TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

Novel Advanced Security Computation over Secure and Dependable Services in Cloud Environment

M. Suresh Kumar[1], Dr. V. Nagalakshmi [2]

[1,2] Department of Computer Science, GITAM Institute of Science, GITAM (Deemed to be University)

Article Info
Volume 82
Page Number: 12585 - 12592
Publication Issue:
January - February 2020

Abstract

The implementation and development of cloud computing made the users think about data privacy with main obstacles which implies the implementation of cloud computing from other outside environment distributed sources. These types of concerns are operated by cloud service providers to provide privacy of sensitive data of different users stored in outsourced public data. Third party auditor (TPA) based security approaches are used to provide efficient privacy to user's sensitive data from outside attackers, computation of outsourced data with privacy preserving for user's data from inside malicious users in distributed environment. In order to provide efficient privacy preserving for outsourced publicly available data, we propose a Novel Security based Privacy Preserving Framework (NSPPF), which allows each user to outsource their data over multi dimensions functional protection from outsiders and insiders in distributed environment. In this framework, we use homomorphic based cryptographic system for encryption with partial decryption and Secure calculation for exponential data analysis which is the core sub-protocol in NSPPF. Our proposed framework describes the secure analysis of outsourced public data with private functions without loss of privacy to unauthorized users in distributed environment. Experimental evaluation of proposed approach describe efficient privacy in terms of communication and computation cost analysis in cloud computing.

Article History
Article Received: *18 May 2019*
Revised: *14 July 2019*
Accepted: *22 December 2019*
Publication: *24 February 2020*

Keywords; *Cloud computing, third party auditor, privacy preserving, outsourced data protection, private functionalities, outsourced computation and key sourcing.*

I. INTRODUCTION

In different types of outsourced business related organizations like e-commerce, Internet of Things (IOT), research related to scientific issues, cloud computing plays major role to store and outsource data to different users in distributed manner. Based on the basic nature of data sharing in cloud, it is classified as private, public and hybrid clouds, in which private and public clouds work within an organization while hybrid cloud is the combination of both private and public which describes on-demand premises. Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are the real time examples to store data in cloud computing manner. These services give huge amount of space for storage and describe customizable operations on storage data based on the responsibilities of different users for maintenance of data at storage and other related aspects. The users worry about their data at cloud service provider (CSP) for integrity checking and maintenance of different user's data. On the other hand, users may not outsource their data on local cloud where exists different incentives for cloud service provider to access user's data and cloud service provider also performs actions to hide data loss incidents. Therefore outsourced cloud data attracted technically and economically but needs data privacy i.e. data integrity to its enterprise and individual cloud servers in cloud computing.

Although functions relating to outsourcing data can certify and benefit to different users which contains

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

computational and communicational capabilities, but the user still hinges on managing, maintaining and understanding in flexibility of data representation and privacy and security challenges may appear as complex tasks in data sharing on distributed manner. Based on above mentioned privacy issues in outsourcing data on public and private multi-dimensional functionalities in cloud, we propose and a Novel Security based Privacy Preserving Framework (NSPPF), which allows each user to outsource their data over multi dimensions functional protection from outsiders and insiders in distributed environment. It also protects both multi dimensional functionalities on storage data based on user's input/output representation. Main contributions behind proposed approach as follows:

Propose NSPPF framework which describes outsourced computation over privacy preserving on multi accessible functionalities defined by each user in distributed environment. With proposed approach user's secure/sensitive information will not be accessed by third/ other users present in distributed environment. Enhance the NSPPF to advance secure functions to improve the performance.

Implement novel core related cryptographic approach i.e. homomorphic encryption with partial decryption procedure to perform multiplicative random encryption and decryption generations in distributed data sharing in cloud.

Implement secure exponential protocol for secure analysis of outsourced public data with private functions without loss of privacy to unauthorized users in distributed environment.

Explore the performance evaluation of proposed NSPFF with efficient simulated results in terms of encryption time, token generation time, decryption time, user access time and others in communications via distributed environment.

