ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

An Application for Online Corporate Elections Using Blockchain Technology

Ajitha S M[1], Nandhini R[2], Priya T[2], Saranya D[2], Sujitha K[2]

Assistant Professor, M.E Department of Information Technology, Meenakshi College of Engineering, Chennai, Tamilanadu, India [1]

B.Tech., Department of Information Technology, Meenakshi College of Engineering, Chennai, Tamilanadu, India[2]

ABSTRACT: A block chain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. For use as a distributed ledger, a block chain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although block chain records are not unalterable, block chains may be considered secure by design and exemplify a distributed computing system. An internet casting a ballot framework for Indian race is proposed without precedent. The proposed model has a more prominent security as in voter high security secret word is affirmed before the vote is acknowledged in the primary database of Election Commission of India. The extra element of the model is that the voter can affirm on the off chance that his/her vote has gone to address competitor/party. In this display an individual can likewise cast a ballot from outside of his/her dispensed voting public or from his/her favored area. In the proposed framework the counting of the votes will be finished naturally. Using block chain technique in the cloud server improves security as well as it implements our online voting system without malicious user.

KEYWORDS*:* Voting System, Block Chain, Online Voting, Election.

I. INTRODUCTION

nline voting is a modern technique used to avoid going to any physical polling station, instead voters only have to Ologin and put their votes. The process of voting online limits any expectations and can be easily violated so a strong maintaining supervision process must take place; our intelligent system verifies the results and gives expectations with respect to the relation of how similar the candidate is to the voter using fuzzy logic.

This relation is built by giving each voter and a candidate a unique fuzzy set representing his main characteristics and so these fuzzy numbers can be compared to get an estimation of similarity. The standard majority and fuzzy weighted-average voter with scores cases of two exclusive groups of voting techniques. One with an innovative level of safety yet with a low level of availability and the other with a low level of safety compare to the majority voting yet an innovative level of availability. As we are searching for a fuzzy set representation for the main characteristics of a person so we can acquire these information in two separate ways [1] implicitly by using the listeners to collect the data but may have some problems with the privacy policies so the second way is preferred [2] explicitly by a simple first time questionnaire in which you can get the information directly from the person and can modify it throw time by learning from persons actions and choices. After getting the desired information about each person a fuzzy number is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

set to represent this information as example on a scale of 1 to 5 a person is social, for this example a person may evaluate himself with 5 but throw time this number will be reduced as the system learns from the person behavior. Unless the resulting estimation gives 100% correct the voters' fuzzy set representing the characteristics should be changed according to the real-time votes they have done though a simple algorithm of calculating the average of the separate adjacent fuzzy numbers representing each characteristic, the candidate fuzzy set must be taken in count as not an absolute then it can be recounted according to each voter for the candidate or the average of the adjacent fuzzy numbers of all voters to this candidate.

II. SYSTEM ANALYSIS

A. Existing System Summary

The process of collecting data and entering this data into the database takes too much time and is expensive to conduct, for example, time and money is spent in printing data capture forms, in preparing registration stations together with human resources, and there after advertising the days set for registration process including sensitizing voters on the need for registration, as well as time spent on entering this data to the database. Existing communication protocols are insufficient for IoT Block chain applications. MQTT, which is a rather popular communication protocol for IoT, is used for this prototype. However, it requires a central MQTT broker, which is a single point for distribution of information. It makes systems vulnerable against attacks and break-downs. Block chain-based, de-central communication.

Disadvantages

- Too much paper work and paper storage which is difficult as papers become bulky with the population size.
- Not all people have free time during the given short period of time to check and update the voter register.
- The process of collecting data and entering this data into the database takes too much time and is expensive to conduct.

