PEER-TO-PEER CLOUD: ANONYMOUS AUTHENTICATION AND KEY AGREEMENT

[#1]BONGONI MADHURI,
[#2]P.SATHISH, ***Assistant Professor,***
[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

Abstract: Cross-cloud data migration is a typical issue for mobile consumers, and it is a required step when customers transfer mobile phone providers. Customers frequently find it difficult to backup all data from the original cloud servers to their mobile phones before migrating the downloaded data to the new cloud provider due to smart phones' limited local storage and computing capabilities. To solve this issue, we present an efficient data transit model among cloud providers, as well as an elliptic curve certificate-free mutual authentication and key agreement technique for peer-to-peer cloud. The proposed technique builds trust among cloud providers and lays the groundwork for cross-cloud data transfer deployment. The mathematical veracity and security correctness of our technique are compared to important current data migration strategies, demonstrating that our proposed scheme surpasses other state-of-the-art schemes in terms of both computational and communication cost reduction.

***Index Terms*—**Cloud computing, data migration, elliptic curve, authentication, key agreement.

1. INTRODUCTION

Data must be transferred from the cloud server of the current smart device provider to the cloud server of the new smart device provider if a customer decides to switch to a different smart device made by a different firm. It is normal practice to access the primary cloud server, transfer the data to intelligent terminal devices, access the secondary cloud server, and then transfer the data to the secondary cloud server.

In order to accomplish this, it is necessary to devise a safer and more streamlined method of transferring data between different cloud services. The most efficient method for transferring user data from one cloud server to another. The term for this process is "data migration." Implementing this ideal data migration strategy is complicated by the wide variety of cloud service providers available. This is due to issues with compatibility, lack of trust, and potential security breaches during data transfer.

Data migration research has been demonstrated to have significant practical ramifications. It can be challenging to move data from one cloud to another for a variety of reasons. There are currently a number of issues that make data migration to the cloud less efficient. To make it simpler and quicker for consumers to transfer their data between cloud servers when they switch phones, additional research is needed on the context of cloud data mobility. Multicloud setups make it challenging to establish trust, which is especially problematic for apps that transfer sensitive data and must adhere to stringent security protocols. Mutual authentication, secure communication keys, and uncompromised data transfer are all crucial considerations. These concerns can be addressed by implementing authentication and key agreement procedures.

2. RELATED WORK

The transition to computing on the cloud is the natural next step. Computing resources, both hardware and software, are pooled and made available across a network (such as the Internet, an intranet, or an extranet) as a service in cloud computing. In cloud computing, everything from data storage to application and operating system software to networking hardware is housed on a central server, or "cloud server." These features can be accessed through desktop computers, smartphones, tablets, and other devices, all at the user's discretion. As a metaphor for abstraction in a highly coordinated architectural framework, "the cloud" captures this essence. In cloud computing, all of a user's information is stored and processed by third-party servers rather than on their local device. Multiple entry points are made available to the user in this way. Accessing hardware, software, and application resources is simplified by using the Internet and mobile wireless technology. These assets are managed by external services. External users or web browsers can access the cloud servers' resources and use them as they see fit.

Users of these services are frequently granted entry to robust server-based computer networks and applications. It's conceivable that "cloud computing" will be the next big thing for Internet-connected devices. The use of cloud computing can lessen the quantity of hardware and the maintenance costs associated with it. Having a centralized system that can accommodate a huge user base's demands for resources and services also makes it easier to employ environmentally friendly practices. Cloud architecture has been proposed as a viable solution to the issues of capital expenditure, maintenance, and minimizing security risks.

In the following diagram, we see how cloud computing is structured. According to McDaniel, better security decisions may be made with accurate, up-to-date, and comprehensive origin information. Many people now suffer from a lack of background knowledge because of the Internet. Data is frequently sifted, sliced, diced, compressed, and otherwise processed before being put to new uses. The slow increase in entropy brought on by these processes causes the information's validity to degrade over time. This presentation explores the necessity, use, and constraints of facilitating information systems' access to provenance information.