II. REVIEW OF LITERATURE

This section describes about different security approaches used in cloud via third party auditor and other security aspects. In other related work, M.A. Shah et al. [2] planned to guarantee information ownership of various reproductions over the circulated capacity framework. They broadened the PDP plot to cover various reproductions without encoding every copy independently, giving assurance that various duplicates of information are really kept up. M.A. Shah and R. Swaminathan et.al [3] proposed to check information respectability utilizing RSA-based hash to exhibit non cheatable information ownership in distributed record sharing systems. In any case, their proposition requires exponentiation over the whole information record, which is obviously illogical for the server at whatever point the record is huge. Ximeng Liu et al. [5] proposed enabling a TPA to keep online capacity legit by first encoding the information at that point sending various pre-computed symmetric-keyed hashes over the scrambled information. B. Chamberlin et.al [8] embraced a few thoughts of their dispersed stockpiling check convention. R. Lu, H. Zhu et al. [12] introduced a Point to Point reinforcement plot in which squares of an information record are scattered crosswise over m þ k peers utilizing a (m; k)-deletion code. Companions can demand arbitrary squares from their reinforcement peers what's more, confirm the uprightness utilizing separate keyed cryptographic hashes appended on each square. Their plan can identify information misfortune from free-riding peers, yet does not guarantee that all the information is unaltered. C. Gentry et.al [13] proposed to guarantee static record honesty over numerous dispersed servers, utilizing deletion coding and square level record trustworthiness checks. S. Kamara et al. [17] gave a study on many existing arrangements on remote information respectability checking, and examined their advantages and disadvantages under various structure situations of secure distributed storage administrations.

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

III. BASIC NOTATIONS USED IN IMPLEMENTATION

In this section, we describe the basic procedures with respect to homomorphic encryption and secure exponential parameters used in proposed approach and discussed in literature. Main notations are described in table 1.

a. Preliminaries related to homomorphic cryptosystems

Basically partial homomorphic encryption and decryption follows multiplicative homomorphic cryptosystems, let us consider $E_{pk+}(m1)\,\&\,E_{pk+}(m2)$ are the two basic cipher text related cryptosystems under public key with properties of additive homomorphic as

$$D_{sk+}(E_{pk+}(m1).E_{pk+}(m2)) = m_1 + m_2$$

If cipher text operations are multiplicative homomorphic representation as follows:

$$D_{sk^{\times}}(E_{pk^{\times}}(m1).E_{pk^{\times}}(m2)) = m_1.m_2$$

Symbol	Definition
pk^{+}, sk^{+}	Additive homomorphic (ADD) public & private key
$pk^{\times}, sk^{\times}$	Multiplicative homomorphic (MUL) public & private key
$E_{pk^{+}}(\cdot)$	ADD encryption algorithm with ADD public key
$E_{pk^{\times}}(\cdot)$	MUL encryption algorithm with MUL public key
$(a\|p)$	Legendre symbol (odd prime p and an integer a)
$(a\|n)$	Jacobi symbol (two integer a and n)
$\mathcal{F}, \mathcal{F}', \mathcal{F}''$	The outsourced function
$\vec{\mathbf{C}}$	A plaintext vector $\vec{\mathbf{C}} = (C_1, \cdots, C_n)$
$\vec{\mathbf{C}}^{E+}$	An ADD encrypted vector $\vec{\mathbf{C}}^{E+} = (E_{pk^{+}}(C_1), \cdots, E_{pk^{+}}(C_n))$
$\vec{\mathbf{C}}^{E\times}$	A MUL encrypted vector $\vec{\mathbf{C}}^{E\times} = (E_{pk^{\times}}(C_1), \cdots, E_{pk^{\times}}(C_n))$
$a \cdot b$	Multiplication between a and b over cyclic group

