International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

EFPB: Efficient Fair Payment Based on Blockchain for Outsourcing Services in Cloud Computing

Pathipati Chandra Sekhar[1]
Assistant Professor, Guru Nanak Institute of Technology, Department of CSE, Hyderabad

K.Suresh Babu[2]
Assistant Professor, PACE Institute of Technology and Sciences, Department of CSE, Ongole

ABSTRACT

Despite the maturity of cloud services (e.g., outsourcing of computational tasks), a number of operational challenges remain. For example, how do we ensure trust between outsourcers and workers in a zero-trust environment? While a number of blockchain-based solutions that eliminate the reliance on trusted third parties have been presented, many of these existing approaches do not achieve robust fairness and/or support compatibility with other systems. In this paper, we propose an efficient fair payment system using blockchain (EFPB), designed to achieve robust fairness and compatibility. Specifically, EFPB comprises a number of cryptographic building blocks, mainly: one-way accumulator (RSA-based construction), stealth address and symmetric encryption. We then evaluate the performance of EFPB to demonstrate that it is more efficient and low-cost than other competing schemes, as well as presenting a comparative summary of functionalities.

I.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. If x satisfies some predicate ψ (i.e. $\psi(x) = 1$), O is willing to pay price P to W for performing/completing x. However, we have to also ensure that the transaction is executed fairly between O and W. Specially, if O is dishonest, (s)he may refuse to pay the pre-agreed service fee even after receiving x from W. Similarly, if W is dishonest, O cannot ensure that the received x is correct after (s) he paid the service fee. As a countermeasure, Pagnia and Gärtner introduced the notion of strong fairness, and since then a number of solutions based on a trusted thirdparty (TTP; often referred to as an escrow service) have been proposed in the literature. For example, an efficient conditional payment scheme for outsourcing computation, where a banking institution is designated as the TTP to ensure the fairness. In reality, however, it can be challenging to construct such a perfect TTP, without incurring significant cost. To eliminate the reliance on TTP, put forward the concept of optimistic fairness in which TTP will only be involved when a dispute arises. Similarly, a number of approaches to support optimistic fairness were proposed but as explained in most of the existing solutions do not ensure robust fairness. There have also been recent attempts to ensure robust fairness using zero-knowledge proof (ZKP). For example, two zero knowledge contingent service payment protocols, but their approach incurs significant computational cost to both parties in the transaction. Similar limitations were observed in the approach in this paper, we design an efficient fair payment scheme based on block chain (hereafter referred to as EFPB) to facilitate outsourcing of computational tasks. EFPB is designed to ensure robust fairness without using ZKP or relying on TTP. Specifically, EFPB comprises one-way accumulator (RSA based construction), stealth address and symmetric encryption. In our approach, fair payment is carried out using smart contracts, which play the role of a communication bridge between the outsourcer 2 and the worker. Consequently, our approach incurs lower communication overhead compared to approaches that rely on TTP. In addition, due to the ZKP-free feature, our solution incurs lower computational cost. The payment function of our

EFPB scheme is realized by cryptocurrencies that supports stealth address technique to protect user transaction privacy. Many other blockchain-based solutions are generally implemented on Ethereum, and the transaction fee is expensive because users need to pay fees to miners for every step of executing a smart contract, storing and computing complex instructions. In comparison, transaction fee required to transfer in Monero is negligible. We also remark that our EFPB scheme is compatible with other blockchains that do not support tokens, in comparison to other competing approaches that require not only the blockchain to support smart contracts but also the function of tokens. The rest of the paper is organized as follows. We review a number of related approaches in Section II before introducing the relevant preliminaries.

