



ACCESS CONTROL WITH EFFICIENT REVOCATION FOR MULTI-AUTHORITY CLOUD STORAGE SYSTEM USING 2PVC

¹R.Dinesh Raj, ²V.Abinaya, ³C.Anitha, ⁴R.Parkavi, ⁵G.Thilagavathi

¹ Assistant Professor, ^{2,3,4,5} Students
Computer Science and Engineering,

Sri Ramakrishna College of Engineering, Perambalur, India.

Abstract: An important application of the Internet-of Things & cloud computing, many remote monitoring systems adopt a device-to-cloud network paradigm.. Software-Based Solutions that adopt advanced cryptographic tools, such as Attribute-Based Encryption and fully homomorphic encryption.IOT, many remote monitoring systems adopt a device-to-cloud network paradigm. In a remote patient monitoring case, various resource-constrained devices are used to measure the health conditions of a target patient in a distant non-clinical environment and the collected data are sent to the cloud backend an authorized health care service for processing and decision-making.Software-Based Solutions that adopt advanced cryptographic tools, such as Attribute-Based Encryption and fully homomorphic encryption, can address the problem, but they also computation overhead on both client and server sides. In this Project work front end ASP.NET and SQLSERVER software-based solutions and propose a secure and efficient remote monitoring framework, called 2PVC techniques such .NET Technology . In addition a robust and lightweight “heartdata” protocol to handle notoriously difficult key revocation problem. An implemented a prototype of the framework for ASP.NET and SQLSERVER can protect user data privacy against unauthorized parties, with minimum performance cost compared to existing software-based solutions.

IndexTerms – Two Phase Verification Commit,Cipher text Attribute based encryption,Object Revocation Based Access Control.

1 INTRODUCTION

1.1CLOUD COMPUTING

Cloud Computing is an emerging knowledge and its popularity is increasing drastically day-by-day. Although the advantages are understandable taking up users ‘physical control’ of their outsourced information, which unavoidably creates new security threats towards the accuracy of the information in cloud. To start working on data access control, initially a study is necessary to find out effectiveness of cryptographic algorithms so that data operations on mobile could be fast and consistent. Making use of mobile tools, computing ability from cloud computing technology and Internet convenience jointly is making a new surge, which is mobile cloud computing for organization.

1.2 CLOUD COMPUTING APPLICATION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand structure access to a common pool of configurable computing resources (e.g., networks, servers, storage, applications, and

services) that can be speed provisioned and unconfined with minimal management effort or service provider interaction. Key supervision is another vast area of research and still studies are going on to make key management more secured and resourceful. Let us in brief have a discussion regarding the security problems that take place with key management on mobile devices with outsourcing information on cloud server. Common security problems in key management are

- Effectiveness in mobile operations
- Strong protection of cryptographic algorithms
- Keys being fetch
- Keys being susceptible to hack or cooperation
- Supervision of all keys

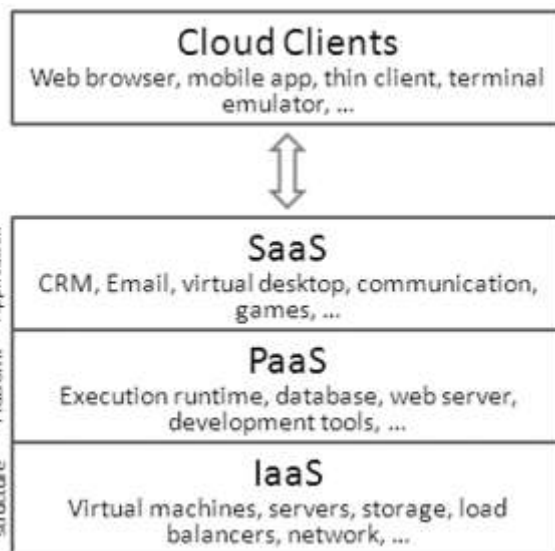


Fig 1.1.1 Cloud Service Provider Infrastructures

2 MODULES

- Cloud User Registration
- Cloud Member Login
- Data Owner Registered With Authorization Policies
- Upload File
- Threshold Cryptosystems
- Symmetric Key Cryptosystem
- Cloud Formation
- Safe Transaction

2.1 MODULES DESCRIPTION

2.1.1 CLOUD USER REGISTRATION

For the registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase.