Table 1. Basic notations used in proposed approach

b. Cryptographic Homomorphic switchable preliminaries

It describes the relation between server and client to transform additive homomorphic operations into multiplicative cryptographic related homomorphic cipher text and act as vice versa described in [7-9]. Preliminaries as follows

GenOfKey: Let us consider security parameters k with regressive prime numbers p,q $p = 2p' + 1 \,\&\, q = 2p' + 1 \,\&\, |p| = |q| = k$,define key generator g which describes the random numbers then based on odd prime numbers with respect to public-private key pairs as follows

$$\{pk^{+}; sk^{+}\} := \{N; (\lambda, p, q)\},$$
$$\{pk^{\times}; sk^{\times}\} := \{N, g, h); \theta\}$$

Encryption w.r.t. Add primitive and multiplicative: It takes public key as i/p and transmitted message i.e. files/records and others then random encrypted key process as follows:

$$E_{pk+}(m) = (1+N)^{m}.r^{'N^{i}} \bmod N^2$$

Primitive multiplicative encryption as follows:

$$E_{pk+}(m) = \{C_1, C_2\} = \{m.h^{r}, g^{r} \bmod N\}$$

Combine additive /multiplicative operations: This is completely run and authorized by server, output cipher text as follows:

$$E_{pk^{+}, pk^{\times}(m)} = \left\{(1+N)^{mh^{r}}, r^{'N} \bmod N^2, g^{r} \bmod N\right\}$$

Computation of proxy server communication (T_1, c_1, c_2) with respect to different proxy computes, then cipher text with combined recovery files

$$(T_1^{'}) = E_{pk^{+}}(mh^{-s}.h^{s}) = E_{pk^{+}}(m)$$

Basic key notations to describe cloud storage processing with secure auditing describes in figure 1.

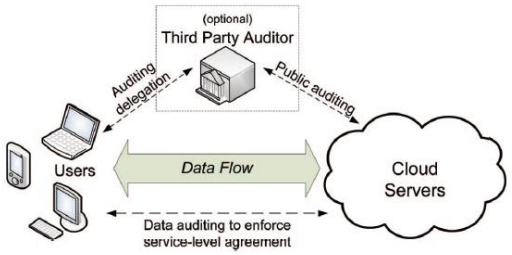

Figure 1 Description of secure cloud storage system via different users

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

c. Basic Adversary Problem Description

In cloud information stockpiling framework, clients store their information in the cloud and never again have the information locally. In this way, the rightness and accessibility of the information records being put away on the dispersed cloud servers must be ensured [14-16]. One of the key issues is to adequately distinguish any unapproved information adjustment and debasement, perhaps because of server bargain as well as irregular Byzantine disappointments. In addition, in the dispersed situation when such irregularities are effectively recognized, to discover which server the information mistake lies in is likewise of incredible essentialness, since it can generally be the initial step to quick recoup the capacity blunders and additionally distinguishing potential dangers of outside assaults.

IV. PROPOSED MODEL

This section defines the description of basic security model used in this implementation and it is described in figure 2.

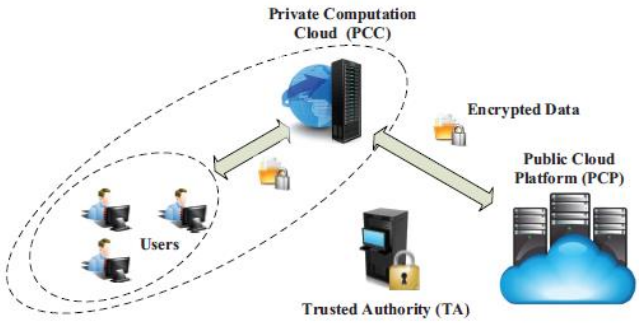

Figure2. Architecture of proposed cloud security model

Above figure consist of four components, i.e. clients, trusted authority (TA), Platform cloud relates to public (PCP) and Private related cloud computation (PCC). Trusted authorities verify each entity to maintain and manage all the keys, user details involved in distributed environment.