II .LITERATURE REVIEW

An attribute based controlled collaborative access control scheme for public cloud storage. Y.Xue, K.Xue, N.Gai, J.Hong, D. S.Wei, and P. Hong,2020 In public cloud storage services , data are out sourced to semi-trusted cloud servers which are outside of data owners' trusted domain. To prevent untrustworthy service providers from accessing data owners' sensitive data, outsourced data are often encrypted. In this scenario, conducting access control over these data becomes a challenging issue. Attribute-based encryption (ABE) has been proved to be a powerful cryptographic tool to express access policies over attributes, which can provide a fine-grained, flexible, and secure access control over outsourced data. Extensive performance analysis shows that Methodologies for data quality assessment and improvement**.** C. Batini, C. Cappiello, C. Francalanci, and A. Maurino. 2009..The literature provides a wide range of techniques to assess and improve the quality of data. Due to the diversity and complexity of these techniques, research has recently focused on defining methodologies that help the selection, customization, and application of data quality assessment and improvement techniques. The goal of this article is to provide a systematic and comparative description of such methodologies. Methodologies are compared along several dimensions, including the methodological phases and steps, the strategies and techniques, the data quality dimensions, the types of data, and, finally, the types of information systems addressed by each methodology. The article concludes with a summary description of each methodology.Research on risk avoidance and coordination of supply chain subject based on block chain. Liu, Li, and Qi. 2019.Based on the influence of block chain technology on information sharing among supply chain participants, mean-C VaR (conditional value at risk) is used to characterize retailers' risk aversion behavior, while a Stack el berg game is taken to study the optimal decision-making of manufacturers and retailers during decentralized and centralized decision-making processes. The revenue sharing contract can achieve the coordination of the supply chain to the level of centralized decision-making. Through block chain technology, transaction costs among members of the supply chain can be reduced, information sharing can be realized, and the benefits of the supply chain can be roved. Finally, the specific numerical. Simulation is adopted to analyze the weighted proportion, risk aversion and the impact of block chain technology on the supply chain, and verify the relevant conclusions**.**

Differentially private auction for block chain based micro grids energy trading.

M.Ul Hassan,M.H. Rehmani, and J.Chen**.** 2020 Modern smart homes are being equipped with certain renewable energy resources that can produce their own electric energy. From time to time, these smart homes or micro grids are also capable of supplying energy to other houses, buildings, or energy grid in the time of available self-produced renewable energy. Therefore, researches have been carried out to develop optimal trading strategies, and many recent technologies are also being used in combination with micro grids. One such technology is block chain, which works over decentralized distributed ledger. In this paper, we develop a block chain based approach for micro grid energy auction. We compare DEAL with Vic kre y-Clarke- Groves (VCG) auction scenario and experimental results demonstrates that DEAL outperforms VCG mechanism by maximizing sellers' revenue along with

maintaining overall network benefit and social welfare.

Block chain for supply chain traceability: Bus. Requirements and critical success factors. G.M.HastigandM.S.Sodhi.2020.We seek to guide operations management (OM) research on the implementation of supply chain traceability systems by identifying business requirements and the factors critical to successful implementation. We first motivate the need for implementing traceability systems in two very different industries—cobalt mining and pharmaceuticals—and present business requirements and critical success factors for implementation. Next, we describe how we carried out the mastic analysis of practitioner andscholarlyarticlesonimplementingblockchainforsupplychaintraceability.Finally, wepresentourresultspertainingtotheneedsofdifferentstakeholderssuchassuppliers, consumers, and regulators.

The impact of digital technology and industry 4.0 on the ripple effect and supply chain risk analytics .D. Ivanov, A. Dolgui, and B.Sokolov.2019
The impact of digitalization and Industry 4.0 on the ripple effect and disruption risk controlanalyticsinthesupplychain(SC)isstudied.Theresearchframeworkcombines the results from two isolated areas, i.e. the impact of digitalization on SC management (SCM)andtheimpactofSCMontherippleeffectcontrol.Tothebestofourknowledge, this is the first study that connects business, information, engineering and analytics perspectives on digitalization and SC risks. With these two frameworks, this study contributes to the literature by answering the questions of

(1) What relation sex it between big data analytics, Industry 4.0, additive manufacturing, advanced trace & tracking systems and SC disruption risks?

(2) Howdigitalizationcancontributetoenhancingrippleeffectcontrol;and

(3)

III .SCOPEOFTHE PROJECT

OBJECTIVE

The issue of trust between outsourcers and workers is one main factor hindering the promotion of cloud computing and outsourcing services. Therefore, fair payment as a possible solution to this problem has been studied in recent years. To remove the dependence on TTPs which seriously affect the efficiency of fair payment, proposed a weaker security model named optimistic fair exchange. In this model, a TTP can be consulted only in case the out sourcers or workers deviates from the expected behavior.

PROBLEM STATEMENT

The issue of trust between outsourcers and workers is one main factor hindering the promotion of cloud computing and outsourcing services. Therefore, fair payment as a possible solution to this problem has been studied in recent years. To remove the dependence on TTPs which seriously affect the efficiency of fair payment, proposed a weaker security model named optimistic fair exchange. In this model, a TTP can be consulted only in case the outsourcers or workers deviates from the expected behavior. As mentioned in, however, the existence of TTP leads to the failure of robust fairness.