The term "provenance" has been adopted by a variety of academic disciplines as a means of establishing the credibility of a source. Rajbhandari et al. conducted research to determine whether or not provenance information influences the efficiency of a Bio-Diversity initiative. The "provenance" of a process outcome is the record of the process steps that lead up to the result, including the people, methods, and resources used. If researchers are supposed to analyze and trust the data, they need to know more about its origins. In this research, we demonstrate how to determine the reliability of information by analyzing workflow-related provenance data. This research is grounded in a wide range of applications for variety. In addition, our trust architecture is presented in a straightforward layout.

3. SYSTEM DESIGN

More and more individuals are relying heavily on their smartphones, tablets, and other portable electronic gadgets. Keep in mind that one person can have and utilize multiple smart devices. Many people dispose of their old smartphones and tablets since the newest models have more desirable functions preinstalled.

Data stored in the cloud by one smart device provider must be transferred to the cloud server of a second smart device provider if a customer decides to switch to a different smart device made by a different company. It is normal practice to access the primary cloud server, transfer the data to intelligent terminal devices, access the secondary cloud server, and then transfer the data to the secondary cloud server. Currently, a lot of time is wasted, and results aren't as good as they could be.

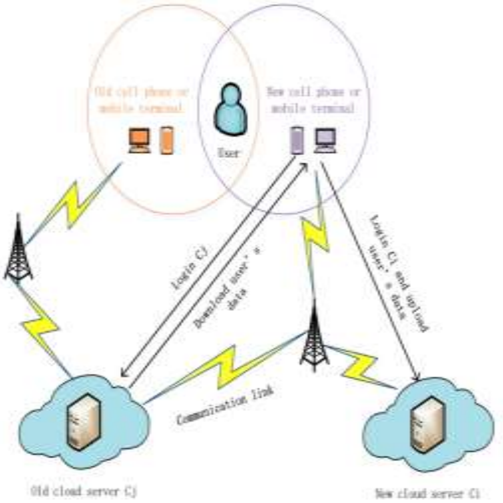

Old cell phone or mobile terminal
User
New cell phone or mobile terminal
Login Cj
Download user's data
Login Ci and upload user's data
Communication link
Old cloud server Cj
New cloud server Ci

Fig. 1. Original data migration model

The study of information exchange between cloud services has been demonstrated to have important real-world implications. There are a number of potentially serious problems that might arise when moving data from one cloud to another. The efficiency of existing efforts in the field of cloud data migration is hampered by a number of obstacles. As a result, it's clear that more research is needed into the context of cloud data migration, particularly with regards to streamlining the transfer of data across cloud servers when users switch phones. Trustworthiness is also difficult to achieve in multi-cloud settings, which is especially problematic for apps that transmit sensitive data. More severe safety precautions are required for these applications. Achieving mutual authentication, building communication keys securely, and protecting data flow from assaults are all important considerations. The use of authentication and key agreement processes helps alleviate these worries. In light of these considerations, this study presents a novel method for achieving authentication and key agreement in P2P cloud environments. The suggested method makes use of anonymous identification to facilitate easy and secure data movement between different clouds.

4. SYSTEM ANALYSIS

The meetings occurred at the same time.

The prevalent Internet standard, the parallel Network File System (pNFS), allows for the construction of fast and scalable parallel secure sessions between users and storage units. This is analogous to the scenario in which an adversary compromises the long-term confidential key and then has access to all subsequent sessions. After a trusted client and storage device have completed a matching session, they will have produced the same session key. Two of the protocols I've created also have the property of forward secrecy, which is a plus. In terms of protecting several sessions within a certain window of time, one of these protocols can be categorized as moderately forward secure, while the other may be deemed entirely forward secure.

Key exchange is the safe and secure transfer of cryptographic keys between parties after their identities have been verified.

The project's primary objective is to provide secure and efficient protocols for authenticated key exchange that meet the requirements of pNFS.Three new authenticated key exchange mechanisms are presented in this research that show promise for improving safety. This study provides a summary of the design goals and investigates the many potential pNFS authenticated key exchange6 (pNFS-AKE) protocols.

Definition of secretive actions

It is crucial for the protocol to assure the continuous security of earlier session keys in the event that the client's or storage device's extended-term secret key is compromised.However, there is no provision for forward secrecy in the agreement.To allay worries about key escrow and achieve forward secrecy, the Kerberos-like pNFS-AKE-I protocol incorporates a Diffie-Hellman key agreement mechanism.However, it must be emphasized that partial forward secrecy was achieved by putting practicality ahead of security.

