Security and Privacy Challenges in Cloud: Survey and Research Directions

*V. Swathi[1], Dr. M. P.Vani[2]

[1]Research Scholar ,School of Computer Science and Engineering (SCOPE),Vellore Institute of Technology ,Vellore-Tamil Nadu ,India.
[2]Associate Professor-SITE VIT University, Vellore- Tamil Nadu, India
Corresponding Author: V. Swathi

ABSTRACT

Cloud Computing is known to be a new computing model which provides reliable, secure and quality assured computational environment for users. Most of the users prefer to store their data inside the cloud in an encrypted format to decrease the security concerns. However, to perform any operation on data at server, cloud needs to first decrypt the data. This operation might cause the challenging issues e.g. confidentiality along with privacy of confidential data, stored inside the cloud. Therefore secure outsourcing mechanisms are much needed to protect the sensitive information by enabling computations with encrypted data as well as to verify and validate the computation end result. To design such type of mechanisms is a big challenge. This paper presents an extensive literature study and review of latest advances, developments and new methodologies in cloud computing, concerning security and privacy challenges. We have discussed various design challenges and some significant characteristics of these schemes. Finally, we have outlined some open problems in this domain and our further research aims and directions.

***Keywords**: Cloud, Security and privacy, Data integrity, Complexity, Biometrics, Identification.*

Date of Submission: 11-08-2017 Date of acceptance: 24-08-2017

I. INTRODUCTION

Most of the users prefer to store their data inside the cloud in an encrypted/unoriginal format to decrease the security concerns as how to protect the data that is processed and generated by the customers, is becoming the major concern [16][18][22] in the present day situation. Basic advantage of cloud computing [19][20][21] is that it is having the benefits of centralized large computational power, space and efficiency, so that the clients can outsource their complex problem to the cloud for computation purpose. Although the cloud computing is being used to outsource large-scale computations to the cloud, data privacy [36][37] has become a major issue. Though, to perform any operation on data at server, cloud needs to first decrypt the data. This operation might cause the challenging issues [34][35] like - confidentiality along with privacy of confidential data, stored inside the cloud. Cloud computing is a computational mechanism, which is used for the convenient non-demand network access to the shared pool of the computing resources which is having the greater efficiency as well as large computational power [23][24][32][33]. General framework of cloud-client model is shown as below diagram:-

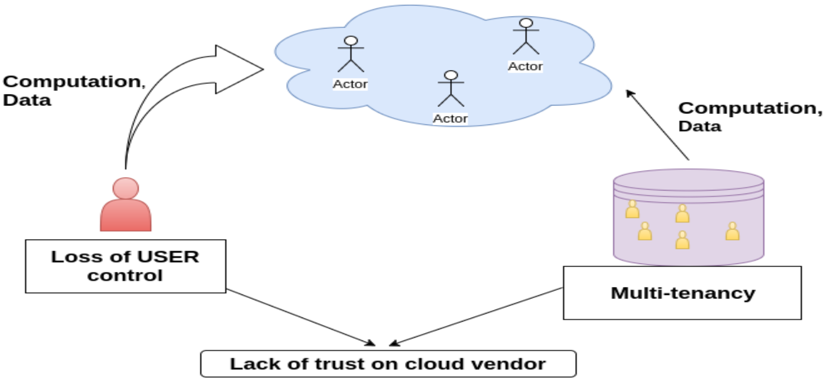


Figure 1: Secure outsourcing in cloud computing

Cloud is having the great potential of robust computational power to the aggregated management of the elastic resources. The outsourced problem constraints from the customers' side may contain private and sensitive information e.g. Personal identifiable business information, sensitive research data etc. So to protect this data from unauthorized use, customers need to encrypt their data prior to outsourcing, but further performing the computations on this encrypted data makes a very hard problem for the cloud server [25][26][27][28].

A. Motivation to the problem

There exist a much powerful thrust to provide the security at various infrastructure levels inside cloud [29][30][31], while any outsourced computing or any third party computations are being performed. To resist against unauthorized information leak, sensitive data essentially has to be encrypted before outsourcing to cloud. Common data encryption methods [38][39] in essence limit cloud from performing any meaningful operation of the underlying plaintext data, causing the computation over encrypted data a very difficult problem. Homomorphic encryption [6][7][40] is evolved as an special form of encryption that use to allow the computations to be carried out on ciphertext, therefore generating an encrypted result which, when decrypted, will give a match with the result of operations, performed on plaintext data. In 2010, Gentry proposed the Fully Homomorphic Encryption mechanism, which was a great breakthrough in cryptography [41][42].