EXISTING SYSTEM:

Despite the maturity of cloud services (e.g., outsourcing of computational tasks), a number of operational challenges remain. For example, how do we ensure trust between outsourcers and workers in a zero-trust environment? While a number of block chain- based solutions that eliminate the reliance on trusted third parties have been presented, many of these existing approaches do not achieve robust fairness and or up port compatibility with other systems. The issue of trust between outsources and workers is one main factor hindering the promotion of cloud computing and outsourcing services. Therefore, fair payment as a possible solution to this problem has been studied in recent years.

Existing System Disadvantages:

- Collection of quality characteristic data, high-speed safe transmission.
- Next-generation information technology.

PROPOSED SYSTEM

This paper proposes a block-chain –based aviation supplier manufacturing process quality data-sharing platform. Firstly, the paper introduces the possibility of integrating manufacturing supply chain quality management with block-chain technology. Secondly, the quality and data sharing platform architecture of the production process of new aviation suppliers is presented based on quality state and island kinds of aviation suppliers. Then, a detailed method for the implementation of quality and data security sharing is proposed to support the sharing platform's real-time and orderly operation. Build critical technologies such as manufacturing quality data block pack aging models, data storage security sharing, and supplier assessment model on this foundation. Finally, depending on data collection of supplier product production processes to shared application practices based on a specific aircraft industrial park under the supervision of the platform architecture and technology. The application platform integrates the data supply and request components, providing practical and intelligent sharing solutions for airlines' product quality data.

PROPOSED SYSTEM ADVANTAGE

- Sharing platform's real-time and orderly operation.
- Data storage security sharing, and supplier assessment models on this foundation
- Providing practical and intelligent sharing solutions for airline

