Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 11070 – 11076

Research Article

Black Money Monitoring With Secured Cloud Data Storage With Big Data Analysis Using Block Chain

K.Thirumalarao*[1], Magesh Kumar[2]

Abstract

A challenge in such scenarios is that cloud vendors may offer varying and possibly incompatible ways to isolate and interconnect virtual machines located in different cloud networks. Our approach is tenant driven in the sense that the tenant provides its connectivity mechanism. We are implementing Blockchain concept in this project. We implement both Public and Private cloud data storage, Private is for sensitive data storage and public cloud normal data storage. We implement this concept for banking system, to identify overall user behaviour with personal identification. Integration of all his / her transactions like Banking, Land Registrations, Gold Purchase or any cash transactions more than Rs. 20k is accounted and monitored.

Keywords: Block chain, Cloud networks, Public and Private cloud data storage,Virtual machines

1. Introduction

The past few years this community has very well understood the benefits of this concept by transforming their applications to virtualized service offerings at a rapid pace. The benefits include easier and faster deployment of scientific applications, and the use of public cloud offerings for rapidly scaling out services. A hybrid cloud employs both a private and public cloud for rapid deployment of services. This is crucial for computationally demanding applications which require expedited scalability at global scale. As such hybrid clouds represent an opportunity for scientific applications as well. Organizations temporarily scaling-out their infrastructure from a private to a public cloud during peak hours, primarily have an economic advantage by eliminating any upfront cost for new hardware, and secondly reducing any administrative overhead with new resources introduced. Scientific applications are inherently complex and often have dependencies on legacy components that are difficult to provide or maintain. Thus, existing scientific applications should be virtualized in a backward compatibleway. In addition, utilizing hybrid clouds represent additional challenges, such as interoperabilitybetween different cloud vendors. The interoperability aspects include portability of virtual machines, crossvendor connectivity between virtual machines, and securing of computation, data and networks. In this paper, we touch "the tip of iceberg" and make some of the challenges more explicit, and show an approach for running virtualized scientific applications in a hybrid cloud setting. Our main contribution is in the design, implementation, evaluation and analysis of the proposed solution using a highly challenging scientific application that requires legacy components and secure connectivity in a distributed environment. The scientific application is a high energy physics grid software bundle that we have virtualized and ported to an OpenStack production environment.

2. Related Work

In paper [1], author Morgen PeckBlockchain, as an industry, has entered its Cambrian phase. A glut of investor interest has led to an explosion in the technical diversity of projects now underway. During the first half of 2017 alone, over one billion dollars was directed to the funding of blockchain start-ups.1 This money, which supports the development of competing technologies, is accelerating the speed of fragmentation in the industry. At the heart of the burgeoning innovation in the blockchain space is an undeniable contradiction: though the impulse to compete is at its peak, so too is the need for collaboration. Blockchain technology is poised to change nearly every facet of our digital lives, from the way we send money to the way we heat our homes. By obviating third parties, blockchains promise to make our systems more efficient. By circumventing censorship, they promise to make our systems more equitable. And if properly implemented, they could make our systems more reliable and secure.

In paper [2], authorFeng Tian and Tian Lan there is evidence that an increasing number of enterprises plot together to evade tax in an unperceived way. At the same time, the taxation information related data is a classic kind of big data. The issues challenge the effectiveness of traditional data mining-based tax evasion detection methods. To address this problem, we first investigate the classic tax evasion cases, and employ a graph-based method to characterize their property that describes two suspicious relationship trails with a same antecedent node behind an Interest Affiliated Transaction (IAT). Next, we propose a colored network-based model (CNBM) for characterizing economic behaviors, social relationships and the IATs between taxpayers, and generating a Taxpayer Interest Interacted Network (TPIIN). To accomplish the tax evasion detection task by discovering suspicious groups in a TPIIN, methods for building a patterns tree and matching component patterns are introduced and the completeness of the methods based on graph theory is presented. Then, we describe an experiment based on real data and a simulated network. The experimental results show that our proposed method greatly improvesthe efficiency of tax evasion detection, as well as providesa clear explanation of the tax evasion behaviors of taxpayer groups.

