JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Role and TPA Based Concept of Cloud Data Access Using Blockchain Technology

Ramjanam Kumar[1], Miss Anamika[2]

[1]M.Tech Scholar, [2]Assistant Professor

[1,2]Department of Computer Science and Engineering, K. K. University Nalanda (Bihar)

Abstract : Shifting some data to the cloud enables users to access it from anywhere. There are, however, two main issues with this- ensuring that only the correct user has access to the data, and ensuring the security of such data in the cloud. It is important for companies to digitize their work, and as COVID-19 has shown, it is important to be able to upload data quickly in times of crisis.

With the security challenges of cloud computing data, we proposed a new Role Base Access and TPA model to keep data safe. In the block chain, we will be using two concepts. One is based on profiles and the other is based on the grid of images. In addition to the shared ledger, there is a TPA which specifies how documents are accessed and exchanged. The result then tested on various platforms to evaluate the performance.

Index Terms **– Cloud Security, TPA, Blockchain.**

I. INTRODUCTION

Cloud computing is a new resource that provides big businesses higher bandwidth and data storage at a competitive price.With these Cloud Computing features, you can focus on what matters without needing to worry about the technologies that are being used. A network provided by a cloud computing provider will help you focus on your work, instead of focusing on technical things like the infrastructure.[1]

Cloud services are on-demand and require less data than before. Cloud computing is a $42 billion industry that has been growing 27% per year. This is an opportunity for associations, as they provide ICT services that contribute to this $42 billion industry and contribute 2% to CO2 emissions, which is comparable to the contribution of the flight business.[1]

Cloud computing reduces the amount of power required to run HPC and Web applications. This saves both companies and customers money, but creates an issue with storing all these valuable data, which consumes more energy. [2] To prevent severe temperature increases, a 15-30% reduction in energy is necessary. Cloud computing will help, but research on CIOs concerns around efficiency needs to be done as well.[2]

Cloud computing is a growing prospect, it involves re-evaluating all computing needs, such as storage, computing, and software, such as office and ERP, through one vast Internet. [3]

The advantage of the cloud has three indisputable characteristics that distinguish it from standard work. It is sold on demand, typically as you go or by the hour; it is adaptable - customers may need as much or as little of an organization as they need at a random time; and the organization is fully monitored by the service provider (customers only need a PC and Internet access). [3]

Huge advances in virtualization and circular computing, coupled with improved fast internet access and economics, have fueled the energy for cloud computing. [3]

Cloud computing reevaluates IT needs, like storing and computing, as well as office software. A cloud advantage is a service sold on demand. It can be large or small and flexible because it's supervised by the customer, meaning they only need a PC and internet access. Cloud advantages are sold on demand, adaptable and can be configured to the needs of the customer. [4]

The cloud computing industry has boomed due to advancements in IT and computer science, such as the increased efficiency of cloud computing. [4]