SYSTEM ARCHITECTURE

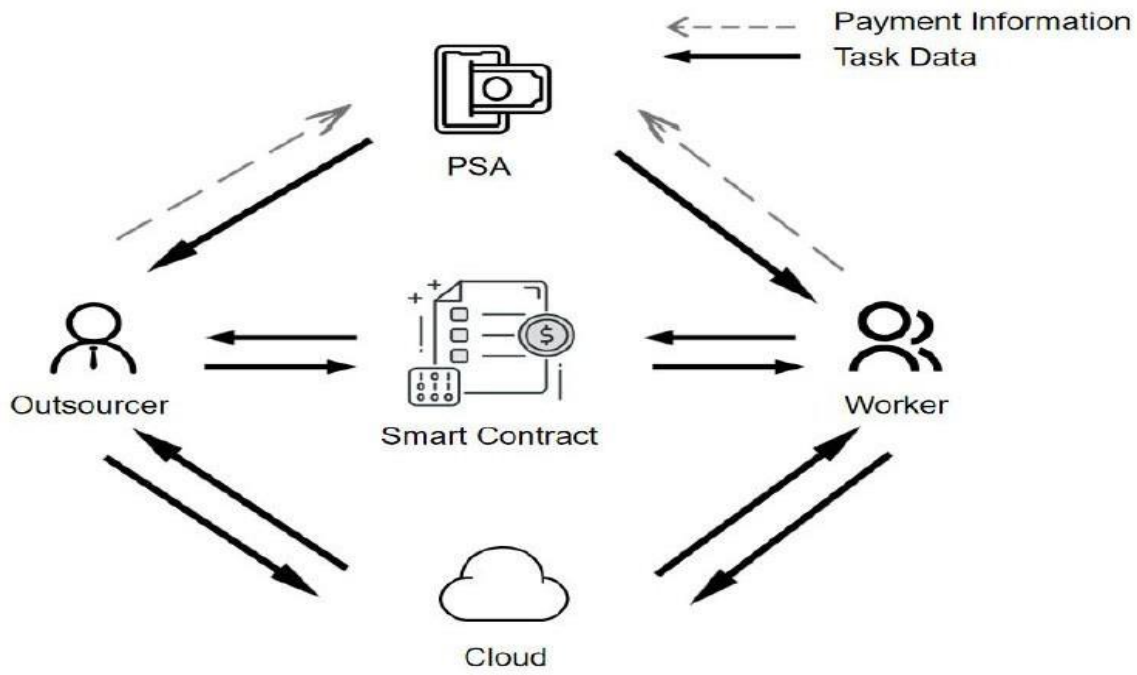

Fig: System Architecture

In this project data owner has a register all details and then login. Data owner can be an upload a document. Data owner can have a send request to the data user. Data user can search a query with uploaded document. The file has also a download it will show an encryption format. Data user also send a request to the cloud server. Cloud server can a login. It will accept a key approve. Cloud server can also see all the data information's. Cloud server can also see all the user information. Cloud server can see all the stored information. Cloud server can approve a key request from the user. Then data owner has get there quest data owner can send a secret key to the user. Then user can also down load a file. If the user has given wrong keys it gets warning the user has a block permanently. The file it gets an attacks.

PROJECT DESCRIPTION
GENERAL:

We assume that the data owner is trusted, and the data users are authorized by the data owner. The communication channels between the owner and users are secure on existing security protocols such as SSL, TLS. With regard to the cloud server, our scheme resists a more challenging security model which is beyond the "semi-honest server" used in other secure semantic searching schemes. In our model, the dishonest cloud server attempts to return wrong/forged search results and learn sensitive information, but would not maliciously delete or tamper with the

outsourced documents. Therefore, our secure semantic scheme should guarantee the verifiability, and confidentiality under such a security model.

METHODOLOGIES

MODULESNAME:

1. User Inter-face Design
2. Outsourcer
3. Worker
4. Cloud Server
5. PSA

RESULT&DISCUSSION

GENERAL:

This project is implements like web application using COREJAVA and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.

SCREENSHOTS

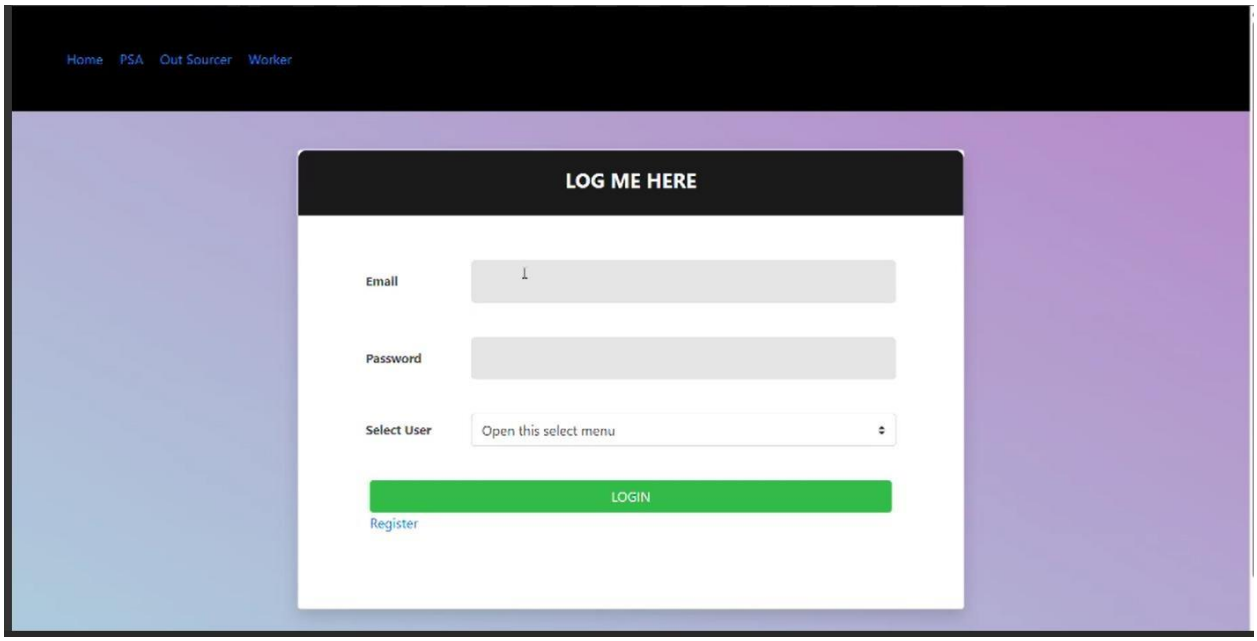

Fig:HomePage

This login page allows different types of users (workers, admins, outsourcers) to log in with their respective credentials. it also provides options for password recovery and account creation. Additionally, there are links to contact support and access the company's privacy policy and terms of service for transparency and compliance purposes.