In paper [3], authorTodor Arpadwhile the 2016 Paris Agreement is in many ways an important attainment with the potential to represent a milestone in humanity’s path towards sustainable development, and avoid thus a potential calamitous and destructive future, the achievement of the goals set in the agreement is a long way off. This paper investigates one of the most important worldwide hurdles frustrating the implementation of the policies required to limit environmental degradation and limit pollution, namely the still insufficient public support for the necessary environmental policies and their associated cost. Using a comparative database generated through an experimental study on tax compliance and policy preferences run in five countries (USA, UK, Italy, Sweden and Romania), I will evaluate five explanatory models of the degree to which people support environmentally friendly policies by accepting higher tax burdens and increased collective solidarity.

In paper [4], author**:** Marten van Dijk cloud computing denotes an architectural shift toward thin clients and conveniently centralized provision of computing resources. Clients' lack of direct resource control in the cloud prompts concern about the potential for data privacy violations, particularly abuse or leakage of sensitive information by service providers. Cryptography is an oft-touted remedy. Among its most powerful primitives is fully homomorphic encryption (FHE), dubbed by some the field's "Holy Grail," and recently realized as a fully functional construct with seeming promise for cloud privacy. We argue that cryptography alone can't enforce the privacy demanded by common cloud computing services, even with such powerful tools as FHE. We formally define a hierarchy of natural classes of private cloud applications, and show that no cryptographic protocol can implement those classes where data is shared among clients. We posit that users of cloud services will also need to rely on other forms of privacy enforcement, such as tamperproof hardware, distributed computing, and complex trust ecosystems.

In paper [5], authorSatoshi Nakamoto purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3. SOURCES REQUIRED

3.1 USER REGISTRATION:

In this module we are going to create a User application by which the User is allowed to access the data from the Server. Here first the User wants to create an account and then only they are allowed to access the Network. Once the User create an account, they are to login into their account and request the Job from the Server. Based on the User's request, the service Provider will process the User requested Job and respond to them. All the User details will be stored in the Database.

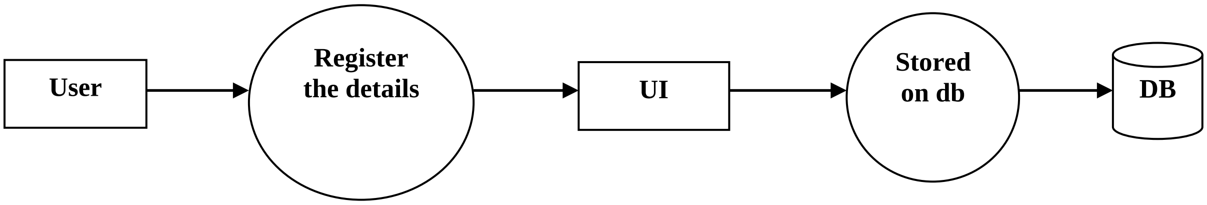


Fig 1. User Registration

3.2 BANK SERVER:

Bank Service Provider will contain information about the user in their Data Storage. Also the Bank Service provider will maintain the all the User information to authenticate when they want to login into their account. The User information will be stored in the Database of the Bank Service Provider. To communicate with the Client and with the other modules of the Company server, the Bank Server will establish connection between them. For this Purpose we are going to create a User Interface Frame.

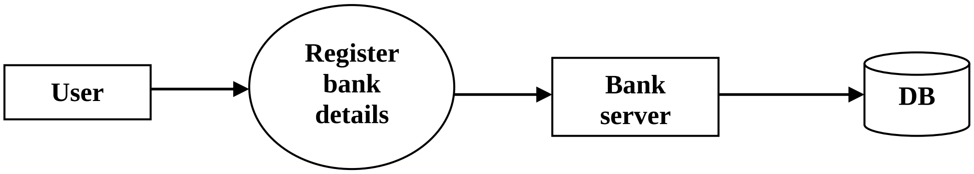


Fig 2. Bank Server Process

3.3 LAND REGISTRATION AND GOLD PURCHASE

In this module we implement land registration and purchased details to be monitor . Here, user name, land documents, price and selling price land. And also we monitor the gold purchase of every user and all other property details will be monitored based on user' Id.