2.1.2 CLOUD MEMBER LOGIN

This module is the first module. From this page only the user can navigate to project. Only the Authorized person can enter giving by valid information. If the user provides the invalid information then permission navigating to other pages. This authentication module concentrates the security of the project from the unauthorized users. User can authenticate only if the cloud authority provides permission else the access is denied to the user.

2.1.3 DATA OWNER REGISTERED WITH AUTHORIZATION POLICIES:

Next Data Owner Registered with authorization policies, valid date from and valid date to in desirable Trusted Third Party or CA. Because this Secret Keys are used to Authentication Purpose. A Data Owner wants to upload his file and end user wants to download a file, both are used this secret key for encryption and decryption.

2.1.4. UPLOAD FILE

Data Owner wants to upload a file. So he encrypted this file using TA's secret Key, First he sends a key request to Trusted Third Party. Then the data owner encrypts his file using this secret key.

2.1.5 THRESHOLD CRYPTOSYSTEMS

Threshold cryptosystems offer to ability to share the power of performing certain cryptographic operations (e.g. generating a signature, decrypting a message, computing a shared secret) among n authorized users, such that any t of them can do it efficiently.

2.1.6 SYMMETRIC KEY CRYPTOSYSTEM

Symmetric encryption also referred to as conventional encryption or single key encryption was the only type of encryption in use prior to the development of public-key encryption.