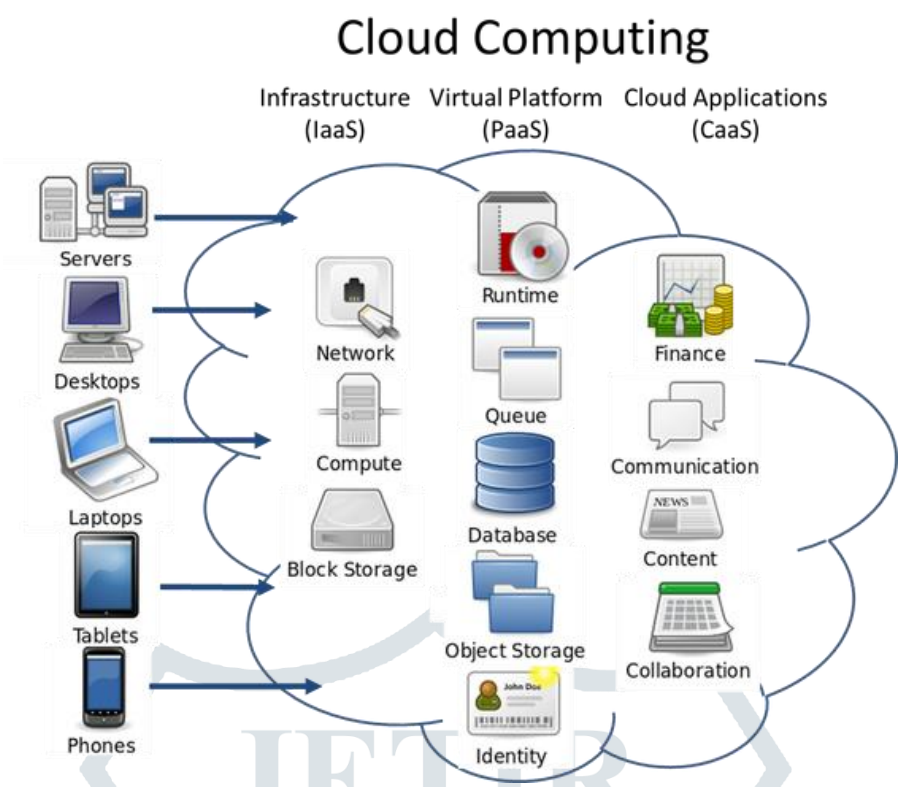

Fig 1. Cloud Computing

RBAC provides a strategy for restricting network access so the roles of individual purchasers are restricted within an enterprise. A role in the enterprise finalizes that individual has the appropriate rights to do their responsibilities and restricts them from accessing information which does not pertain to them. In the access management information model in the manner based on role, roles are supported some variables, together with approval, obligation and employment ability. Consequently, organizations assign no matter if a shopper is a finish customer or an authority shopper and regulate who has access to laptop assets. With role-based access management, a person's access to information is determined by their role in the company. This helps to limit privileged data and only allow certain pieces of information that are needed for each person's job. [5] Lower-level employees may not go near sensitive information with the off chance they don't have to. This helps if you have third-party employees and contract employees who are hard to monitor. Using RBAC can help you ensure your organization's touchy information, as well as its important applications.[5]

Confirming is a procedure for approving the client's login. Verification systems are used to confirm their identity. There are three levels of confirmation that can be used, approval, recognition, and something physical. Approval recognizes who the user is by inputting a username and password through approval recognition and then approval is given when the card is swiped or inserted into a machine. In verification process, security frameworks will be able to give access with biometrics and recognize one thing in that time transaction by inputting data about skin microbes, irises, vein structures along with keys on phones and cards.[6] Blockchain technology creates blocks, which hold information on one another, with cryptography making them secure. The technology allows transactions to be accurate and efficient, as well as transparent. Blockchain helps reduce the costs of complying with demands and is useful in transferring large volume data. Blockchain can verify transactions and track them from source to destination.[6]

II. LITERATURE REVIEW

In this paper, A, Bouchahda, et.al 2010 propose a new system called (RBAC+). This system aims to control who can access or use data on the web. RBAC+ expands on the traditional Role-Based Access Control model and includes ideas like usage, profiling and sub-application of meeting.[7]

"Sanjay Kumar et al. (2020) [8] " introduced a method of authentication that uses two-factor authentication, data encryption with AES, and the misplacing and uploading of data to a cloud.

"F. Z. Glory et al.,2019 [9]" suggests that authentication can be done with a password generated by any algorithm in combination with input from their favorite name, the number of grandmother's children, and secret dates etc.

"Shah Zaman Nizamani et.al 2017 [10]" In the proposed text-based client confirmation scheme, the client alters their input strategy to a printed secret phrase that guarantees their personal information..

III. PROPOSED CONCEPT

3.1 Section 1: Cloud User Validation

Utilizing the concept of the block chain for the security purpose, we will be going to create block chain in two respects, as going for the role base so for the authentication of the user we will create the block chain and also the pattern which is formed using the grid of personalities photos. The user has to select and arrange the photos of the celebrities in the grid and on the basis of the position of the photos in the grid , a pattern is generated which will act as the user authentication key and with the combination of the user name , email id and authentication key, a user identification blockchain is generated.