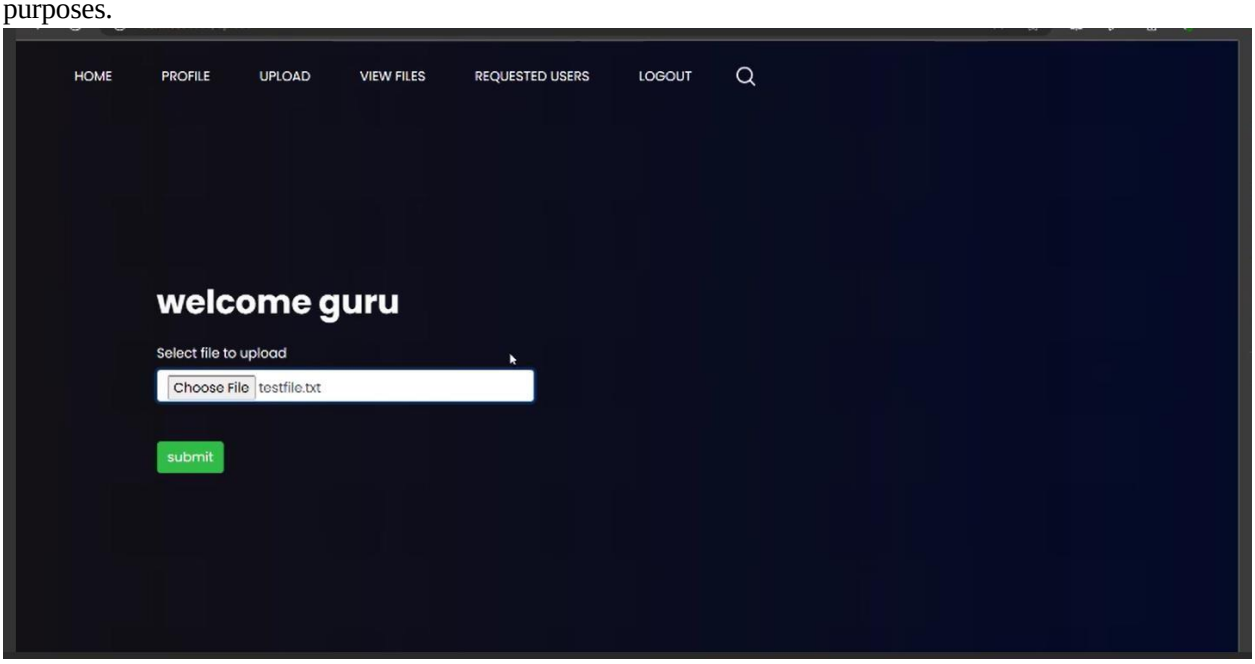

Fig: Outsourcer Page

As an outsourcer, you play a vital role in our operations. This portal is designed to streamline communication, manage projects, and ensure a seamless collaboration experience between you and our company.