III. RELATED WORKS

In the year of 2018, the authors "Xuechao Yang, Xun Yi", proposed a paper titled: "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption", in that they described such as: Advanced security methods are necessary to introduce effective online voting (e-voting) in the whole world. Elections conducted on paper consume a lot of resources and contribute to the destruction of forests, which leads to climate deterioration. Recent online voting experiences in countries such as the United States, India and Brazil demonstrated that further research is needed to improve security guarantees for future elections, to ensure the confidentiality of votes and enable the verification of their integrity and validity. In this paper, we propose a ranked choice online voting system, which addresses these challenges. It eliminates all hardwired restrictions on the possible assignments of points to different candidates according to the voters' personal preferences. In order to protect the confidentiality of the votes, each cast ballot is encrypted using the exponential ElGamal cryptosystem before submission. Furthermore, during voting the system ensures that proofs are generated and stored for each element in the cast ballot. These proofs can then be used to verify the correctness and the eligibility of each ballot before counting without decrypting and accessing the content of the ballot. This validates the votes in the counting process and at the same time maintains confidentiality. The security and performance analyses included in this paper demonstrate that our method has achieved significant improvements in comparison with the previous systems. The outcomes of our experiments also show that our proposed protocols are feasible for practical implementations.

In the year of 2015, the authors "Saber Salehkaleybar, Arsalan Sharif-Nassab", proposed a paper titled: "Distributed Voting/Ranking with Optimal Number of States per Node", in that they described such as: Considering a network with

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

n nodes, where each node initially votes for one (or more) choices out of K possible choices, we present a Distributed Multi-choice Voting/Ranking (DMVR) algorithm to determine either the choice with maximum vote (the voting problem) or to rank all the choices in terms of their acquired votes (the ranking problem). The algorithm consolidates node votes across the network by updating the states of interacting nodes using two key operations; the union and the intersection. The proposed algorithm is simple, independent from network size, and easily scalable in terms of the number of choices K, using only K_2K□1 nodal states for voting, and K_K! nodal states for ranking. We prove the number of states to be optimal in the ranking case; this optimality is conjectured to also apply to the voting case. The time complexity of the algorithm is analyzed in complete graphs. We show that the time complexity for both ranking and voting is O(log(n)) for given vote percentages, and is inversely proportional to the minimum of the vote percentage differences among various choices.

In the year of 2017, the authors "Nirnimesh Ghose, Bocan Hu", proposed a paper titled: "Secure Physical Layer Voting", in that they described such as: Distributed wireless networks often employ voting to perform critical network functions such as fault-tolerant data fusion, cooperative sensing, and reaching consensus. Voting is implemented by sending messages to a fusion center or via direct message exchange between participants. However, the delay overhead of message-based voting can be prohibitive when numerous participants have to share the wireless channel in sequence, making it impractical for time critical applications. In this paper, we propose a fast PHY-layer voting scheme called PHYVOS, which significantly reduces the delay for collecting and tallying votes. In PHYVOS, wireless devices transmit their votes simultaneously by exploiting the subcarrier orthogonally of OFDM and without explicit messaging. Votes are realized by injecting energy to pre-assigned subcarriers. We show that PHYVOS is secure against adversaries that attempt to manipulate the voting outcome. Security is achieved without employing cryptography-based authentication and message integrity schemes. We analytically evaluate the voting robustness as a function of PHY layer parameters. We extend PHYVOS to operate in ad hoc groups, without the assistance of a fusion center. We discuss practical implementation challenges related to multi-device frequency and time synchronization and present a prototype implementation of PHYVOS on the USRP platform. We complement the implementation with larger scale simulations.