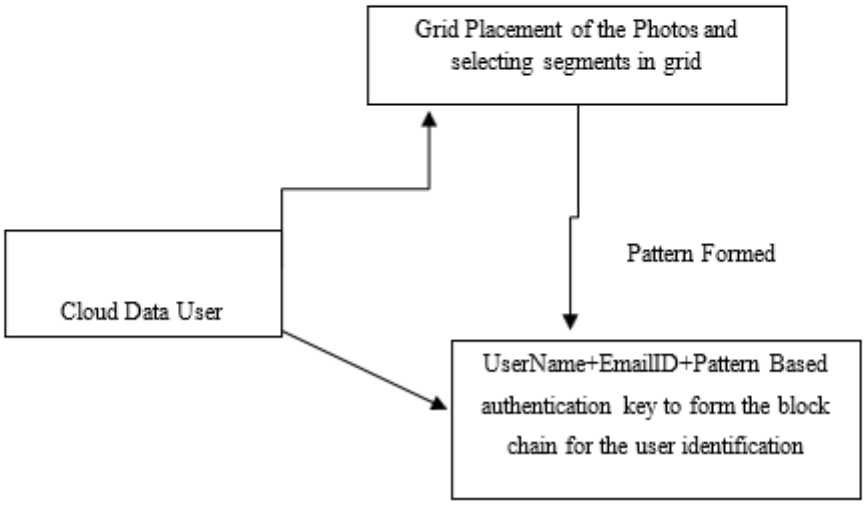

Fig 2. Blockchain formation

3.2 Section 2: Cloud Based Data Access

Secondly for the data sharing or access, TPA will come into role for generation of another block chain related to document, role who can access the document, Pattern of OTP generated for document access, and details for data exchange.

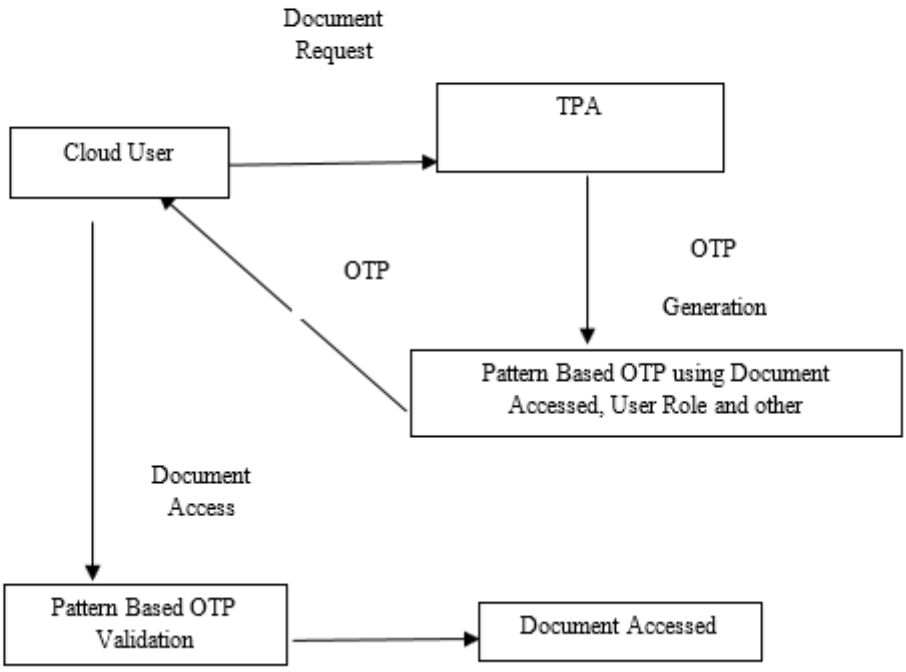

Fig 3. Verification Process

IV. IMPLEMENTATION AND RESULT ANALYSIS

The simulation process is done using the .Net and database as SQL Server Express 2008.

