International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 2, No 2, 2015. ISSN: 2348-6600
Reference ID: IJCS-101 PAGE NO: 580-582.

SECURE MULTIPARTY COMPUTATION FOR PRIVACY-PRESERVING CLOUD COMPUTING

S.Tamizharasi [#1], K. Ravikumar [*2]

[#1] *Research Scholar, Department of Computer Science, Tamil University, Thanjavur, India.*

[*2] *Asst.professor, Department of Computer Science, Tamil University, Thanjavur, India.*

[#1] stamilarasimphil1990@gmail.com

[*2] ravikasi2011@yahoo.com

***Abstract*— Secure multi-party computation (also known as secure computation or multi-party computation/MPC) is a subfield of cryptography with the objective to create methods for parties to equally compute a function more their inputs, and maintenance these inputs private [1].In this paper, we survey the basic paradigms and notions of secure multiparty computation and talk about their significance to the field of privacy-preserving data mining and cloud computing. In addition to reviewing definition and constructions for secure multiparty computation, we discuss the issue of efficiency and demonstrate the difficulties involved in constructing greatly efficient protocols. We also there common errors that are prevalent in the writing when secure multiparty computation techniques are useful to privacy-preserving data mining and cloud computing. Finally, we talk about the relationship among secure multiparty computation and privacy-preserving data mining and cloud computing [2].**

***Index Terms*— Secure Multiparty Computation (SMC), Cloud computing, privacy-preserving and data mining.**

I. INTRODUCTION

Secure computation was formally introduce as secure two-party computation (2PC) in 1982 by Andrew Yao,[3] the first recipient of the Knuth Prize. It is also referred to as Secure function estimate (SFE). The millionaire difficulty solution gave method to a generalization to multi-party protocols.[4][5] more and more efficient protocols for MPC have been future, and MPC can be now used as a realistic solution to various real-life problems such as spread voting, private bidding and auctions ,sharing of signature or decryption functions and private information recovery.[5] The first large-scale and realistic request of multiparty computation took place in Denmark in January 2008 [6].

Many enterprises and other organizations need to store and function on a huge amount of data. Cloud computing aims at renting such income on demand. Today's cloud providers offer together, extremely available and massively parallel computing with High Performance Computing (HPC) Clusters at fairly low costs[8].

II. LITERATURE REVIEW

Vaibhav Kumar et al [7].This research paper introduces a scheme to secure any secret value in cloud network by Mobile Proactive Secret Sharing (MPSS). This is an addition of proactive secret distribution, where causative parties of a network hold the shares of a secret value. Mobile proactive secret sharing is much suppler than proactive secret sharing in terms of set membership: instead of the group of share holders being accurately the same from one instance to the next, we allow the group to change randomly. In addition, we allow for an increase or decrease of the entrance at each instance.

Sven Bugiel et al [8]. In this paper we propose structural design for secure outsourcing of data and random computations to an untrusting product cloud. In our approach, the user communicates with a trusted cloud .which encrypts and verify the data stored and operations performed in the untrusting commodity cloud. We split the computations such that the trusted cloud is typically used for security-critical operations in the less time-critical setup phase, whereas

All Rights Reserved ©2015 International Journal of Computer Science (IJCS Journal)

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 2, No 2, 2015. ISSN: 2348-6600
Reference ID: IJCS-101 PAGE NO: 580-582.

queries to the outsourced data are processed in parallel by the fast product cloud on encrypted data.

Danish jamil et al [9]. This paper introduces four cloud security problems, which are XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and also gives the possible counter measures.

III.MULTI-PARTY COMPUTATION (MPC)

Secure multi-party computation (MPC) can be defined as the problem of n players to compute an agreed function of their inputs in a secure way, where security means guaranteeing the rightness of the output as well as the privacy of the players' inputs, even when some players cheat. Concretely, we assume we have inputs x1,...,xn, where player i knows xi, and we want to compute f(x1,...,xn) = (y1,...,yn) such that player i is guaranteed to learn yi, but can get nothing more than that. The most basic properties that a multi-party computation protocol aims to ensure are:

Input Privacy: The information resulting from the execution of the protocol should not allow any deduction of the private data held by the parties, except for what is exposed by the output of the function.

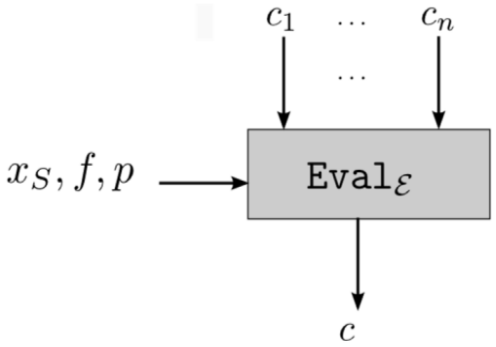
Correctness: Any correct subset of adversarial colluding parties ready to share information or deviate from the orders during the protocol execution should not be able to force truthful parties to output an wrong result.

IV.PRIVACY-PRESERVING CLOUD COMPUTING

Privacy preservation here to mean that S itself should learn no information starting any application execution, while choose clients should make limited output information[11]. The three classes, in order of growing generalization, are:

Private Single-Client Computing: These applications perform over the data xi of a given client Ci. Their access-control policy stipulates that only Ci may study any output. Note that an access-control policy restricting Ci's access to outputs isn't important:
Since xi belongs to Ci, revealing any function of xi to Ci leaks no information[11].