Main task of the user is to compute secure outsourcing results based on their choice with respective functionalities, if any user sends query to PCP describes in privacy preserving conditions, then PCP verifies each instruction and then send back to user, encrypted results can be decrypted by only PCC which means without PCC authorization user can't access data.

PCC describes computational services to user, it can be used to process encrypted with respect to additive/multiplicative over encrypted cloud data. And also PCC has to ability to decrypt cipher texts received from PCP using public keys of different users in distributed environment.

PCP stores unlimited data of different users which stores and manage all the publicly available data, PCP also stores intermediate final result of the encrypted data. Furthermore PCP performs some capacity related operations over encrypted cloud data.

In proposed approach, let us consider D be the data set which consists different dimensions $\{x_1, x_2, ..., x_\gamma\}$, $\forall$ each file of different users performs all secure and unsecure related functions, output of user's function as follows:

$$F : o = \sum_{j=1}^{k} C_j x_1^{t_{j,1}}, ..., x_\gamma^{t_{j,\gamma}}, ^2$$

Basic description of this function can be used to perform and process statistical analysis, if any user describes mean $\ddot{x} = \left(\sum_{i=1}^{\gamma} x_i\right)/\gamma$ across different functional notations and calculate the standard deviation $\sigma = \sqrt{\frac{1}{\gamma \sum_i^{\gamma} (x_i - \bar{x})^2}}$ with different polynomial equations representations.

Proposed Privacy Model

In our implemented privacy model TA generates different public/private related keys and distributes those keys to associate users in distributed environment. PCP and PCC are the honest with respect to curious in user security with private and

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

public user's encryption and decryption data with user privacy, separation of privilege and transmit data in secure format. Satisfy all these requirements with secure adversary requirements in NSPPF framework discussed in next section.

V. PROPOSED NSPPF DISTRIBUTED FRAMEWORK

In this section, we describe the basic procedure of NSPPF in implementation of privacy preserving with different notations in distributed environment. Our proposed approach consists following methods to provide security/privacy for multi user interaction in cloud.

a. Homomorphic encryption with partial decryption (HEPD)

In order to implementation of NSPPF, we use novel cryptosystem i.e. homomorphic encryption with partial decryption based on searchable encryption with homomorphic relations, it consists AddEnc, AddDec, MulEnc, MulDec, AddToMix and MixToAdd with corresponding relations in data encryption and decryption. Procedure of HEPO describes in preliminaries with additive encryption & decryption, multiplicative encryption & decryption with corresponding calculation.

b. Key Distribution in NSPPF

After completion of above steps in construction of user interface for encryption and decryption of user's files. Before implementation of NSPPF key distribution is the main factor to explore user to corresponding user communication in distributed environment. Based on privacy model of NSPPF, one PCC and PCP involved in NSPPF.

Trusted authority firstly runs KeyGen to explore additive for public key i.e. $pk_i^+ = N_i$ each user with associated private keys $sk_i^+ := \left(\lambda_{i,1}, \lambda_{i,2,p_i,q_i}\right)(\forall i = 1,....,\beta)$ and then multiplicative private keys $sk_i^\times = \theta_i \bmod N_i \exists N_i$ corresponding trusted authority check multiplicative public keys $pk_i^\times = (N_i, g_i, h_i)$. Pair of Add, Mul i.e. $\left(pk_i^+, pk_i^\times\right)_{i=1,2,.....,\beta}$ corresponding user interactions, and also θ_i requires partial MUL, ADD private keys i.e. $\left(\theta_{i,1}, \theta_{i,2}\right)$ sent to PCP while associated decrypted keys sent to PCC respectively. Partial decryption with primitive private key $\lambda_{i,1}$ are sent to PCC while running different parties relates to data storage of each user respectively. No intermediate users required for other parties data to encryption and decryption, directly sent to PCC cloud storage system, Main assumption behind partial ADD/MUL private keys PCC directly decrypt the encrypted content, after completion of this procedure NSPPF will be executed with efficient generation of privacy aspects in distributed environment.