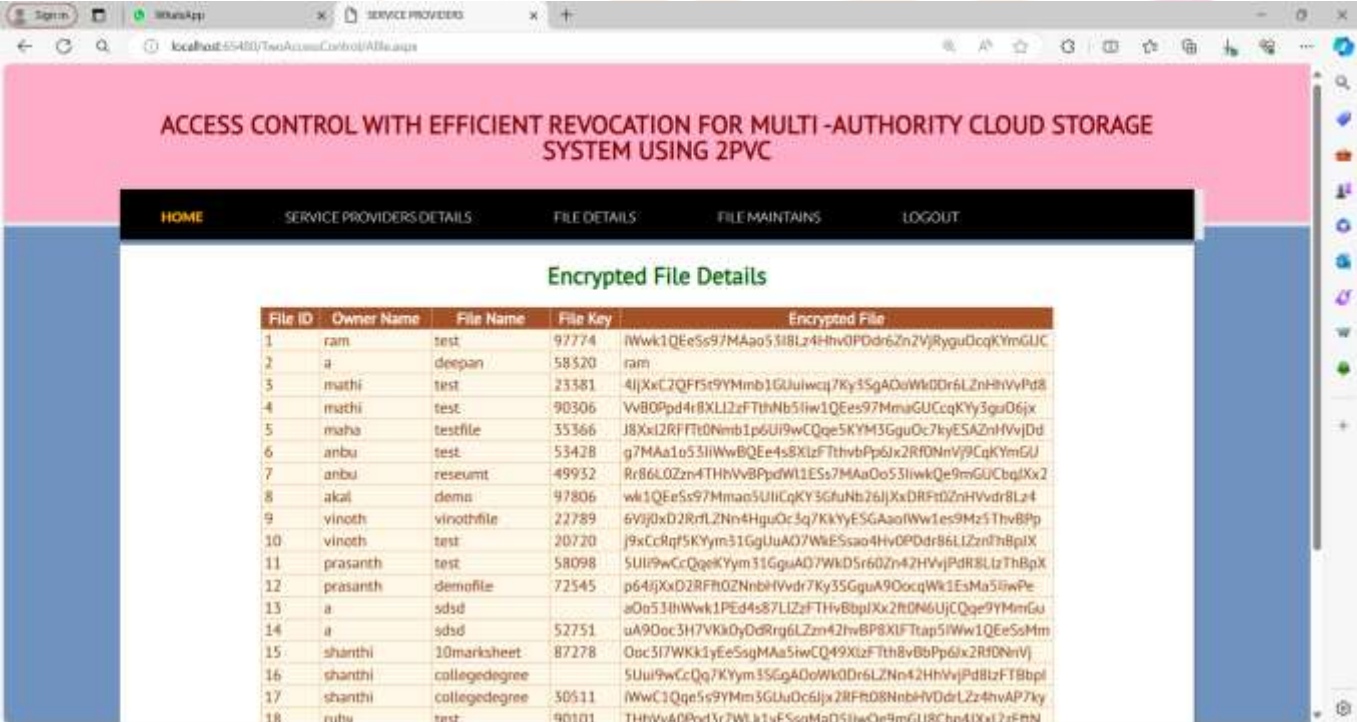
2.1.7 CLOUD FORMATION

First create a cloud infrastructure. It consisting of a set of servers, where each server is responsible for hosting a subset of all data items belonging to a specific application domain. A transaction is submitted to a Transaction Manager (TM) that coordinates its execution. Here each CA offers an online method that allows any server to check the current status of credentials.

2.1.8 SAFE TRANSACTION

A safe transaction is a transaction that is both trusted (i.e., satisfies the correctness properties of proofs of authorization) and database correct (i.e., satisfies the data integrity constraints). It first describes an algorithm that enforces trusted transactions (2PV), and then expands this algorithm to enforce safe transactions (2PVC). In response to this message, each participant 1) evaluates the proofs for each query of the transaction using the latest policies it has available and 2) sends a reply back to the TM containing the truth value (TRUE/FALSE) of those proofs along with the version number and policy identifier for each policy used.

Encrypted File



The screenshot shows a web browser window displaying a web application. The page title is "ACCESS CONTROL WITH EFFICIENT REVOCATION FOR MULTI-AUTHORITY CLOUD STORAGE SYSTEM USING 2PVC". The navigation menu includes "HOME", "SERVICE PROVIDERS DETAILS", "FILE DETAILS", "FILE MAINTAINS", and "LOGOUT". The main content area is titled "Encrypted File Details" and contains a table with the following data:

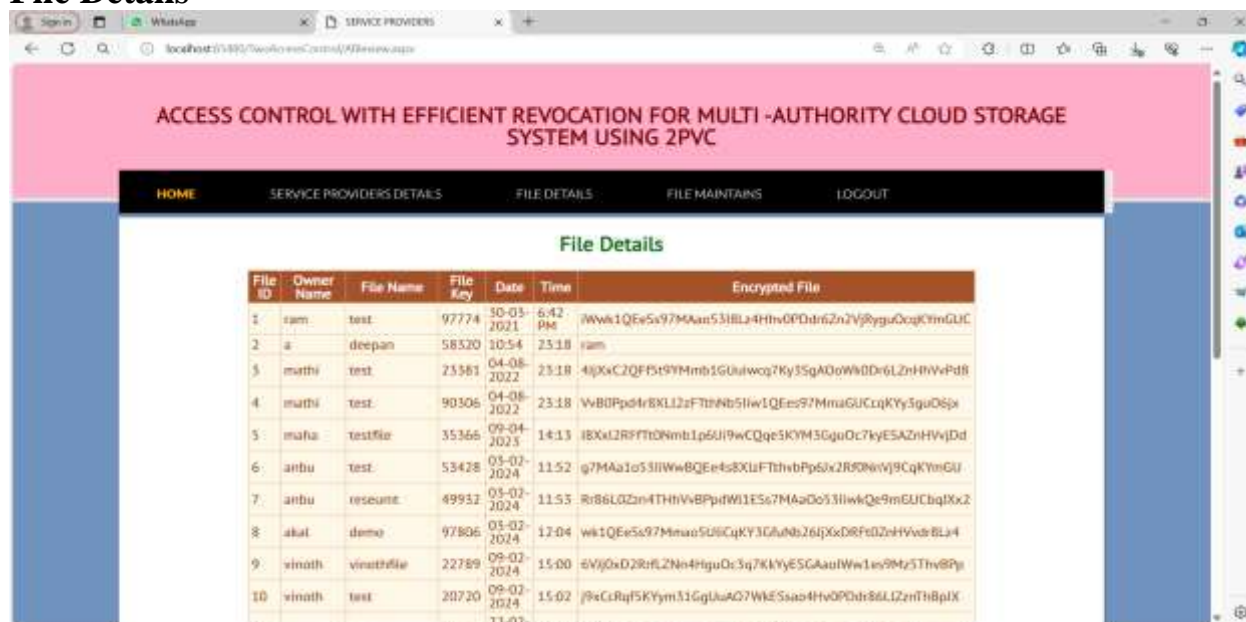
File ID	Owner Name	File Name	File Key	Encrypted File
1	ram	test	97774	IWwklQEe5s97MAao53iBLz4Hhv0PDdr6Zn2VjRyguDcqKYmGUC
2	a	deepan	58520	ram
3	mathi	test	23381	4lJXxC2QF5t9YMmb1GUulwCj7Ky3SgAOuWkDDr6LZnHhVvPd8
4	mathi	test	90306	VvB0Ppd4r8XLl2zFtHnB5liw1QEe597MmaGUcCqKYy3guD6jx
5	maha	testfile	35366	J8Xxl2RFft0Nmb1p6UI9wCQe5KYM3GguOc7kyESAznHvVjDd
6	anbu	test	53428	g7MAa1o53liWwBQEe4s8XlzfTthvBp6jx2Rf0NnVj9CqKYmGU
7	anbu	reseumt	49932	Rr86LOZzn4THhVvBpPdWl1ESs7MAaOo53liwKQe9mGUcbqJkx2
8	akali	demo	97806	wk1QEe5s97Mmao5UliCqKY36fuNb26lJXxDRFt0ZnHvvdRlZ4
9	vinoth	vinothfile	22789	6Vvj0xD2RrL2Nn4HguOcsq7KkYyESGAoIWw1es9Mz5ThvBpP
10	vinoth	test	20720	J9xCclqf5KYym31GguAD7WkESsao4HvOPdr86LlZzn7h8pIX
11	prasanth	test	58098	SUII9wCcQqeKYym31GguAD7WkD5r60Zn42HvVjPdR8LlZThBpX
12	prasanth	demofile	72545	p64jXxD2RFR0ZnNbhVvdR7Ky3SGguA9OocqWk1EsMa59wPe
13	a	sdsd		aOo53liHwWk1PEd4s87LlZzFtHvBbplXx2Rf0N6UjCQqe9YmMGu
14	a	sdsd	52751	uA9Ooc5H7Vkk0yDdRrg6LZzn42hvBP8XlFtup5iWw1QEe5sMm
15	shanthi	10marksheet	87278	Ooc3i7Wkk1yEeSsgMAa5iwCQ49XlzfTth8vBbPp6jx2Rf0NnVj
16	shanthi	collegedegree		SUII9wCcQq7KYym3SGgAOwWkDre6LZn42HhVvPd8zFTBbpl
17	shanthi	collegedegree	30511	IWwC1Qqe5s9YmM3GUUoc6jx2RFR08NbhHVDdrLz24hvAP7ky
18	ruby	test	90101	THhVvADPod3r7Wlkl1vE5sMaO5liwQe9mGU8Cbo4IXxl2zFBN

Fig2.1.8 Encrypted file

2.1.9 DOWNLOAD FILE

An end User wants to access this upload file, he give the download request to particular DB's Server. The particular Server match this request to its database then retrieve

File Details



File ID	Owner Name	File Name	File Key	Date	Time	Encrypted File
1	ram	test	97774	30-03-2021	6:42 PM	/Ww1QEeSv97MAan53iBLz4HtV0P0dn6Zn2VjRygu0CqKtmGUC
2	a	deepan	58520	10-04-2022	23:18	ram
3	mathi	test	23581	04-08-2022	23:18	4lJXc2QFFSt9YMmb1GUulwoq7Ky3SgAOoWw0D6LznHwVpDf
4	mathi	test	90306	04-08-2022	23:18	/WB0Ppd4r8XL1z2F7hNnb5liw1QEe97MnaGUCqKy3gu06jx
5	maha	testfile	35366	09-04-2023	14:13	/BXx12RFFt0Nmb1p6U19wCQqe5KYM3Gju0c7kyESAznHWJdd
6	anbu	test	53428	05-02-2024	11:52	q7MAa1o53iIwWbQEe4s8XUzFThv0Pp6X2R90NvVj9CqKymGU
7	anbu	reseunt	49932	05-02-2024	11:53	Rr86L0Zrn4THvV4BPp4fW1E5e7MAa0o53liwQe9m6UCbq0Xz
8	akal	demo	97806	05-02-2024	12:04	wk1QEeSv97Mnao5U0CqKy3GJu0b26jXxDRF0ZehYvdrBLz4
9	vinath	vinathfile	22789	09-02-2024	15:00	6Vj0x02RrFLZNe4Hjgu0c3q7K1YyESGAauWw1en9Mz5Thv8Pq
10	vinath	test	20720	09-02-2024	15:02	/RcCoRq5KYym31GJu0a07WkESaao4Hv0P0dn6Zn2VjRygu0CqKtmGUC

