

SECURED PAYMENT ON BLOCKCHAIN FOR OUTSOURCING SERVICES IN CLOUD COMPUTING

¹Ms.Rajashree Sutrawe, ²A Uday Kumar, ³A Sathish Babu, ⁴Akhila Charabudla

¹Associate Professor, Guru Nanak Institutions Technical Campus, Hyderabad

^{2,3,4} Scholar, Guru Nanak Institutions Technical Campus, Hyderabad

ABSTRACT :

Cloud computing has revolutionized outsourcing services, yet concerns about online payment security and mutual distrust persist. Existing solutions often rely on trusted third parties, limiting their applicability. To address this, we introduce BPay, a novel framework leveraging blockchain technology to enable a payment system that is both secure and equitable for outsourcing services without intermediaries. We introduce the system framework, adversary model, and objectives of BPay, emphasizing its compatibility with Bitcoin and Ethereum blockchains. Security and compatibility analyses demonstrate BPay's robustness and efficiency. Cloud computing has revolutionized the manner in which outsourcing services are delivered and accessed, offering unprecedented scalability, flexibility, and cost-effectiveness. However, despite its numerous benefits, concerns about the security of online payments and the lack of trust between users and service providers continue to pose significant challenges. Traditional payment systems often rely on trusted third parties to facilitate transactions, which can introduce vulnerabilities and increase the risk of fraud or data breaches. These limitations hinder the broader adoption of cloud computing in various industries and applications.

Keywords: *efficient fair payment, blockchain-based technology, RSA algorithm, public key private key, security, Encryption-decryption*

INTRODUCTION :

Distributed computing is becoming commonplace in our contemporary society. As a simple example, let us consider a scenario where an outsourcer, say O, wishes to purchase a digital commodity x from a worker, say W. When x fulfils a certain condition ψ (such that $\psi(x) = 1$), O is ready to remunerate W with price P for executing or finishing x . Nonetheless, it's crucial to ensure fair execution of transactions between O and W. Specifically, if O behaves dishonestly, there's a risk of reneging on the pre-agreed service fee even upon receipt of x from W. Likewise, in cases where W acts dishonestly, O faces uncertainty regarding the accuracy of the received x post-payment of the service fee. To address this concern, Pagnia and Gärtner proposed the concept of strong fairness, leading to the development of various solutions leveraging a trusted third-party (TTP), commonly known as an escrow service, as outlined in existing literature. The challenge of establishing trust between outsourcers

and workers stands as a significant barrier to the widespread adoption of cloud computing and outsourcing services. Hence, addressing fair payment as a potential remedy to this matter has received growing attention in recent years.

LITERATURE SURVEY :

Title: Enhancing Public Cloud Storage Security: An Attribute-Based Collaborative Access Control Approach"

Author: Y. Xue, K. Xue, N. Gai, J. Hong, D. S. Wei, and P. Hong

Year: 2020

Description:

In the realm of public cloud storage services, data is entrusted to cloud servers with a level of trust that is partial or intermediate. that operate beyond the

confines of data owners' secure domains. To safeguard sensitive data from potentially untrustworthy service providers, encryption is commonly employed on outsourced data. However, managing access control in this context presents a formidable challenge. Attribute-based encryption (ABE) has arisen as a potent cryptographic solution for articulating access policies based on attributes. ABE offers a nuanced, adaptable, and robust mechanism for controlling access to outsourced data, thereby addressing these complexities effectively.

Title: Approaches for Evaluating and Enhancing Data Quality.

Author: C. Batini, C. Cappiello, C. Francalanci, and A. Maurino.

Year: 2009.

Description:

Various methodologies have been proposed in the literature to evaluate and enhance data quality, reflecting the broad spectrum of available techniques. Given the diversity and intricacy of these methods, recent research efforts have concentrated on delineating frameworks that facilitate the selection, adaptation, and implementation of data quality assessment and improvement techniques. This article aims to offer a systematic and comparative overview of these methodologies.

EXISTING SYSTEM :

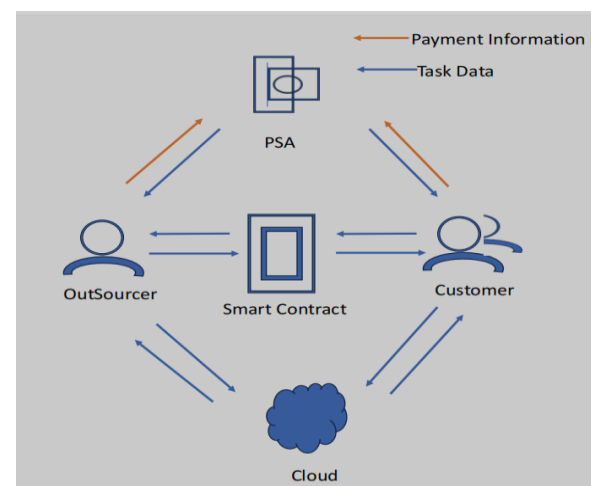
Even with the advanced state of cloud services, such as the delegation of computational tasks, several operational hurdles persist. One such challenge is establishing trust between outsourcers and workers within a zero-trust framework. Despite the emergence of numerous blockchain-based solutions aiming to eliminate the need for trusted third parties, many of these approaches fail. To attain strong equity and accountability, support compatibility with other systems. The absence of trust between those outsourcing tasks and the workers completing them stands as a significant obstacle to the widespread

adoption and advancement of cloud computing and outsourcing services.