In the year of 2014, the authors "A. Bendahmane, M. Essaaidi", proposed a paper titled: "The Effectiveness of Reputation-based Voting for Collusion Tolerance in Large-Scale Grids", in that they described such as: Large scale grids permit to share grid resources spread over different autonomous administrative sites in the internet. The rapid progress of grid systems opens the door for numerous companies to adopt this technology in their business development. This progress is characterized by the increasing openness and opportunity of resource-sharing across organizations in different domains. In the business context, these shared resources can be misused by some malicious users that can abuse the provided resources and make them behave maliciously to return wrong results and sabotage the jobs execution. The common technique used by most grid systems to deal with this problem is based on replication with voting. Nevertheless, these techniques rely on the assumption that the grid resources behave independently. They may be ineffective where a number of collusive resources collectively return the same wrong results of a job execution. In order to overcome this threat, we propose a Reputation-Based Voting (RBV) approach, which investigates the trustworthiness of the grid resources through a reputation system, and then takes a decision about the results. In addition, the performance of our approach and other voting techniques, like m-first voting and credibility-based voting, are evaluated through simulation to perceive the effect of collusive grid resources on the correctness of the results. The obtained results show that our approach achieves a lower error rate and better performance in terms of overhead.

In the year of 2017, the authors "Lingling Xu, Yi Shen, and Hock Chuan Chan", proposed a paper titled: "Understanding Content Voting Based on Social Foraging Theory", in that they described such as: Why do people want to vote for or against content at some online communities and not at others? Social foraging theory, particularly research on insect and other animal information sharing behavior, offers a new perspective. Borrowing concepts from social foraging theory, this study proposes that four factors drive people's intention to vote online content (positively or negatively): 1) altruistic motives; 2) identification with the community; 3) information quality; and 4) knowledge self-efficacy. The research model was tested in a survey of online news communities. It found that positive voting intention

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

was predicted by altruistic motives, community identification, and knowledge self-efficacy. Information quality is important for positive voting, but it works indirectly through fostering stronger community identification. Negative voting intention was predicted by altruistic motives and information quality. Prior research has applied foraging theory to individuals acting alone, e.g., when an individual uses Google to search for information online. This study expands the application of foraging theory to the community context where individuals provide votes to influence others in their chosen community. The findings advance our knowledge about content voting and provide implications for practitioners of voting systems.

A. Proposed System Summary

A cloud database is a database that typically runs on a cloud computing platform, and access to the database is provided as-a-service. Database services take care of scalability and high availability of the database. Database services make the underlying software-stack transparent to the user. By making public cloud database, it will store all the required details in the cloud using block chain algorithm. More thorough and formal examination of the tradeoff between performance and data integrity guarantees is required to prove the efficacy of our design against the identified threats. It is worth finally noticing that our block chain-based database proposal, in this preliminary design, has been designed upon a total consensus mechanism. The approach surely permits to achieve integrity among the distributed replicas and to simplify the thread addressing. Block chain is a database or ledger that is shared across a network. This ledger is encrypted such that only authorized parties.

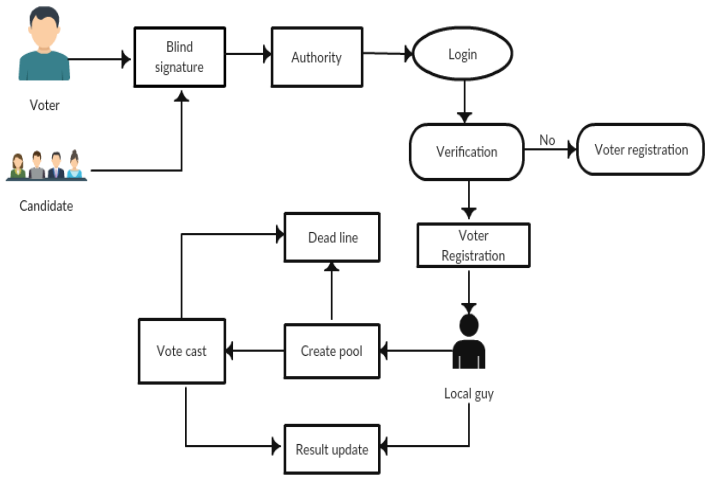

Fig.1 Proposed System Architecture

Advantages

- Time Saving
- Work Load Reduced
- Secure the data in the cloud with all possible.
- Improves technology to avoid malicious users.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

IV. SYSTEM IMPLEMENTATION

A. Employee and candidate Registration

Companies must now file the required information electronically, so it can be accessible to the public more quickly. Companies must also file a prospectus, which provides a summary of the company's share offering including the size, what the funds raised will be used for, and contact information for the company. Some securities are exempt from the SEC's registration process. These include limited and private offerings and municipal, state and federal security offerings. Employees of Company wants to enter Employee id, Employee name, date of birth , cell number, address, email Id etc.