c. NSPPF Privacy Level

Outsourcing function of NSPPF privacy model describes different co-efficient with respect to encryption, once user upload data then encrypted co-efficient i.e. $E_{pk_a} + (C_i)$ with secure functionalities $x_1^{t_{j,1}}, x_1^{t_{j,2}}, ..., x_\gamma^{t_{j,\gamma}} (j = 1,2,....., k)$ should be outsourced to PCP, PCP calculates monomial secure representation for updated data $\square_j x_1^{t_{j,1}}, ..., x_\gamma^{t_{j,\gamma}}$. For all user's data stored in PCP in plain text format $\vec{a}_i = (a_{i,1}, a, ...a_{i,\gamma})$ then encrypted content in PCP i.e. $a_{i,1}^{t_{j,1}}, ..., a_{i,\gamma}^{t_{j,\gamma}} \left(i = 1,....., \tau;; j = 1,.....\kappa\right)$ can be evaluated monomial secure functions as described as follows:

$$E_{pk_\alpha^+}\left(C_j\right)^{a_{i,1}^{t_{j,1}}, ..., a_{i,\gamma}^{t_{j,\gamma}}} = E_{pk_\alpha^+}\left(C_j a_{i,1}^{t_{j,1}}, ..., a_{i,\gamma}^{t_{j,\gamma}}\right)$$

Used for processing other sequences in terms of privacy preserving in distributed environment. Once secure monomial calculation completed then PCP requires $E_{pk_\alpha^+}\left(C_j a_{i,1}^{t_{j,1}}, ..., a_{i,\gamma}^{t_{j,\gamma}}\right)$ computing encrypted

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

results $E_{pk_\alpha^+}(o_j)$ for every user i to secure outsourced function. Because of homomorphic relation of encryption with partial decryption can be achieved for cipher text as described as follows:

$$E_{pk_\alpha^+}(o_j) = E_{pk_\alpha^+}\left(\sum_{j=1}^{k} C_j a_{i,1}^{t_{j,1}}, \ldots\ldots, a_{i,\gamma}^{t_{j,\gamma}}\right)$$

After completion of these steps, decrypted results are downloaded by user i. NSPPF efficiently outsourced secure data over different user's protection in distributed environment.

VI. PERFORMANCE ANALYSIS

In this section, we describe performance evaluation of NSPPF in terms of communication and computation overhead in distributed environment. We use JAVA and Net Beans latest version for simulate the results, these experiments runs on latest i3-i5 processor with suitable RAM and Hard Disk. Real time user data can be used to test our application in data sharing between different users with secure communication and computation costs.

Following figures show the performance of proposed approach with respect to response time, encryption time, decryption time, average precision in matrix accuracy and memory for user uploaded requests in the form of files and user input details in cloud data security. Table 2 represents the time for different user instances data sharing in cloud.

No. of User Instances	Flexible Distributed Storage Integrity Auditing Mechanism (FDSIAM) [1]	Privacy-Preserving Human Tracking Scheme (PPHTS) [11]	Homomorphic Cryptographic System (HCS) [15]	Proposed approach
10	4.3	3.7	3.6	1.9
30	5.4	4.8	5.2	3.4
50	6.4	5.4	4.6	3.7
70	7.3	6.2	7.1	4.6
100	8.6	7.4	6.3	7.3

Table 2. Different user instance values with respect to time

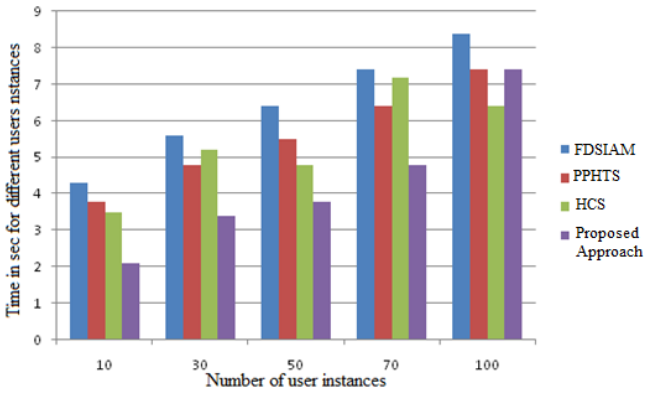

Figure 3 Total time taken for different approaches in cloud data storage setup.