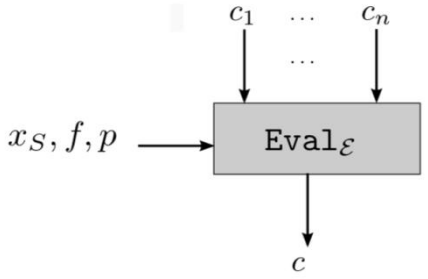
$$\text{if } \forall_i \; \exists_{x_i} \; [c_i = \texttt{Enc}_p(x_i)]$$



$$\text{then } c = \texttt{Enc}_p(f(x_S, x_1, \ldots, x_n))$$

Private Multi-Client Computing: These applications perform over the data {xi}n i=1 of multiple clients {Ci}n i=1. Since clients may not be mutually trusting (and might collude with S), a multi client application's access-control policy must stipulate release of information selectively to different clients[11]. Such release may be asymmetric, i.e., for a given f, Cj may be granted permission to learn f(xi,xj), while Ci isn't.

$$\text{if } \forall_i \; \exists_{p_i, x_i, A_i} \left[\begin{array}{l} c_i = \texttt{Enc}_{p_i}(x_i, A_i) \text{ with} \\ A_i(i, f, p) = \texttt{true} \end{array} \right]$$



$$\text{then } c = \texttt{Enc}_p(f(x_S, x_1, \ldots, x_n))$$

There are two new requirements[11]: **Access-controlled ciphertexts:** As computation takes place crossways multiple clients, it's significant that a client Ci be able to specify what functions may be computed on its private input xi. I arbitrary computation is allowable, and then xi itself may be exposed to all other clients (and a colluding S). We refer to this privacy condition as functional privacy[13].

All Rights Reserved ©2015 International Journal of Computer Science (IJCS Journal)
Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 2, No 2, 2015. ISSN: 2348-6600
Reference ID: IJCS-101 PAGE NO: 580-582.

Re-encryption: Privacy-protected transformation of a ciphertext below a key p 0 to a key p is required to enforce functional privacy. If then cryption keys p 0 and p are matching, then any client that can decrypt outputs can also decrypt and learn inputs, preventing any kind of access control[14].

Stateful private multi-client computing: These are private multi-client applications in which the access-control policy on a client's data is stateful, in the sense that it depends on the history of request execution by S [11].

V.CONCLUSION

Cryptographic protocols for secure computation realize remarkable results: it has been shown that general constructions can be used to compute several function strongly, and it has also been established that some functions can be computed even more capably using particular constructions. Believe that additional research in this area is crucial for the development of secure and efficient protocols in this field. Of course, this must go hand in hand with research on privacy in general and the question of what information leakage is acceptable and what is not.

VI.ACKNOWLEDGMENT

We would like to thanks all the reference authors for the completion of this paper.

VII.REFERENCES

[1].https://en.wikipedia.org/wiki /Secure Multiparty Computation.pdf
[2]. Yehuda Lindell and Benny Pinkas,. "Secure Multiparty Computation for Privacy-Preserving Data Mining" The Journal of Privacy and Confidentiality (2009) 1, Number 1, pp. 59–98.
[3]. Andrew C. Yao, Protocols for secure computations (extended abstract)
[4]D.Chaum,C.CrepeauandI.Damgard."Multipartyunconditionallysecureprotocols". .
[5]O.Goldreich,S.MicaliandA.Wigderson."How to play any mental game or a completeness theorem for protocols with honest majority". .
[6] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielse, Jakob Pagter, Michael Schwartzbach and Tomas Toft (2008). "Multiparty Computation Goes Live". nrm me clr atc(Report2008/068).
[7]. Vaibhav Kumar, R. P. Ojha, " Mobile Proactive Secret Sharing in Cloud Computing" IJRREST: International Journal of Research Review in Engineering Science and Technology (ISSN 2278- 6643) | Volume-1 Issue-2, September 2012 ,page no 67.
[8]. Twin Clouds: An Architecture for Secure Cloud Computing(Extended Abstract), Sven Bugiel, Stefan Nu¨rnberger, Ahmad-Reza Sadeghi, Thomas Schneider
[9]. Danish jamil et al. / international journal of engineering science and technology (ijest),"Security issues in cloud computing and countermeasures"
[10]. Secure Outsourced Computation in a Multi-tenant Cloud, Seny Kamara Microsoft Research senyk@microsoft.com,Mariana Raykova Columbia University mariana@cs.columbia.edu
[11]. On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing,Marten van Dijk RSA Laboratories marten.vandijk@rsa.com,Ari Juels RSA Laboratoriesajuels@rsa.com
[12].http://cs.uccs.edu/~cs691/studentproj/projM2011/halshamm/doc/Security%20Issues%20In%20Cloud%20Comuting.pdf
[13]http://www.journal-archieves14.webs.com/1323-1329.pdf
[14.]http://technofist.com/project%20list/cs/CloudComputing/AN%20EFFICIENT%20SECURITY%20MODEL%20IN%20CLOUD%20COMPUTING%20BASED%20ON%20SOFT%20COMPUTING%20TECHNIQUES.pdf

All Rights Reserved ©2015 International Journal of Computer Science (IJCS Journal)

Published by SK Research Group of Companies (SKRGC).