B. Election and Candidate Details

Once employee and candidates filled relevant details those information's will be added into table. When the admin clicks details link a page id displayed with the election details in a grid like having the headings as election date, election name, election remarks, start time, end time. If we have to add new election details we have to click "Add Election Details". When the admin clicks the candidate details link a page is displayed with the candidate details having the headings as candidate image, election details, edit &delete. In the election details column there are some more fields like name, post, name, age & remarks.

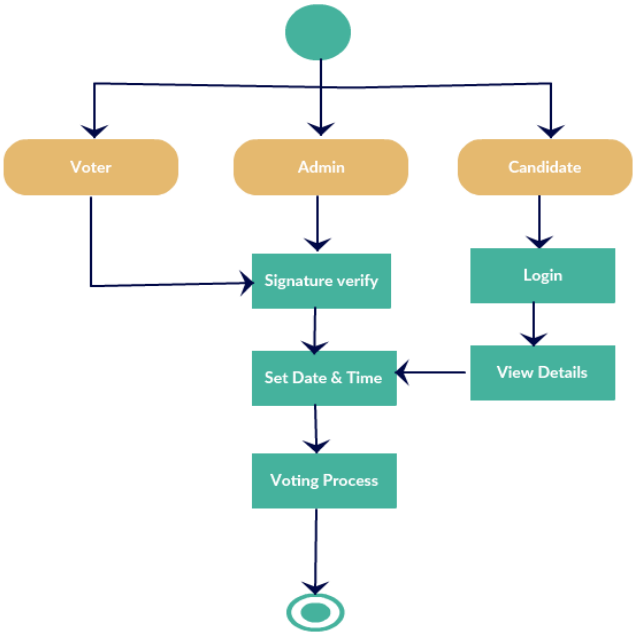

Fig.2 System Activity Illustrator

C. Polling and Login Phase

Before the election, the election officials need to generate and mail image transparencies to eligible voters. To generate them, they need a random number. A transparency is generated for each voter, using visual cryptography. In addition to the image, the transparency includes the password in a human-readable format. After generation of transparencies, the election officials send the generated transparencies and address list of eligible voters to a third party

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

who sends each eligible voter a randomly selected transparency along with a voter information packet including voting instructions. A voter visits the election website and enters the type able username. The election web site maintains a list of the username values used to generate the transparencies and checks that the entered key is on the list and has not been used already. If the entered username is valid, the election server can calculate the corresponding transparency image.

D. Image Authentication

The election server generates an image containing that string rendered as a bitmap image and the web server displays the corresponding image generated from username. Then the voter combines both the images.

E. Election Report Analysis

These processes authenticate the voter to the election server and the election server web site to the voter. Only someone with the correct username transparency could decode the password in the generated image. Only something with knowledge of transparency sent to the voter could generate a sensible password image.

F. DSA Key Generation

DSA is the US Govt approved signature scheme - designed to provide strong signatures without allowing easy use for encryption (they don't mind people having authenticated messages ... as long as they can read 'em!!) Needless to say, loopholes round have been found to do encryption. However the signature scheme has advantages, being both smaller (320 vs 1024bit) and faster (much of the computation is done modulo a 160 bit number) than RSA.

V. RESULTS AND DISCUSSION

The following figure, Fig.3 illustrates the Home Page view of the proposed system, in which this home page allows the user to navigate into the features in the proposed approach.

