International Journal of Engineering & Technology, 7 (2.7) (2018) 803-806

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Enhanced Security using Secure Multiparty Computation to E-voting application in cloud

Umang Kishor Chaudhari[1]*, A. Vijaya Kumar[2], G Venkata Sai[3]

[1,2,3]Computer Science & Engineering Department, (KLEF) K L University , Vaddeswaram , Andhra pradesh
**Corresponding author E-mail:umangchaudhari19@gmail.com*

Abstract

Secure outsourcing of computation on sensitive data is an important topic that has received a lot of attention recently. E-Voting system is interested in method collaboration system to ameliorate the quality of System. Cloud computing is integrating in communication and information technologies in the E-Voting. In fact, the paradigm is to provide the computational resources or result at the end of the services. Further it needs to reveal the voting information result but if faces several challenges in the security it must be overcome without reveal any sensitive data to unauthorized parties. To accomplish this objective, we proposed secure multiparty computation techniques (SMC). The main aim of our work is to use the suitable model for parties to together compute their function based on their inputs without revealing their private inputs. The idea behind is the several collaborate system use to their shared objectives without allow any gathering to information and private information.

Keywords: *Security; Cloud; Secure multiparty computation; E-voting; collaborative system.*

1. Introduction

Voting system in this modern era play the vital role of electing a leader in an organization. We vote the leader whom we want to get elected. It allows feeling the responsibility for making an organization a better place. In real time we elect our political leader by voting by putting ballets into ballet box. This is the time taking process and also involves in duplication of votes. As the Technology in today's world has been progressing in various aspects. The Information Technology industry is playing a vital role as it undertakes part in creating various projects that deals with real time applications. Where it eases the work load of any job which we intend of. Likewise, we can improve this system using the services IT industry. This will help us to provide a new scenario of E-Voting System. E-Voting System is the process which is used to elect the party leader form any place. But it would expose the identity of the voter and to who is casting the vote, by who is hosting the voting process. To avoid this, we are going to introduce the cloud computing which aim to deliver the security. This will help us the identity of the voter and to whom he had voted. And this will also not know to the computing system which is operating the computing system. Hence, distributed computing is the most proficient way for out sourcing the IT services.

In this new concept, E-voting system based upon cloud administrations to control the process of E-voting data rather than local data center. [1] The below figure 1 Outlines the important qualities and attributes of this model. There are numerous focal points, the moving of cloud computing rises the various provocations. Moreover, to share data among different parties to computation system cause major security and privacy concerns. In fact, the voter identity and votes are delicate information that requires to be guaranteed against unauthorized substances to overcome these challenges secure multiparty computation (SMC) technique is useful to propose the solution.

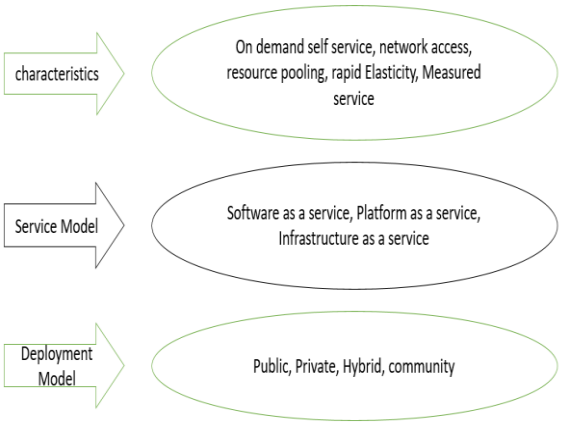


Fig. 1: Cloud computing definition

2. Cloud Computing

In this part, the outline of cloud computing, general definition with various parallel concept, and advantages of cloud computing. Cloud computing is the on-demand service, pool of resource which is easily able in the internet for user. [10] [11] Cloud computing is based on the sharing of resources which is use gain

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

economy of scale and the quality of being consistent and logical, comparative to a benefit.