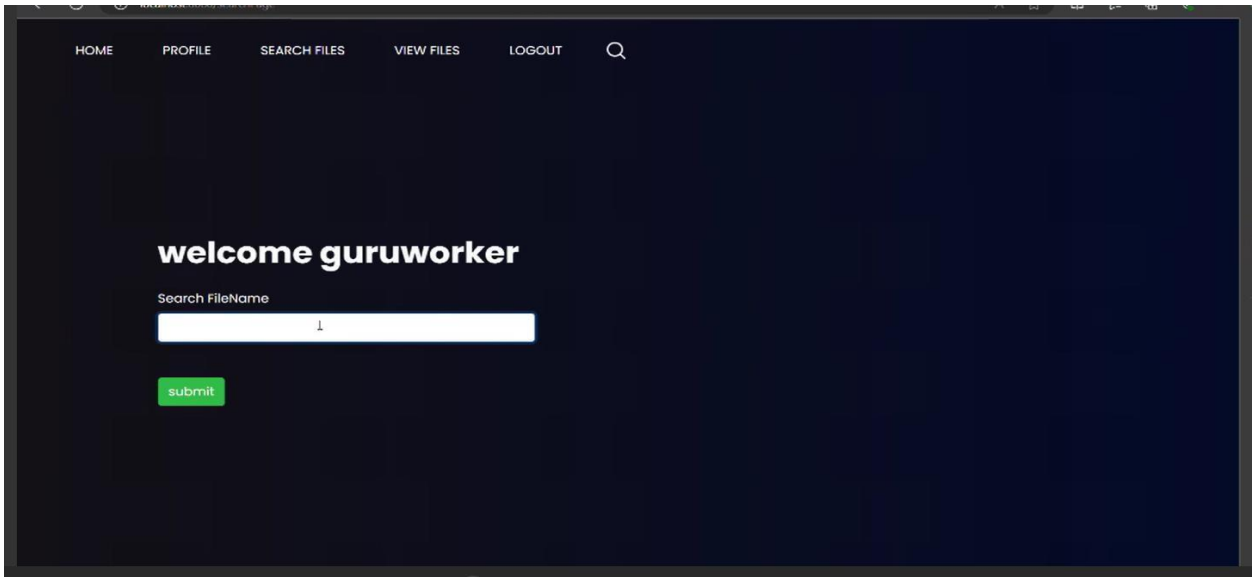

Fig: Worker Page

As a worker in our cloud computing environment, you are an integral part of our digital ecosystem. This platform empowers you to efficiently perform tasks, collaborate with teammates, and leverage cloud resources to drive innovation and productivity.

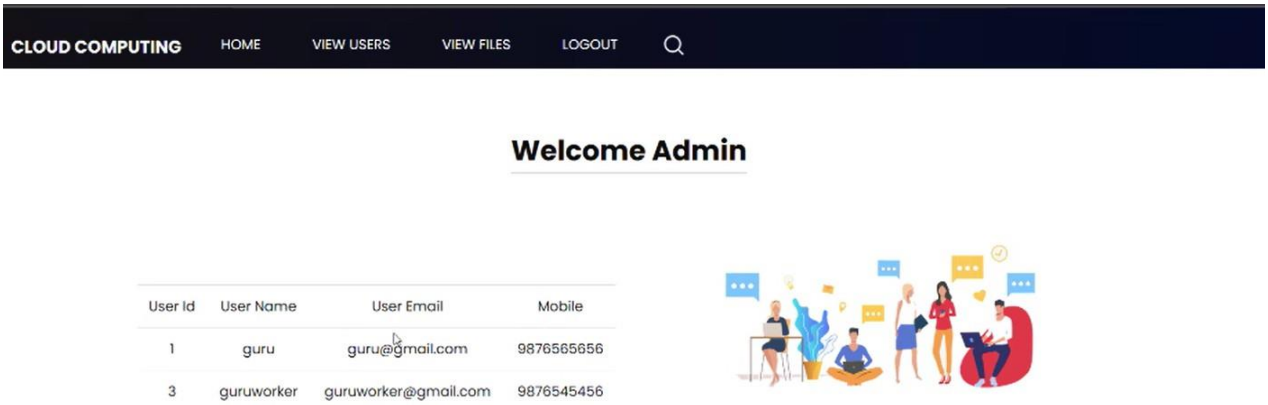

Fig: Admin Page

As an administrator, you play a crucial role in overseeing and managing our digital infrastructure. This dash board provides you with powerful tools and insights to efficiently monitor, control, and optimize our systems and resources

VI.CONCLUSION

We have described our proposed efficient block chain-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 (i.e., one-way accumulator, stealth address, symmetric encryption)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.

Deploying the smart contract on Remix environment to assess gas costs and analyzing communication and computing overheads, especially in comparison to existing solutions like OBFP, provides valuable insights into the efficiency and feasibility of your approach.

While your security and performance evaluations have indicated the potential utility of EFPB, collaborating with a real-world service provider for a prototype implementation and practical evaluation would be a significant next step. This real-world validation would provide invaluable feedback on the scalability, security, and usability of your scheme in actual deployment scenarios, helping to refine and improve its effectiveness.

FUTUREENHANCEMENT

Finally, we mention that we didn't take into account the communication overhead of SC since it obtains data directly from the local database. 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. Considering that you didn't incorporate the communication overhead of the smart contract (SC) in your evaluation, as it retrieves data directly from the local database, it's a commendable point that you've acknowledged. Collaborating with a real-world service provider for a prototype implementation and practical evaluation will offer an opportunity to assess the security and performance of your solution in a real-world environment, including the impact of communication overhead. This collaboration could reveal insights into how your scheme operates under real-world conditions,

helping to refine and optimize its performance for practical deployment scenarios. This real-world validation would provide invaluable feedback on the scalability, security, and us ability of your scheme in actual deployment scenarios, helping to refine and improve its effectiveness. By considering these additional aspects and focusing on continuous improvement and refinement, you can further enhance the effectiveness, security, and usability of your EFPB scheme for practical deployment in real-world cloud computing environments.