Fig.3 Home Page

The following figure, Fig.4 illustrates the Employee Registration view of the proposed system, in which this registration page allows the employee to register their identity into the system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

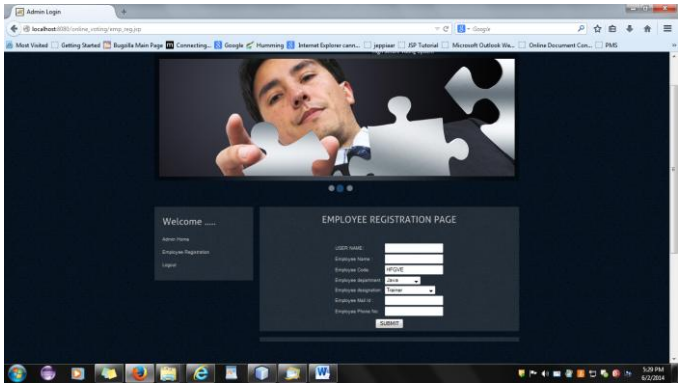

Fig.4 Employee Registration

The following figure, Fig.5 illustrates the Administrator Authentication Page view of the proposed system, in which it allows the Administrator to navigate into the main page, if the credentials are valid.

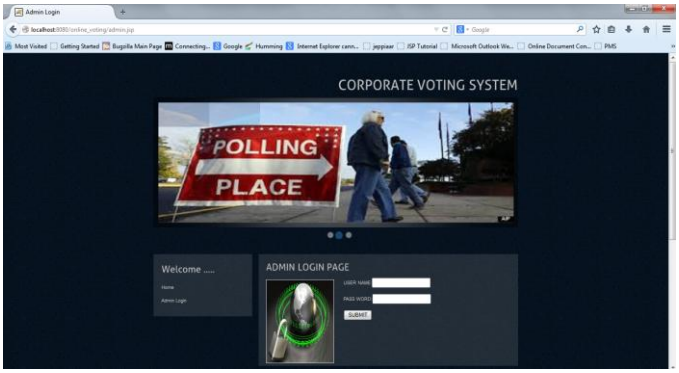

Fig.5 Administrator Authentication

The following figure, Fig.6 illustrates the Election Details View of the proposed system.

Fig.6 Election Details View

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

The following figure, Fig.7 illustrates the Voting Page view of the proposed system. By using this option, users can vote for the particular candidates and get the response from system accordingly.

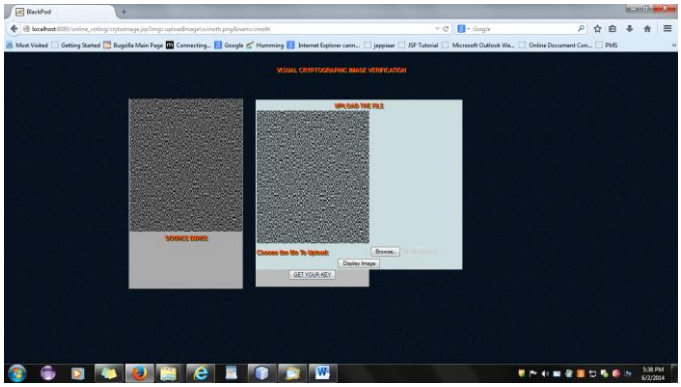

Fig.7 Voting Page

The following figure, Fig.8 illustrates the Voting Visual Key generation view of the proposed system.

Fig.8 Visual Key generation View

VI. CONCLUSION AND FUTURE SCOPE

Block chain applications have to be formally verified. A misuse of a smart contract for material replenishment can create a lot of damage in the supply chain. Recent hacks have shown that attacks on the overall Block chain application can be dangerous and costly. Therefore, it is necessary to develop techniques for formally verifying Block chain applications for supply chains. Secure online voting system that is free from unauthorized access while casting votes by the voters. The server aspects of the proposed system have such distribution of authority that server does not enable to manipulate the votes. It is expected that the proposed online voting system will increase the transparency and reliability of the existing electoral system. It is concluded that registering the voter's details in the cloud with block chain improves efficiency and avoids malicious users.