2.1. Characteristics of cloud computing

Distributed computing gives numerous unmistakable highlights those are not quite the same as conventional framework. Multi-tenure: In this cloud condition, administrations claimed by various suppliers are situated to one single server farm. The common administration and execution issues will be shared among specialist co-op. Shared asset pooling: Resource pooling permits cloud supplier to give one pool of vast IT scale assets to serve numerous cloud shoppers. Distinctive assets will be relegated or reassigned by the cloud customer demand.

2.2. Benefit of cloud computing

Cloud causes you to study in major measure of information and in distinguishing any disparity. It gives system to upgrade the security and dependability of information. It Provides the space for free stage for the correspondence utilizing fast solid network with effective fast noticing power, so a client can work whenever shape any place using the webcast. It enables you to Increase and furthermore re-store the information. It is giving the quality administrations at the time of high load by using the quantity of resources. E voting application can speed up the use of cloud engineering that gives more intense server, CPU, more memory and quick stockpiling gadget.

3. Overview of Secure Multiparty Computation (SMC):

As a rule, SMC enables various frameworks to compute information upon their delicate data and reducing the danger of exposure. Therefore, it is a productive arrangement to guarantee security in the information sharing framework.

3.1 Fundamental of SMC

In general terms, a SMC will be outlined as a condition wherever number of parties though where consist of private inputs x1, x2 ..., xn are interested to compute the cost required function which is open (public) in such the least complex way that at the beat of the computation no party is learned any of the private inputs of elective parties [2][14].SMC idea was initial introduced by Yao in 1982 through the “millionaire problem” [3] and since then SMCs have being deployed in a very sort of applications like voting systems, auctions, business related private computations and privacy-preserving data mining, etc. on paper, a SMC is pictured with the existence of a trusted third party (TTP) that will the desired user intended multi-party computation. However, this is often much infeasible due to the very fact that an external entity cannot be trusted at hand over the private data of users. Therefore, SMC is all concerning finding appropriate cryptographic protocols which will replace the use of a TTP, to hold out a certain user intended function whereas ensuring data privacy of users [4]. The term cloud will be seen as a sweetening done to the net in terms of hardware virtualization and resource sharing. Cloud computing will be visualised as computing over net. A lot of precisely, it's a collection of resources and facilities offered to its users economically via the net [5]. A cloud makes it possible for its users to access their info within the cloud from anyplace, anytime through the net. On the opposite hand users don't need to worry about the maintenance and availability of resources, due to the very fact that it's the responsibility of the CSP. A lot of significantly cloud computing is an on-demand service, wherever users are charged solely supported their resource consumption. Due to such edges, cloud computing has become more and a lot of common among business entities. The most issue with most of the standard SMC protocols is that they incur a significant quantity of communication overhead affecting the potency of the protocol [6]. As an answer, it's potential to outsource the computations to a CSP which might facilitate to scale back the expenditure yet because the operational overhead. However, the issue that we confront is anyway we will authorize the security prerequisites of a multi-party calculation like information security, protection and secrecy; once we area unit managing an un-trusted external entity. This issue will be self-addressed through secure multi-party cloud computing solutions. To achieve the SMC goal, Ideal and Real model is suggested. In ideal model parties or a client’s send Private data to trusted third party (TTP), later return the input with function f to the client or parties.

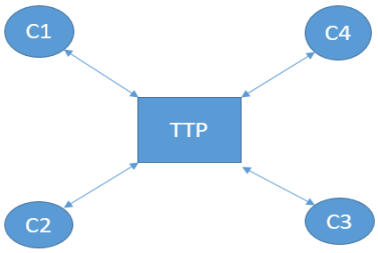


Fig. 2: Ideal Model.

In Real model, on Trust third party (TTP) is present, they participant with the run protocol and exchanging their message with each other as shown in figure 2

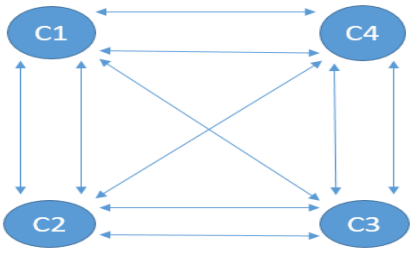


Fig. 3: Real Model.