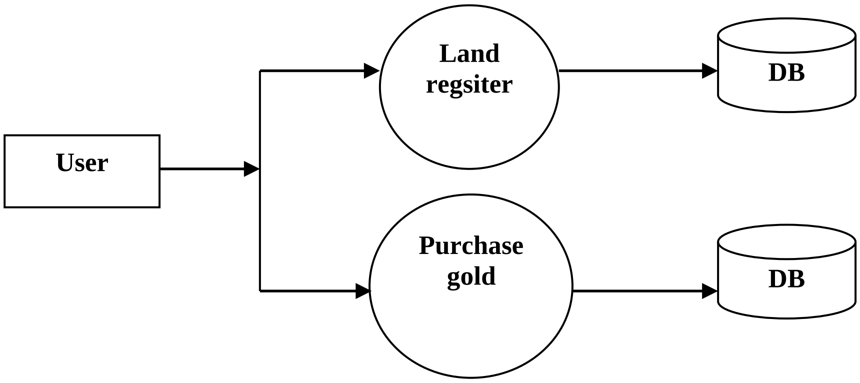


Fig 3. Land and Gold Purchase

3.4 CLOUD DEPLOYMENT

User 3.3will upload their data to the cloud server and request for a particular file is send to cloud server. To deploy our system we use dropbox cloud storage to store our details. Here we store sensitive and normal information on private and public cloud server respectively.

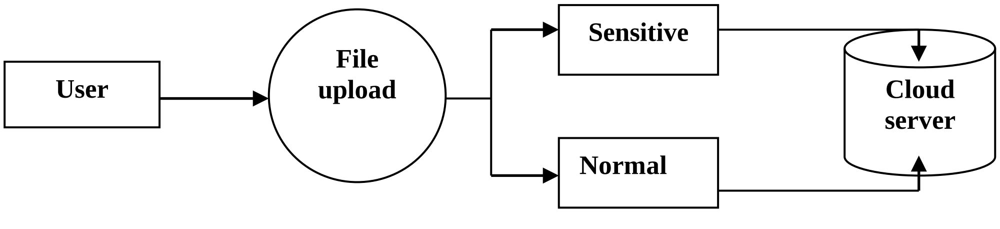


Fig 4. Cloud Deployment

3.5 BLOCKCHAIN DEPLOYMENT

A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificates number will be created as a block. For every block an hash code will generate for security. Here we store all transaction information like land purchase, gold purchase and all other purchasing details will stored on block chain. For every transaction we a block will create with hash code to refer the other block. Transaction detail will be more secure on block chain.

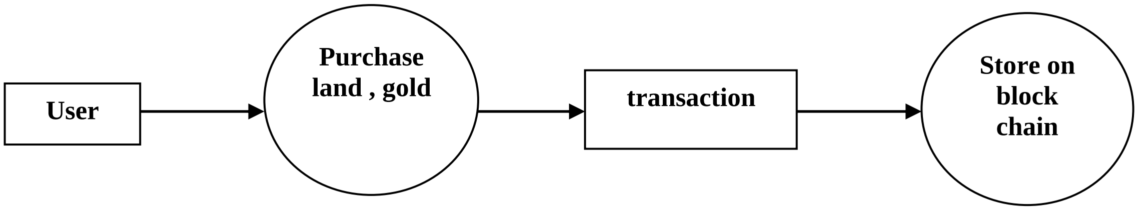


Fig 5. Block chain Deployment

3.6 BIGDATA ANALYSIS & BLACK MONEY NOTIFICATION

Throughout all transaction here we monitor proper payment of tax payment. Because, more number of forgeries were made on purchasing of land, people shows a fake price for land purchase and gold purchase. So, in this module we get the details of purchasing rate more than 20K. If user purchasing rate is increased more than 20K, system will alert the income tax notification to the user. Using aadhar number we can monitor all bank transaction also.