Table 3 shows encryption time with service requests done by users to upload data into cloud storage in encrypted format with different notations.

No. of User Instances	Flexible Distributed Storage Integrity Auditing Mechanism (FDSIAM) [1]	Privacy-Preserving Human Tracking Scheme (PPHTS) [11]	Homomorphic Cryptographic System (HCS) [15]	Proposed approach
100	4.3	3.7	3.6	3.5
200	5.4	4.8	5.2	4.1
300	6.4	6.7	5.2	4.3
400	7.3	6.2	7.1	4.6
500	8.6	7.4	6.3	7.3

Table 3. Different values for user request instances

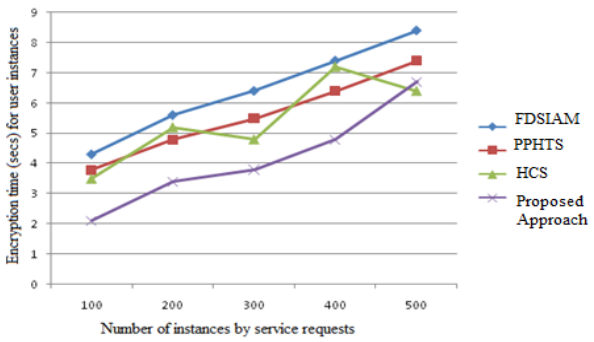

Figure 4 Encryption time with different user service instances.

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

Decryption time with different user request instances to access data from multi cloud storage show in table 4

No. of User Instances	Flexible Distributed Storage Integrity Auditing Mechanism (FDSIAM) [1]	Privacy-Preserving Human Tracking Scheme (PPHTS) [11]	Homomorphic Cryptographic System (HCS) [15]	Proposed approach
100	3.7	4.7	4.2	3.8
200	4.2	5.6	4.8	3.6
300	3.7	7.4	5.3	4.3
400	6.3	5.82	4.6	4.7
500	5.7	6.4	6.8	5.3

Table 4. Description time values

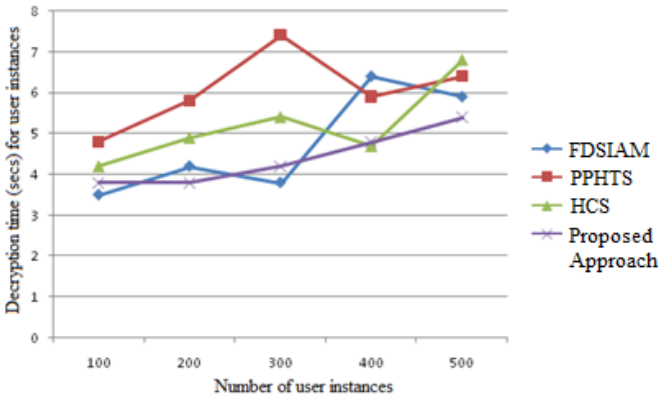

Figure 5 Decryption time with different users instance from encryption.

Figures from 3-5 show the performance with respect to total time, encryption, decryption time with different user instances, Proposed approach gives better performance than traditional approaches like SAML Flexible Distributed Storage Integrity Auditing Mechanism (FDSIAM) [1], Privacy-Preserving Human Tracking Scheme (PPHTS) [11], Homomorphic Cryptographic System (HCS) [15] designed in secured cloud storage environment.