3.2 Secure Multiparty Computation Background

3.2.1. Security Model

Security in multiparty calculation goes for considering dangers and issues associated with circumstance where an ill-disposed substance controls a few subsets of the sharing parties keeping in intellect the conclusion objective to attack the tradition execution. To this point, an arrangement of necessities should be considered when planning a multiparty calculation convention. In such manner, any protected convention must satisfy the accompanying prerequisites: security, rightness, freedom of data sources, ensured yield transfer and reasonableness. The last parameter implies that all gatherings ought to get their yields. Thus, it is essential to fea-

ture the energy of the rival who controls elements which took an interest in the protocol SMC. In this specific situation, three noteworthy parameters are utilized to distinguish the effect of the enemy on convention safety: debasement system, ill-disposed conduct and unpredictability.

3.2.2. Complexity

It is another factor that should be contemplated while actualizing the SMC Protocol. Officially, the time required for a problem to solve and unbounded are the two parameters that a rival can take. In the vital case, the equal utilizes time required for a computer for calculations in the middle of the tradition execution. All things considered, the enemy has no computational focuses of control in the computationally unbounded show.

3.2.3. Corruption Scheme

This approach goes for characterizing when and how parties are ruined because of the way that they go under the control of a foe. When all is said in done, there are two models in defilement technique. The First to begin with is called inactive in which undermined parties are set ahead of time. Conversely, the quantity of taking an interest element within the control of the enemy are subjectively put in the middle of the tradition execution in the versatile defilement demonstrate.

3.2.4. Adversarial

On the totally, this specification depicts behaviors of the undermined parties amid the running program. In the semi-honest ill-disposed demonstrate, all parties indeed debased one's take after convention determinations. Be that as it may, the debased parties can self-assertively veer off the protocol execution by taking after enlightening given by the enemy when it comes to the pernicious ill-disposed show.

4. Basic Primitives

4.1 Boolean Circuit

The standard point of view was acquainted by Yao by taking millionaire problem. [12] [13] to achieve these, he proposed an answer in view of Oblivious Transfer (OT) which is known as Garbled Circuit. These model, capacity of 'f' might be demonstrated and accomplish in a protection saving it as a Boolean circuit. Therefore, recommended system depends on mixed circuit assessment. [7] [8] [9] along these lines, one gathering makes the mixed circuit by and encoding the data sources, at that period of time several parties assesses mixed circuit.

4.2 Shamir Secret Sharing

Shamir Secret Sharing scheme technique is used in this the secret message is separated into the piece and circulated among the parties and some threshold value is chosen and just approved gathering combine, this technique is used in Distributed K-mean clustering where the parties are arranged in group which have the own secret value and share through this technique.

4.3. Secure Sum model

It is the extension of the secure sum protocol. k-secure sum protocol which is use to manage number of the segments,[13] where parties start the sending the segment from the protocol initiator and the flow will be continuous among the parties and the resulting sum will be announced by protocol initiator.

4.4. K-Secure Sum model

The another extension of the k- secure protocol is an Ck-secure sum protocol which is the segment is change when it is sending to neighbor parties or neighbor to each round of segment computation, which assure the no two parties learn data segment of the victim party.[13] Here parties are break into data blocks for the kth segment. As the same protocol initiator passes the segment to another but in this is an exchange in the position after each round, till the (ith) round and then at final round the protocol initiator will announce the sum.it is the advance technique of K- secure sum protocol.