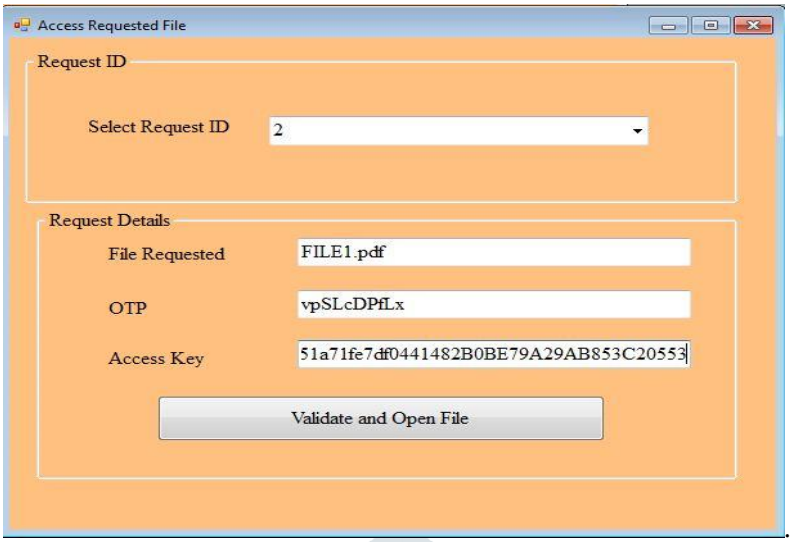

Fig 4. File Access Form

Result Analysis: Rumkin Tool

Base Paper, Sankaj Kumar, et.al 2020 makes use of access key as based on AES 10 round key e.g., 28FDDEF86DA4244ACCC0A4FE3B316F26