PROPOSED SYSTEM :

This paper suggests a platform for sharing quality data in aviation supplier manufacturing processes, based on blockchain technology. Firstly, the paper introduces the possibility of integrating Quality management within the manufacturing supply chain utilizing blockchain technology. Next, we introduce the platform for sharing quality and data for the production processes of emerging aviation suppliers, focusing on quality status and categorization of aviation suppliers. Subsequently, we outline a comprehensive methodology for implementing secure quality and data sharing to ensure the real-time and systematic functioning of the sharing platform.

SYSTEM ARCHITECTURE :



METHODOLOGIES:

Modules names:

1. User Interface Design
2. Outsourcer
3. Customer

4. Cloud Server

5. PSA

1. User Interface Design :

In this module, we develop secure login windows for the project, facilitating user access to the server. Users are required to input their username and password to establish a connection with the server. If the user is already registered, they can directly log in; otherwise, they must register by providing their username, password, and email ID.

2. Outsourcer :

This is the module outsourcer can register and Login. After login User have an option of searching the files as a file name. User can also have a download file it will show an encrypted data. Data user can also send a trapdoor request to the server. Server can accept the request and then data user can takes permissions from the owner then the file it will downloaded in plain text.

3. Customer :

In this module user should register and Login. User will Uploads the files into the database.

4. Cloud Server :

This module constitutes the third phase of the project. It enables the Cloud Server to log in and access information pertaining to all data owners. Additionally, the Cloud Server is capable of viewing user details, accessing stored data files, requesting encryption keys from users, and retrieving information about potential attackers associated with files.

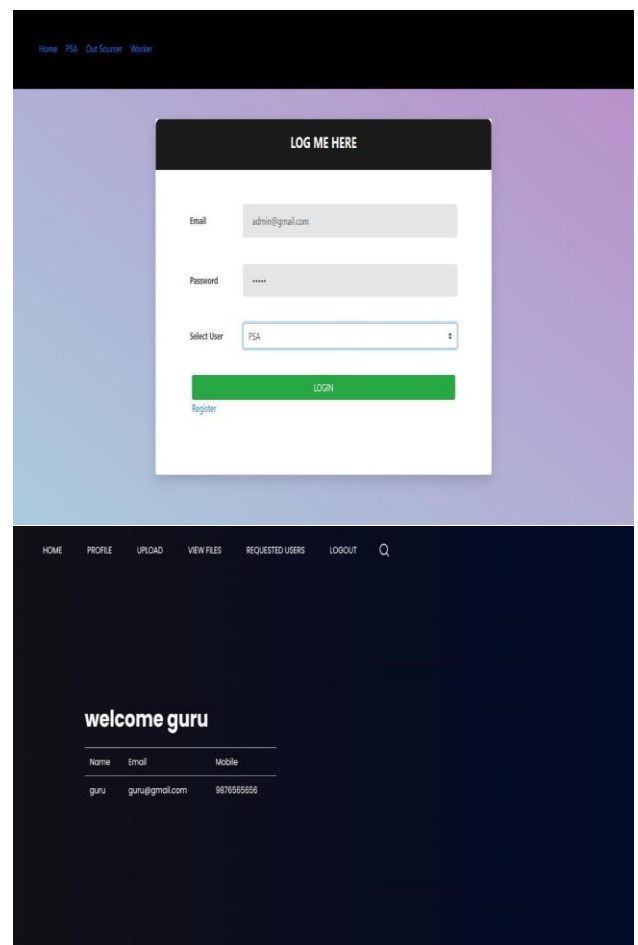
5. PSA:

In this module Cloud Server can login. After login it will to realize the payment function and thus is perfectly compatible with some permission block chains that do not support token functions. Pay-As-YouGo: This feature ensures the convenience of payment.

ALGORITHM:

EFPB uses a several cryptographic components, including one-way accumulator, stealth address, and symmetric encryption, to achieve Efficient Fair Payment Based on Blockchain (EFPB) is a payment system designed to ensure robust fairness without using zero-knowledge proofs or relying on trusted third parties. It is mainly used for delegating services in cloud computing, where trust between outsourcers and customers is a challenge. systems. robust fairness and compatability with others.

OUTPUTS/SCREENSHOTS:



Name	Email	Mobile
guru	guru@gmail.com	9876555555

CONCLUSION:

We have described our proposed efficient blockchain-based fair payment scheme (EFPB) that can be used to facilitate computational outsourcing in a cloud computing environment. We then demonstrated how EFPB uses three cryptographic primitives to ensure completeness, robust fairness, compatibility, pay-as-you-go, ZKP-free, TTP-free. We also deployed the smart contract on the Remix environment to calculate the gas cost and analyze EFPB's communication and computing overheads also in comparison to OBFP outlined in. While our security and performance evaluations suggested the utility of EFPB, one future extension of this work is to collaborate with a real-world service provider and evaluate the security and performance of the (prototype) implementation in practice.

FUTURE SCOPE:

Lastly, it's important to note that we haven't considered the communication overhead of the SC as it retrieves data directly from the local database. An area for future development involves partnering with a real-world service provider to assess both the security and performance of the implementation in real-world scenarios.

REFERENCES:**Articles and books:**

1. Pressman, Roger (2010) Software Engineering : A practitioner's Approach, McGraw Hill, New York, NY.
2. Stephens, Rod (2015) Beginning Software Engineering, Wrox
3. L. Ecekey, S. Faust, and B. Schlosser, "OptiSwap: Fast optimistic fair exchange," in Proc. 15th ACM Asia Conf. Comput. Secur., Oct. 2020
4. A. Chiesa, E. Tromer, and M. Virza, "Cluster computing in zero knowledge," in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Cham, Switzerland: Springer, 2015
5. B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," in Proc. IEEE Symp. Secur. Privacy, May 2013.
6. Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Ambiguous optimistic fair exchange," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Cham, Switzerland: Springer, 2008.