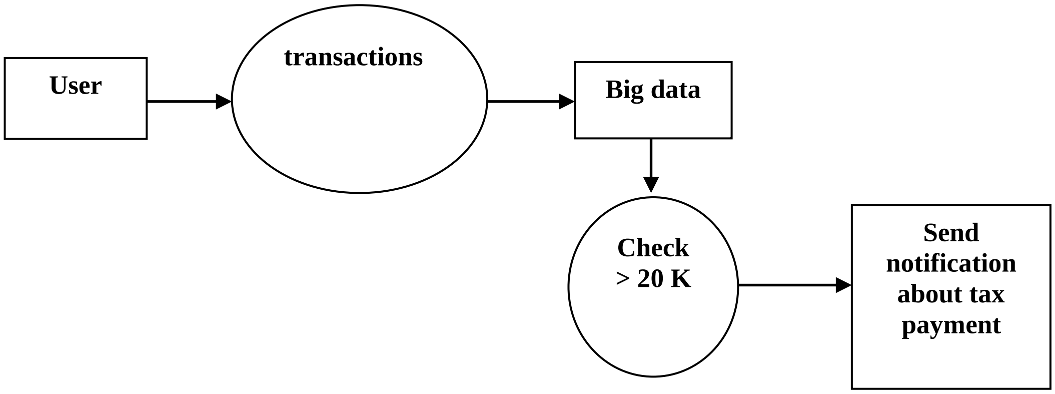
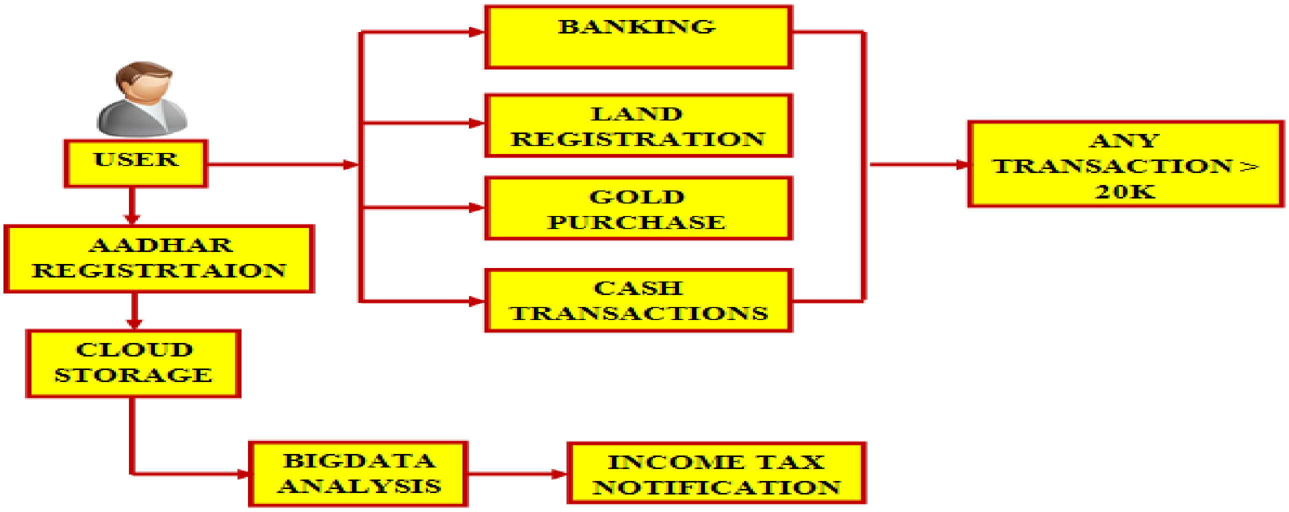


Fig 6. Black money notification

4. DESIGN

The Overall architecture explain about the entire process of project. User will register their basic information with their aadhar number and they made transaction on their bank account, purchase gold and land using their account. Those transaction information is stored on blockchain and cloud, but in cloud it will stored in three folder like gold, land and bank. Big data will analyze the those information using MapReduce and send those information to RBI what are the transaction are having more than 20K.