In this project, future enhancement document plays a vital role in the development life cycle as it describes the complete requirement of the system. It is meant for use by the developers and will be the basic during testing phase.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Any changes made to the requirements in the future will have to go through formal change approval process. It is a limitation of our system is that we have to assume that at least one authority is honest, since otherwise the system is not secure. In future work, we plan to address this issue and potentially could consider further generalizations.

REFERENCES

[1] Feng Bao, Robert H Deng, Xuhua Ding, and Yanjiang Yang. Private query on encrypted data in multi-user settings. In International Conference on Information Security Practice and Experience, pages 71– 85. Springer, 2008.
[2] John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07), pages 321–334. IEEE, 2007.
[3] Ian F Blake, Gadiel Seroussi, and NP Smart. Advances in elliptic curve cryptography, volume 317 of london mathematical society lecture note series. Cambridge University Press, Cambridge, 19(20):666, 2005.
[4] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identity based encryption with constant size ciphertext. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 440–456. Springer, 2005.
[5] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 506–522. Springer, 2004.
[6] Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. Contemporary Mathematics, 324(1):71–90, 2003.
[7] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Transactions on parallel and distributed systems, 25(1):222–233, 2014.
[8] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y Thomas Hou, and Hui Li. Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications, pages 226–234. IEEE, 2014.
[9] Zhihua Xia, Xiongfei Wang, Xinghua Sun, and Qijie Wang. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. 2015.
[10] Yanjiang Yang, Haibing Lu, and Jian Weng. Multi-user private keyword search for cloud computing. In Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, pages 264–271. IEEE, 2011.
[11] Qingji Zheng, Shouhuai Xu, and Giuseppe Ateniese. Vabks: verifiable attribute-based keyword search over outsourced encrypted data. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications, pages 522–530. IEEE, 2014.
[12] A. J. Feldman, W. P. Zeller, M. J. Freedman, and E. W. Felten, "Sporc: Group collaboration using untrusted cloud resources." in OSDI, vol. 10, 2010, pp. 337–350.
[13] F. Dabek, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Wide-area cooperative storage with cfs," in ACM SIGOPS Operating Systems Review, vol. 35, no. 5. ACM, 2001, pp. 202–215.
[14] L. P. Cox and B. D. Noble, "Samsara: Honor among thieves in peer-to-peer storage," ACM SIGOPS Operating Systems Review, vol. 37, no. 5, pp. 120–132, 2003.
[15] H. Zhuang, R. Rahman, and K. Aberer, "Decentralizing the cloud: How can small data centers cooperate?" in Peer-to-Peer Computing (P2P), 14-th IEEE International Conference on. Ieee, 2014, pp. 1–10.
[16] H. Zhuang, R. Rahman, P. Hui, and K. Aberer, "Storesim: Optimizing information leakage in multicloud storage services," in Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on. IEEE, 2015, pp. 379–386.
[17] S. Choy, B. Wong, G. Simon, and C. Rosenberg, "A hybrid edge-cloud architecture for reducing on-demand gaming latency," Multimedia Systems, pp. 1–17, 2014.
[18] T. Zou, R. Le Bras, M. V. Salles, A. Demers, and J. Gehrke, "Cloudia: a deployment advisor for public clouds," in Proceedings of the VLDB Endowment, vol. 6, no. 2. VLDB Endowment, 2012, pp. 121–132.
[19] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," Dependable and Secure Computing, IEEE Transactions on, vol. 10, no. 4, pp. 212–224, 2013.
[20] H. Harkous, R. Rahman, and K. Aberer, "C3p: Context-aware crowdsourced cloud privacy," in 14th Privacy Enhancing Technologies Symposium (PETS 2014), 2014.