Table 1 Analysis of Keys Test 1

	Authentication Key	Access Key
Proposed Approach	445.1	168.8

Table 2 Analysis of Keys Test 1 Base Key

	Access Key
Base Paper	127 bits

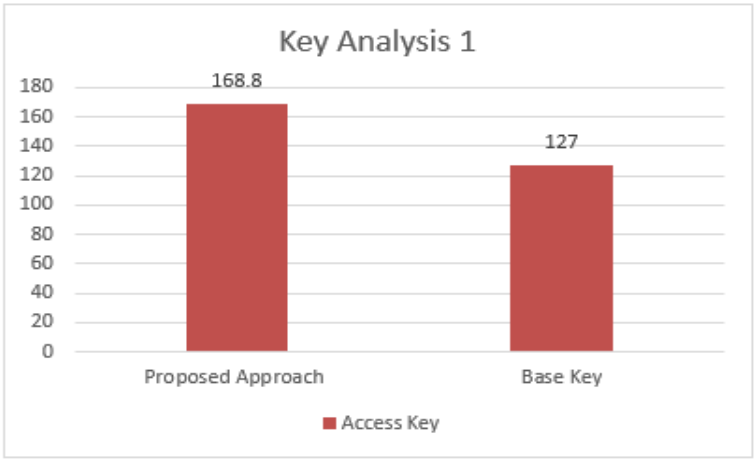

Fig 5. Key and Blockchain Analysis Test 1

Result Analysis : zxcvbnTest

Table 3. Analysis of Keys Test 2

	Authentication Key	Access Key
Proposed Approach	319	131

Table 4. Analysis of Keys Test 2 Base Key

	Access Key
Base Paper	104

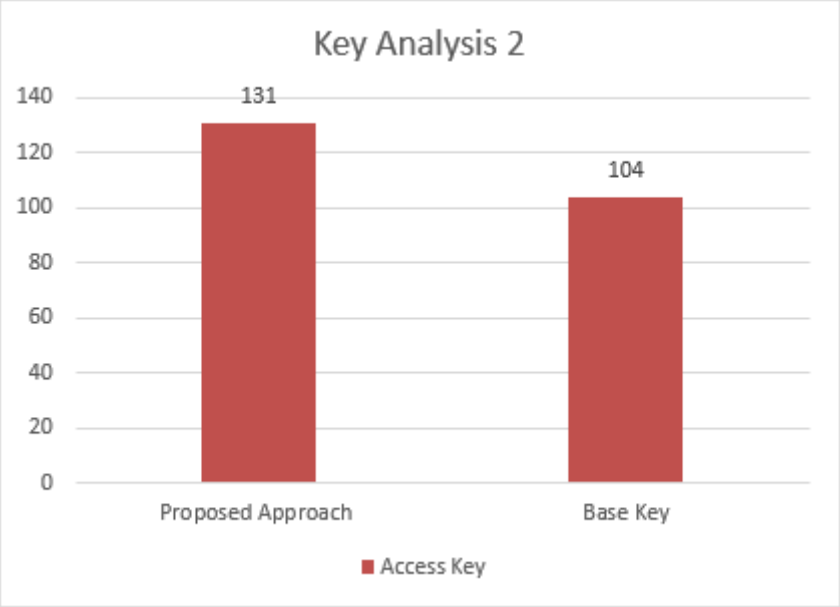

Fig 6. Key and Blockchain Analysis Test 2

V. Conclusion

Shifting some data to the cloud enables users to access it from anywhere. There are, however, two main issues with this- ensuring that only the correct user has access to the data, and ensuring the security of such data in the cloud. It is important for companies to digitize their work, and as COVID-19 has shown, it is important to be able to upload data quickly in times of crisis.

With the security challenges of cloud computing data, we proposed a new Role Base Access and TPA model to keep data safe. In the block chain, we will be using two concepts. One is based on profiles and the other is based on the grid of images. In addition to the shared ledger, there is a TPA which specifies how documents are accessed and exchanged. The result then tested on various platforms to evaluate the performance.

References

1. G. F. Nadlamani and S. Shaikh, "Preserving privacy using TPA for cloud storage based on regenerating code," *2016 International Conference on Recent Trends in Information Technology (ICRTIT)*, Chennai, India, 2016, pp. 1-5.
2. N. Shimbre and P. Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm," *2015 International Conference on Computing Communication Control and Automation*, Pune, India, 2015, pp. 35-39.
3. R. K. Saripalle, A. De La Rosa Algarin and T. B. Ziminski, "Towards knowledge level privacy and security using RDF/RDFS and RBAC," *Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015)*, Anaheim, CA, USA, 2015, pp. 264-267.
4. S. Muthurajkumar, M. Vijayalakshmi and A. Kannan, "Intelligent temporal role based access control for data storage in cloud database," *2014 Sixth International Conference on Advanced Computing (ICoAC)*, Chennai, India, 2014, pp. 184-188.

5. B. Schmidt-Wesche, T. Bleizeffer, J. Calcaterra, D. Nair, R. Rendahl and P. Sohn, "Cloud User Roles: Establishing Standards for Describing Core Tasks of Cloud Creators, Providers, and Consumers," *2011 IEEE 4th International Conference on Cloud Computing*, Washington, DC, USA, 2011, pp. 764-765.
6. Wenhui Wang, Jing Han, Meina Song and Xiaohui Wang, "The design of a trust and role based access control model in cloud computing," *2011 6th International Conference on Pervasive Computing and Applications*, Port Elizabeth, South Africa, 2011, pp. 330-334.
7. A. Bouchahda, N. L. Thanh, A. Bouhoula and F. Labbene, "RBAC+: Dynamic Access Control for RBAC-Administered Web-Based Databases," *2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, Venice, Italy, 2010, pp. 135-140.
8. Sanjay Kumar, Syed Akbar Abbas Jafri, NishitArun Nigam, Nakshatra Gupta, Gagan Gupta1 and S K Singh,"A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing",IOP Conf. Ser.: Mater. Sci. Eng. ,2020
9. F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based On User Inputs," *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2019.
10. Shah Zaman Nizamani, Syed Raheel Hassan, Tariq Jamil Khanzada and Mohd Zalisham Jali, “A Text based Authentication Scheme for Improving Security of Textual Passwords” International Journal of Advanced Computer Science and Applications(ijacsa), 8(7), 2017