RESULTS

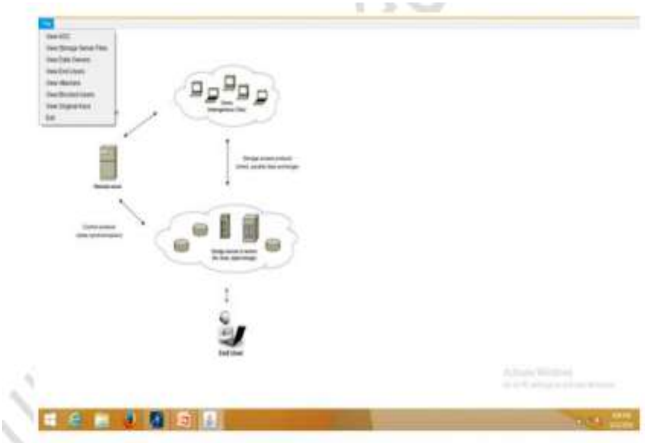
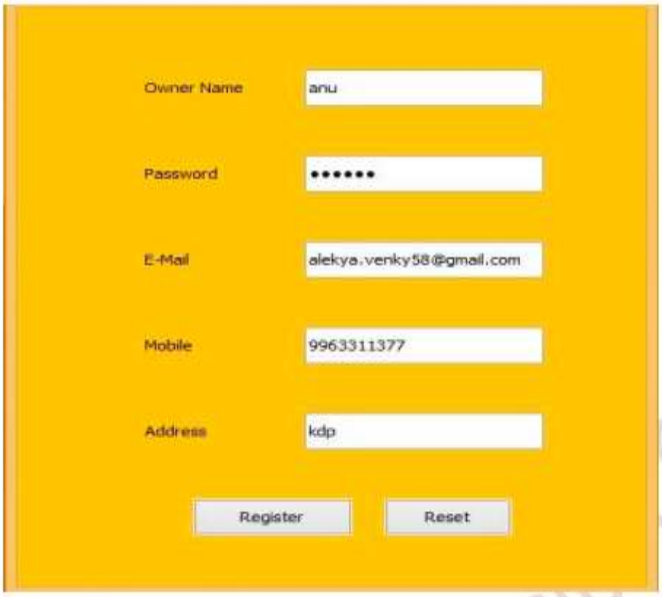


Fig 1: Handling of files

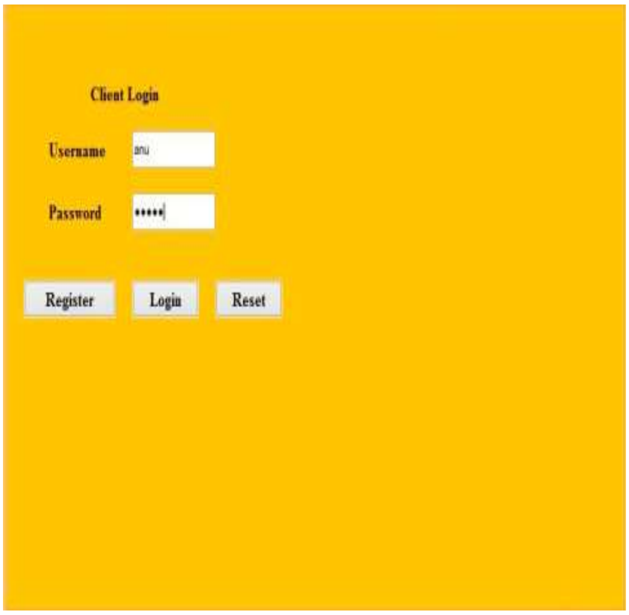
The term "file management" is used to describe the process of saving a program's output to a specific file and then performing various tasks on that file. The term "stream" is used to describe a hypothetical instrument that can both receive and send information.