CONCLUSION

In this paper, we propose a Novel Security based Privacy Preserving Framework (NSPPF), which allows each user to outsource their data over multi dimensions functional protection from outsiders and insiders in distributed environment. NSPPF enable identify based user security for outsourced computation of security without compromising the user security with effective privacy results. Main key points present in proposed approach i.e. NSPPF implements novel crypto system for user encryption with partial decryption using advanced homomorphic procedure. Furthermore, we demonstrated that our proposed approach gives better performance with computational and communication user security in cloud environment. Future work behind proposed approach is to implement user based fine gained access control with respect to data sharing in secure cloud storage environment.

REFERENCES

[1] Cong Wang, Qian Wang, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Services Computing, VOL. 5, NO. 2, APRIL-JUNE 2012.

[2] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, “Auditing to Keep Online Storage Services Honest,” Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS ’07), pp. 1-6, 2007.

[3] M.A. Shah, R. Swaminathan, and M. Baker, “Privacy-Preserving Audit and Extraction of Digital Contents,” Cryptology e-Print Archive, Report 2008/186, http://eprint.iacr.org, 2008.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: Multiple-Replica Provable Data Possession,” Proc. IEEE 28th Int’l Conf. Distributed Computing Systems (ICDCS ’08), pp. 411-420, 2008.

[5] Ximeng Liu, Baodong Qin,"An Efficient Privacy-Preserving Outsourced Computation over Public Data" Citation information: DOI 10.1109/TSC.2015.2511008, IEEE Transactions on Services Computing.

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 12585 - 12592

[6] D. Gardner, "Mit Media Lab Computing Director Details the Virtues of Cloud for Agility and Disaster Recovery," https://www.linkedin.com/pulse/20141007202429-135530-mit-medialab-computing-director-details-the-virtues-of-cloud-for-agility-anddisaster-recovery, 2014.

[7] "CDC/National Center for Health Statistics," http://www.cdc.gov/nchs/data access/ftp data.html.

[8] B. Chamberlin, "Iot (internet of things) will go nowhere without cloud computing and big data analytics," http://ibmcai.com/2014/11/20/iotinternet-of-things-will-go-nowhere-without-cloud-computing-and-bigdata analytics/.

[9] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure k-nearest neighbor query over encrypted data in outsourced environments," in IEEE 30th International Conference on Data Engineering, Chicago, ICDE 2014, IL, USA, 2014, 2014, pp. 664–675.

[10] B. K. Samanthula, F. Rao, E. Bertino, X. Yi, and D. Liu, "Privacy preserving and outsourced multi-user k-means clustering," CoRR, vol. abs/1412.4378, 2014.

[11] Y. Chen, C. Chu, J. Hwang, and J. Yoo, "A privacy-preserving human tracking scheme in centralized cloud based camera networks," in IEEE International Conference on Communications, ICC 2014, Sydney, Australia, June 10-14, 2014, 2014, pp. 793–798.

[12] R. Lu, H. Zhu, X. Liu, J. K. Liu, and S. Jun, "Towards efficient and privacy-preserving computing in big data era," IEEE Network Magazine, 2014.

[13] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 2013. Proceedings, Part I, 2013, pp. 75–92.

[14] J. Coron, T. Lepoint, and M. Tibouchi, "Scale-invariant fully homomorphic encryption over the integers," in Public-Key Cryptography – PKC 2014 - 17th International Conference on Practice and Theory in Public- Key Cryptography, Buenos Aires, Argentina, 2014. Proceedings, 2014, pp. 311–328.

[15] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings, 2010, pp. 420–443.

[16]L. Morris, "Analysis of Partially and Fully Homomorphic Encryption," http://www.liammorris.com/crypto2/Homomorphic%20Encryption%20Paper.pdf , 2013.

[17] S. Kamara and K. E. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security, FC 2010 Workshops, RLCPS, WECSR, and WLC 2010, Tenerife, Canary Islands, Spain, January 25-28, 2010, Revised Selected Papers, 2010, pp. 136–149.

[18] M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions," Journal of Systems and Software, vol. 86, no. 9, pp. 2263–2268, 2013.

Published by: The Mattingley Publishing Co., Inc.