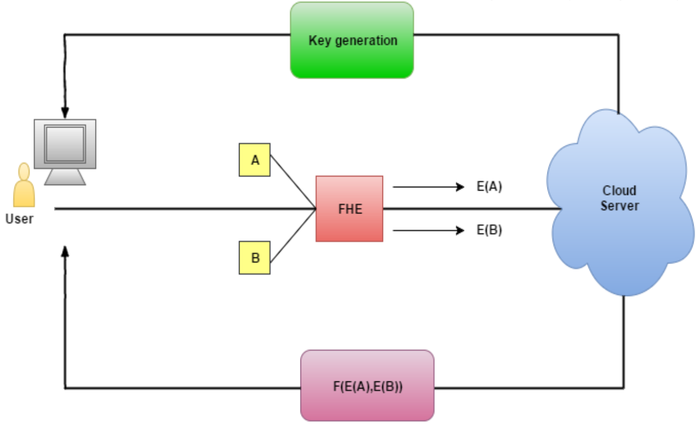


Figure 2: FHE application in cloud computing

Fully Homomorphic encryption (FHE) is a tremendous way to perform processing and computations on the encrypted data in cloud environment, which is being used by any third parties without the knowledge of private secret key.

B. Organization order of the paper

In rest of the paper, section 2 discusses some security and privacy challenges in this domain. An extensive literature review is presented in section 3. Section 4 summarizes some significant issues of cloud storage and need for the data robustness schemes. Our further research directions are given in section 5. Finally section 6 concludes the paper.

II. SECURITY AND PRIVACY CHALLENGES

Many traditional and modern techniques like partitioning, virtualization and other cloud based applications are being utilized in cloud scenarios.

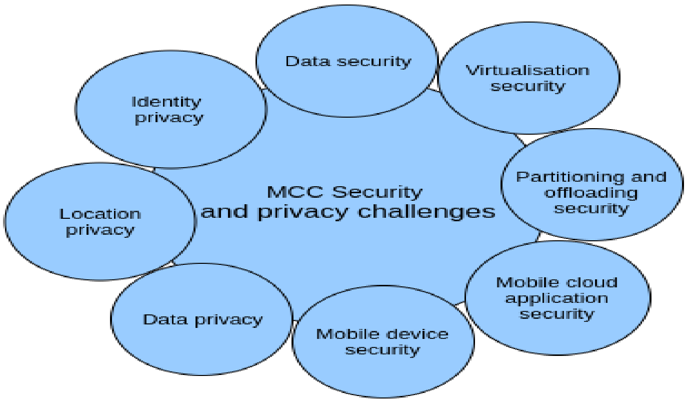

MCC Security and privacy challenges
Data security
Virtualisation security
Identity privacy
Partitioning and offloading security
Location privacy
Mobile cloud application security
Data privacy
Mobile device security

Figure 3: Overview of privacy challenges

We are going to discuss several security and privacy challenges in this section.

A. Offloading and Partitioning security challenges

During the offloading procedure [35][36][39][40], it need to access the cloud through wireless networks. Since the mobile users do not have any access as well as control over their offloading processes, so, there involved a risk of unofficial access to offloaded content. The confidentiality and integrity challenge grows because after the execution of offloaded content, if result is modified, the mobile devices cannot perform verification easily about the correctness of results [70].

B. Data security challenges

The data related challenges include data loss, data recovery, data locality as well as data privacy. The data loss and data breach break mainly the two security requirements such as integrity and confidentiality. Here, the data loss means – the users' data is in error condition that damaged or skipped by any physical means during processing, transmitting or storage. The correctness of data becoming one of the concerns for mobile users in cloud scenario [71][72].

C. Security challenges in Virtualization aspect

In cloud end, an image of virtual machine (VM) of the mobile device is pre-equipped and the tasks of the mobile device are offloaded to the virtual machine for processing [36][39][73]. This virtual machine is also called thin virtual machine or phone clone. The prime function for virtualization is to give various virtual machines running on same mobile devices but isolated to each other.

D. Cloud applications security challenges for mobility

cloud based mobile application level attacks can affect the integrity and confidentiality of both the data and applications by several procedures e.g. integrating malwares. Malwares like worm, rootkit, botnet etc. are unfavorable, intrusive applications or programmed codes. The targets of these malwares are to run with intentions at mobile devices or attach with applications without users' compliances. As a consequence, the functionalities of mobile applications can be changed.