5. Proposed E-Voting System Solution

It is to design a distributed process, E-voting system is a voting process, where the candidate votes for the parties to get majority party to win but it faces a few challenges while proceeding. In this zone, the security is a major calculate that piece the large acknowledgment in this area. The sensitive data should be confidential. Therefore, to overcome this problem we propose the SMC technique for proper solution. To proceed these, we are using AES encryption based on AES algorithm. Regarding these, each voter private data will successfully get encrypted and further proceed computations. Here the voters from various will get into process with the high secure function as captcha and get login, then the vote the parties, where in the data as voter id and the party to whom the candidate has voted will get encrypted using their private key and it will get store into the cloud server, and the final result is execute by the computation system without revealing the sensitive by itself as well as any other third parties. We conclude that these methods allow multiple voting system as well mutually to compute a work over their private inputs without appearing voter data. The below algorithm represents the step by step process of E-Voting System.

Process of E-Voting System.

Step1: Start.
Step2: Register the Candidate and store in Cloud.
Step3: Validate the Candidate Credentials.
Step4: If the candidate in valid
Proceed further to vote go to step5.
Else
Go to step2.
Step5: If the candidate is valid and voted.
Go to end step11.
Else
Proceed the voting process.
Step6: choose the party from options and vote.
Step7: Encrypt the vote and candidate Id and store in cloud.
Go to step 8.
Step8: Stop.
System Compute:
Step9: Enter the Valid password.
Step10: If the password valid
Display the number of vote to each parties
Else
Go to step9.
Step11: Stop.

To get the final computation result the votes will get decrypted in background and the count will be increase as the candidate's votes to the parties.

The summary of this whole technique is to secure the private data and perform the computation. Therefore it is an appropriate solution to get security in cloud environment.

6. Conclusion

Cloud computing is a leading area with an advance topic that aims to produce computational assets as services. Additional it is an approach to provide an appropriate result to improve the compute and security aspects in E-Voting application. With this judgment, SMC algorithms are used to guard voter identity and the vote privacy. So, the present paper proposed a structure established on the AES algorithm, where it's use to achieve data encryption. Therefore, it is providing the solution in an order of method to execute the process in the distributed database. It enables the voting system to jointly compute votes, calculate the total number vote for individual parties and show the result without uncovering any delicate data related to voter and to whom a candidate has voted.

References

[1] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).
[2] XU Guang-hui. Deploying and researching Hadoop in virtual machines[C]//Automation and provision (ICAL), 2012 IEEE International Conference on Zhengzhou, 2012: 395-399.
[3] LIUK. The security Analysis on Otway-Rees Protocol based on BAN Logic[C]. Computational and information Sciences (ICCIS), twenty urban center, 2012: 341-344.
[4] MUNIER M. Self-Protecting Documents for Cloud Storage Security[C]. Trust, Security and Privacy in Computing and Community, Liverpool, 2012: 1231- 1238
[5] SHAIKH FB. Security threats in cloud computing[C]. Internet Technology and Secured Transactions (ICIT, Abu Dhabi, 2011: 214-219.
[6] V. Winkler, "Securing the Cloud Computer: Security Techniques and tactics," Elsevier Inc., ISBN: 978-1-59749-592-9, 2011.
[7] Jian Feng Zhao "Research on Framework for Urban Railway massive data based on Cloud Computing Platform", 2014 IEEE.
[8] Lindell, Yehuda, and Benny Pinkas. "Secure multiparty computation for privacy-preserving data mining.
[9] Feigenbaum, Joan, Yuval Ishai, Tal Malkin, Kobbi Nissim, Martin J. Strauss, and Rebecca N. Wright. "Secure multiparty computation of approximations.
[10] Ishai, Y., Kushilevitz, E., Ostrovsky, R., & Sahai, A. (2007, June). Zero-knowledge from secure multiparty computation.
[11] Zhang, Q., Cheng, L. and Boutaba, R., 2010. Cloud computing: state-of-the-art and research challenges.
[12] Palugulla, M.R., Electronic-voting approach with an open cloud computing architecture.
[13] Yao, Andrew C. "Protocols for secure computations." In *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*, pp. 160-164. IEEE, 1982.
[14] Sheikh, Rashid, Beerendra Kumar, and Durgesh Kumar Mishra. "Changing Neighbors k Secure Sum Protocol for Secure Multi Party Computation.