REFERENCES

1. H. Pagnia and F. C. Gartner, ‘‘on the impossibility of fair exchange without a trusted third party,’’ Darmstadt Univ. Technol., Darmstadt, Germany, Tech. Rep. TUD-BS-1999- 02.
2. A. Küpçü and A. Lysyanskaya, ‘‘Usable optimistic fair exchange,’’ in Proc. Cryptographers’ Track RSA Conf. Cham, Switzerland: Springer, 2010, pp. 252–267.
3. X. Chen, J. Li, and W. Susilo, ‘‘Efficient fair conditional payments for outsourcing computations,’’ IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1687–1694, Dec. 2012.
4. N.Asokan,M.Schunter,andM.Waidner,‘‘Optimisticprotocolsforfairexchange,’’in Proc. 4th ACM Conf. Comput. Commun. Secur., 1997, pp. 7–17.
5. Q.Huang,G.Yang,D.S.Wong,andW.Susilo,‘‘Ambiguousoptimisticfairexchange,’’ inProc.Int.Conf.TheoryAppl.Cryptol.Inf.Secur.Cham,Switzerland:Springer,2008,pp. 74–89.
6. M. T. Dashti, ‘‘Efficiency of optimistic fair exchange using trusted devices,’’ ACM Trans. Auto. Adapt. Syst., vol. 7, no. 1, pp. 1–18, Apr. 2012.
7. Q.Huang,G.Yang,D.S.Wong,andW.Susilo,‘‘Ambiguousoptimisticfairexchange: Definition and constructions,’’ Theor. Comput. Sci., vol. 562, pp. 177–193, Jan. 2015.
8. H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, ‘‘Bitcoin-based fair payments for outsourcing computations of fog devices,’’ Future Gener. Comput. Syst., vol. 78, pp. 850– 858, Jan. 2018.
9. L. Eckey, S. Faust, and B. Schlosser, ‘‘OptiSwap: Fast optimistic fair exchange,’’ in Proc. 15th ACM Asia Conf. Comput. Commun. Secur., Oct. 2020, pp. 543–557.
10. Y.Zhang,R.H.Deng,X.Liu,andD.Zheng,‘‘Outsourcingservicefairpaymentbased onblockchainanditsapplicationsincloudcomputing,’’IEEETrans.ServicesComput.,vol. 14, no. 4, pp. 1152–1166, Jul. 2021.
11. M. Campanelli, R. Gennaro, S. Goldfeder, and L. Nizzardo, ‘‘Zero knowledge contingentpaymentsrevisited:Attacksandpaymentsforservices,’’inProc.ACMSIGSAC Conf. Comput. Commun. Secur., Oct. 2017, pp. 229–243.
12. E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, ‘‘Scalable zero knowledge via cycles of elliptic curves,’’ Algorithmica, vol. 79, no. 4, pp. 1102–1160, Dec. 2017.
13. I.Giacomelli,J.Madsen,andC.Orlandi,‘‘ZKBoo:FasterzeroknowledgeforBoolean circuits,’’ in Proc. USENIX Secur. Symp., 2016, pp. 1069–1083.
14. A.Chiesa,E.Tromer,andM.Virza,‘‘Clustercomputinginzeroknowledge,’’inProc. Annu.Int.Conf.TheoryAppl.Cryptograph.Techn.Cham,Switzerland:Springer,2015,pp. 371–403.

Author's:

Mr. P.Chandrasekhar is working as Assistant Professor Department of Computer Science and Engineering at Guru Nanak Institute of Technology, Hyderabad. He completed his B.Tech CSE from Nagarjuna University, in 2011, M.Tech CSE with First Class from JNTU Kakinada University, in 2016, He has 5 years of teaching experience.

Mr.K. Suresh Babu is working as Assistant Professor Department of Computer Science and Engineering at PACE Institute of Technology and Sciences, Ongole. He completed his B.Tech Information Technology from JNTU Kakinada University, in 2012, M.Tech CSE with First class with Distinction from JNTU Kakinada University, in 2017, He has 6 Years of Teaching Experience.