Fig 2.1.9 File Details

2.1.10 CLOUD AUTHORITY

This module is main module which is developed for cloud authority. The cloud authority gives access credentials to the registered users. Then only the users can access further to upload and download files.

3 CONCLUSION

The project conclusion a secure and efficient remote monitoring framework named any organization in the context of IoT, which enables two fundamental security functionalities for users, i.e., a user can control which deployed devices can be accessed by which monitoring services, and he/she can be further assured that functions over his/her data are securely executed without leaking the privacy information to unauthorized entities. To this end, we leverage the off-the-shelf secure hardware, i.e., Intel 2PVC algorithm those cumbersome crypto-based solutions in previous works. Furthermore, we also introduce a “heartbeat” mechanism to solve the key revocation issue and thus efficiently support service un-subscription for users.

4 FUTURE ENHANCEMENT

In future work will focus on further improvements of the scheme based on the community feedback. Security wise, finding an alternative solution to the trusted index repository service and removing this limiting component from the scheme seems a reasonable next step.

REFERENCE

- [1] A. Adya et al., “Farsite: Federated, available, and reliable storage for an incompletely trusted environment,” in Proc. of the OSDI, 2002.
- [2] Data Security Issues in Cloud Computing: From Single to Multi-Clouds [Mohammed A. AlZain, Ben Soh and Eric Pardede] Information Security Agency (ENISA), Tech. Rep., 2012.
- [3] D.R. Kuhn, E.J. Coyne, and T.R. Weil, “Adding Attributes to Role- Based Access Control,” IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.
- [4] D. R. Matos, M. L. Pardal, G. Carle, and M. Correia, “Rockfs: Cloud backed file system resilience to client-side attacks,” in Proc. of the Middleware, 2018.
- [5] Efficient Privacy Preserving and Secure Data Integrity Protection In Regenerating Coding Based Public Cloud Storage.
- [6] European Commission, “Data protection,” https://ec.europa.eu/info/law/law-topic/data-protection_en, 2018
- [7] F. Zhao, T. Nishide, and K. Sakurai, “Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems,” Proc. Seventh Int’l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

- [8] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
- [9] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
- [10] Jain S, Kumar R, Kumawat S and Jangir S K, "An analysis of security and privacy issues, Challenges with possible solution in cloud computing", Proc. of the National Conf. on Computational and Mathematical Sciences (COMPUTATIAIV), 2014, 1-7.
- [11] J. Kubiatowicz et al., "OceanStore: An architecture for global-scale persistent storage," in Proc. of the ASPLOS, 2000.
- [12] J. Stribling et al., "Flexible, wide-area storage for distributed system with WheelFS," in Proc. of the NSDI, 2009
- [13]Kandias M, Virvilis N and Gritzalis D, "The insider threat in cloud computing" Proc. of 6th International Conf. on Critical Infrastructure Security, 2011, 95-106.
- [14] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control Multi-Owner Settings" Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm),pp. 89-106, 2010.
- [15] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.
- [16] Secure Data Sharing in Cloud Storage with Key Aggregate Cryptosystem [rof. B. M. Kore #1, Archana Jadhav*2, Prof. V. V. Pottigar]
- [17] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.
- [18] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy Computing and Communications (TrustCom), 2011.
- [19] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.
- [20] T. E. Anderson et al., "Serverless network file systems," ACM Trans. Computer. Syst., vol. 14, no. 1, pp. 41-79, 1996.