Owner Name: anu
Password: ••••••
E-Mail: alekya.venky58@gmail.com
Mobile: 9963311377
Address: kdp

Fig 2 Owner Registration Page

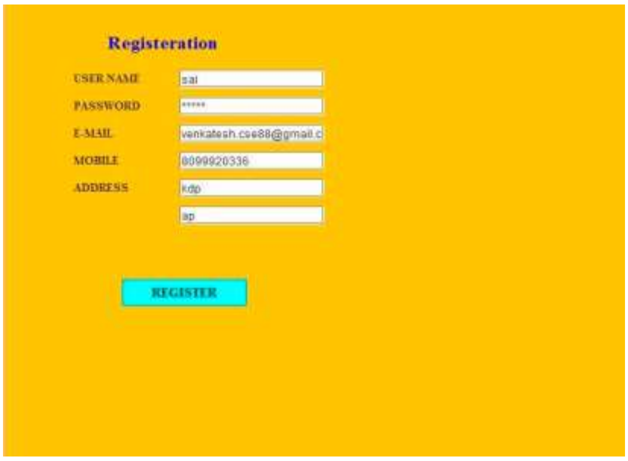
The present user interface displays the owner registration form, which must be filled out for registration to be complete. After then, the user can log in using their authentication information.



Client Login
Username: anu
Password: •••••

Fig 3 Owner Login Page

The term "login page" is used to describe any page or entry point on a website that requires user credentials for access. Typically, this is done by entering a login and password. Logins, which are another term for user authentication credentials, can grant access to an entire website or just a restricted area inside it. Cookies are used by some websites to monitor user behavior while they are signed in.



Registeration
USER NAME: sai
PASSWORD: *****
E-MAIL: venkatesh.cse88@gmail.c
MOBILE: 8099920336
ADDRESS: kdp
ap

Fig 4 End User Registration Page

The accompanying illustration depicts the user interface for the registration form that must be filled out for a successful registration to take place. After that, the person might potentially use their credentials to verify their identity and get entry.

5. CONCLUSION

The research presented a new method, using a key agreement mechanism, to expedite the transfer of user data between different cloud servers. The benefits of our approach in terms of security performance, computation costs, and communication costs are elucidated through a mathematical analysis and comparative evaluation presented in the current study. Our proposed approach has the potential to efficiently overcome the substantial challenge of establishing trust during data transfer between cloud servers while also protecting the identities of those servers. By prioritizing the privacy of cloud service providers, our suggested methodology indirectly guarantees the privacy of consumers. Additionally, our proposed methodology's identity-tracing capabilities equip customers with the tools they need to effectively govern cloud service providers.

REFERENCES

[1] M. Abd-El-Malek, W.V. Courtright II, C. Cranor, G.R. Ganger, J. Hen-dricks, A.J. Klosterman, M.P. Mesnier, M. Prasad, B. Salmon, R.R. Sam-basivan, S. Sinnamohideen, J.D. Strunk, E. Thereska, M. Wachs, and J.J. Wylie. Ursa Minor: Versatile cluster-based storage. In Proceedings of the 4th USENIX Conference on File and Storage Technologies (FAST), pages 59–72. USENIX Association, Dec 2005.

[2] C. Adams. The simple public-key GSS-API mechanism (SPKM).The Internet Engineering Task Force (IETF), RFC 2025, Oct 1996.

[3] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer. FARSITE: Federated, available, and reliable storage for an incompletely trusted environment. In Proceedings of the 5th Symposium on Operating System Design and Implementation (OSDI). USENIX Association, Dec 2002.

[4] M.K. Aguilera, M. Ji, M. Lillibridge, J. MacCormick, E. Oertli, D.G. Andersen, M. Burrows, T. Mann, and C.A. Thekkath. Block-level security for network-attached disks. In Proceedings of the 2nd International Conference on File and Storage Technologies (FAST). USENIX Association, Mar 2003.

[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Communications of the ACM, 53(4):50–58. ACM Press, Apr 2010.

[6] Amazon simple storage service (Amazon S3). http://aws.amazon.com/ s3/.

[7] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key ex-change secure against dictionary attacks. In Advances in Cryptology – Proceedings of EUROCRYPT, pages 139– 155. Springer LNCS 1807, May 2000.

[8] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Advances in Cryptology – Proceedings of CRYPTO, pages 258–275. Springer LNCS 3621, Aug 2005.

[9] B. Callaghan, B. Pawlowski, and P. Staubach. NFS version 3 protocol specification. The Internet Engineering Task Force (IETF), RFC 1813, Jun 1995.