5. RESULTS

The experiments we tend to gift during this section check the detection aspects of the System and Network Analysis Engines (SAE and NAE respectively). Given the very fact that each engines perform online anomaly detection underneath the one-class SVM formulation we tend to at first gift our results associated with the process value of the web coaching and testing of the rule, since they affects the response of the realtime detection method. we tend to afterwards gift our assessment on detection the Kelihos and Zeus malware strains yet because the DDoS attacks. additionally, we tend to additional gift a comparison between the detection accuracy obtained once employing a joint dataset (i.e. composed of each system and network options) with a featureset that strictly considers network-based features. The experiments that specialize in the SAE practicality involve the detection of Kelihos and Zeus underneath static analysis and live-migration employing a twelve dimensional system-level dataset. NAE performance is tested underneath static analysis against DoS employing a nine dimensional network-level dataset and against Zeus victimization the 9 dimensional network dataset and a twenty one dimensional joint-level dataset

6. CONCLUSION

Thus the paper infer that we provide an tracking system while purchasing gold or any asset above 20k. Now a day's forgeries level is increasing in smarter way so to provide security we track the money using block chain technology.

7. REFERENCES

[1] A. Marnerides, C. James, A. Schaeffer, S. Sait, A. Mauthe, and H. Murthy, "Multi-level network resilience: Traffic analysis, anomaly detection and simulation," ICTACT Journal on Communication Technology, Special Issue on Next Generation Wireless Networks and Applications, vol. 2, pp. 345–356, June 2011.

[2] J. P. G. Sterbenz, D. Hutchison, E. K. C¸ etinkaya, A. Jabbar, J. P. Rohrer, M. Scholler, and P. Smith, "Resilience and survivability ¨ in communication networks: Strategies, principles, and survey of disciplines," Comput. Netw., vol. 54, no. 8, pp. 1245–1265, Jun. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet. 2010.03.005

[3] A. K. Marnerides, M. R. Watson, N. Shirazi, A. Mauthe, and D. Hutchison, "Malware analysis in cloud computing: Network and system characteristics," IEEE Globecom 2013, 2013.

[4] M. R. Watson, N. Shirazi, A. K. Marnerides, A. Mauthe, and D. Hutchison, "Towards a distributed, self-organizing approach to malware detection in cloud computing," 7th IFIP/IFISC IWSOS,

5] M. Garnaeva, "Kelihos/Hlux Botnet Returns with New Techniques." Securelist http://www.securelist.com/en/blog/655/ Kelihos Hlux botnet returns with new techniques.

[6] H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L. Wang, "On the analysis of the zeus botnet crimeware toolkit," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on, Aug 2010, pp. 31–38.

[7] T. Brewster, "GameOver Zeus returns: thieving malware rises a month after police actions," Guardian Newspaper, 11, July, 2014, http://www.theguardian.com/technology/2014/jul/ 11/gameover-zeus-criminal-malware-police-hacking.

[8] A. K. Marnerides, P. Spachos, P. Chatzimisios, and A. Mauthe, "Malware detection in the cloud under ensemble empirical model decomposition," in Proceedings of the 6th IEEE International Conference on Networking and Computing, 2015.

[9] L. Kaufman, "Data security in the world of cloud computing," Security Privacy, IEEE, vol. 7, no. 4, pp. 61–64, July 2009.

[10] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni, "Cloud security is not (just) virtualization security: A short paper," in Proceedings of the 2009 ACM Workshop on Cloud Computing Security, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 97–102. [Online]. Available: http://doi.acm.org/10.1145/1655008.1655022