E. Security challenges for mobile devices

Although there are password or pattern based locked features; many mobile users do not use these features. And the identity module card inside the mobile device also can be taken aside from device and accessed by unauthorized persons. Moreover, most of mobile devices are lack of security mechanism against threats. The attackers can attack by utilizing different availability attack techniques such as by sending high malicious traffic stream, huge messages to targeting mobile devices to make unused or reducing the capability [48]. The battery power exhaustion attack is another kind of availability attack where after attacking, the mobile devices start to discharge its battery power rapidly. This attack is unique for mobile device as it is performed by utilizing vulnerabilities of wireless networks, and mobile users are unaware about this kind of attack. the functionalities of present mobile platforms [74][75] are quite close to personal computers but with extra features and these platforms for mobile devices support many applications. Hence, to ensure confidentiality and integrity of these applications, there need to secure the mobile platforms also.

There are three kinds of storage available in mobile devices such as on device storage, plugged in storage and identity module storage. Generally, user's personal data, applications and others are stored in these storages. But if a mobile user avail cloud services, its data and applications are copied in the cloud storages [76]. So, if the mobile device is stolen or lost, then it becomes an important point such as the attackers can get access to the mobile devices and access to the cloud as well.

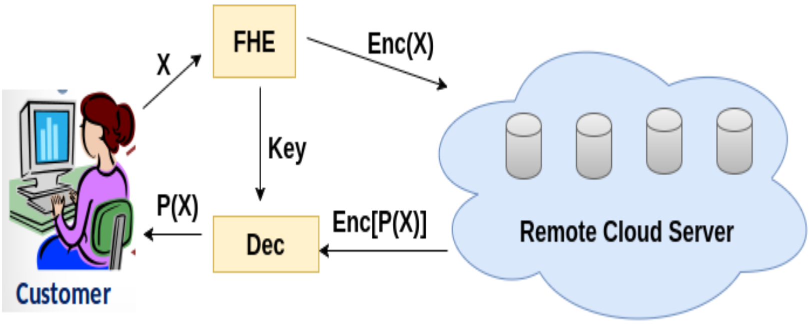
F. Privacy challenges in cloud

Cloud storage and processing in multiple locations raise privacy problems. The cloud servers of service providers are located at different regions and countries. For example, Google's cloud servers are located almost around the world such as seven locations in Americas, two locations in Asia and three locations in Europe. Moreover, it is important to users to get cloud hosting location's information as the law differs from one country to another. Several mobile applications are available which may be unsafe due to having hideous functions, collecting unintentionally users personal information e.g. hobbies, locations, and may spread illegally. The unwanted emails or junk emails can violate the users' privacy [47][77].

The context awareness, enabled by the sensors on mobile devices, is one of the main features of mobile applications that differ from personal computers. The context provides information to service providers by giving users' context and hence, the service providers can provide services with respect to the requirements of users. These location-aware applications and services specifically raise privacy concerns for mobile devices. These can either be user invoked or service provider invoked, and need the user location's knowledge to deliver the location based services.

III. LITERATURE REVIEW

This section extensively represents the research work and developments that has taken place in past years. Cong Wang et. al. [1] has described about secure outsourcing mechanism which is used to solve large scale systems of linear equation of cloud. Applications of Gaussian elimination and LU decomposition approaches are becoming expensive due to large scale LE problems. Hence, another approach named iterative method is used [16][17]. [2][43][44] presented the protocol as secure computation protocol, is used for bridgeing secure storage also secure computation auditing in cloud. [3][45] Has mainly investigated about secure outsourcing of widely applicable linear programming computations. Present mechanism explicitly decomposes LP computation outsourcing [46][47] into the public LP solvers which running on the cloud also those private LP parameters owned by the customer. [4][48] has mainly described practical outsourcing schemes, in which they described how to securely outsource modular exponentiation, that presents the computational bottleneck in public key cryptography [49][50] on computationally limited devices. [5] Discussed about problem of simultaneously achieving scalability, fine grainedness and data confidentiality of acees control. Here, they have defined access policies which are based on data attributes; also they delegate the computation tasks to the untrusted servers without changing any underlying contents in the data. Craig Gentry et. al. [6][51] proposed FHE scheme means schemes that allows to evaluate circuits over the encrypted data which is unable to decrypt. Final solution of this complete issue comes under 3 steps. (i) They have provided general result, which is used to construct the encryption scheme. (ii) Later described public key encryption scheme using the ideal lattices which is almost bootstrapable. (iii) They showed modification of scheme to reduce depth of decryption circuit. An application scenario of FHE is given in fig 4 below –



