruzai, M. R. K. Ariffin, M. A. Asbullah, Z. Mahad and A. Nawawi, "On the Improvement Attack Upon Some Variants of RSA Cryptosystem via the Continued Fractions Method," in IEEE Access, vol. 8, pp. 80997-81006, 2020, doi: 10.1109/ACCESS.2020.2991048.

[15] B. Langenberg, H. Pham and R. Steinwandt, "Reducing the Cost of Implementing the Advanced Encryption Standard as a Quantum Circuit," in IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-12, 2020, Art no. 2500112, doi: 10.1109/TQE.2020.2965697.

[16] A. Nitaj, M. R. B. Kamel Ariffin, N. N. H. Adenan, T. S. C. Lau and J. Chen, "Security Issues of Novel RSA Variant," in IEEE Access, vol. 10, pp. 53788-53796, 2022, doi: 10.1109/ACCESS.2022.3175519.