An Application Scenario: FHE

Fig.4

[7] Has mainly focused on storing of data on cloud in the encrypted format using FHE. Results are downloaded from client machine only. Hence, users data is never stored in plaintext on public cloud [52][53]. [8][54] Described about Cloud Computing Algebra Homomorphic Encryption Scheme Based on Fermat's Little Theorem. They have proposed this application on cloud computing for efficient security. [9][55][56] listed out three fundamental questions about

FHE, purpose of FHE, state of FHE. Also given clarity on different terminologies which are in use and prove connections between FHE notions. [10][57] described about Data Banks and Privacy Homomorphism. In this, it appears similar to that encryption functions which permits encrypted data [58][59] should be operated on without prior decryption. [11] proposed hybrid homomorphic system which is applied to the banking data and is used to perform the operations on encrypted data avoiding decrypting. Khalid El Makkaoui et. al. [12][60] has proposed Challenges of Using Homomorphic Encryption to Secure Cloud Computing. Mainly they goes through challenges facing HE methods for allowing the suppliers of cloud to perform operations on encrypted data, also provides same results after completion as if they are performing these calculations on raw data. Muhammad Baqer Mollah et. al. [13][61] discussed the data which is stored in cloud infrastructure and actual execution is shifted to cloud environment. [14] aims to enhance the understanding of security issues associated with the cloud storage, also highlights the importance of data integrity schemes for the outsources data, and have presented taxonomy of existing data schemes used for the cloud storage. Changhee Hahn et. al. [15] proposed an efficient and privacy preserving biometric identification scheme in cloud computing. This scheme exploits a symmetric homomorphic encryption algorithm in biometric identification, thus achieving both security and efficiency. The client encrypts and enrolls his/her fingerprint. For identification, the client encrypts and sends a newly scanned fingerprint to the cloud. The previous key used to enroll is not re-used but a fresh key [63][63] is generated at every identification to encrypt the fingerprint. In the proposed scheme, Initial client enrollment phase occurs in which the first client has FingerCode $m_1 = \left[x_{11}....x_{1N}\right]$ and a random key $k_1 = \left[k_{11}...k_{IN}\right]$, he encrypts m_1 using k_1. The client then sends the encrypted file to the server, which re-encrypts the file, then sends to the cloud. Next, the client, server, and cloud establish a secure channel among them to run a key-exchange protocol. Further second and subsequent clients enrollment is done. By iterating this process for *n* number of clients, the cloud has encrypted FingerCodes as follows:

$$Enc_{\sum_{i=1}^{n}(k_i+k_{sn}+k'_{sn})}(m_1).....Enc_{\sum_{i=1}^{n}(k_i+k_{sn}+k'_{sn})}(m_n)$$

the encrypted result is decrypted and cloud computes the Euclidean distance between FingerCodes and sends it to the server to verify whether the client is legitimate by using some threshold i.e. if $dist_{\min} \le t$ (where, *t* is threshold), the client is successfully identified. Cloud computing services [23][64] are organized as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [65][66]. Under the umbrella of these services a number of new services have also emerged, e.g. Data Integrity as a Service (DIaaS), Database as a Service, Logging as a Service, Security as a Service etc [67][68][69]. was introduced with or without third party auditor (TPA). Privacy issues such as leakage of data and user anonymity were identified due to the introduction of TPA. Thus, privacy preserving data integrity schemes were developed to overcome the privacy concerns of the users.

IV. ISSUES OF CLOUD STORAGE AND NEED FOR DATA ROBUSTNESS SCHEMES

This section discusses the significant characteristics for data robustness schemes along with design challenges.

A. Characteristics of data robustness schemes

All data integrity schemes have following significant properties:

1) Remote verification: Remote verification means that a verifier should not retrieve file blocks from the remote server for verification. In this verification, the cloud accesses block of a data file and generate a proof of possession, which is later verified by a client to validate data integrity.

2) Unrestricted challenge frequency: means that there should be no restrictions on the numbers of challenges made by a client or auditor to verify the integrity of remote data. A client executes the verification protocol with intervals to timely identify any data corruption. The frequency of challenge requests is directly affected by the computation efficiency of the data integrity scheme [78][79]. If verification process of a data integrity scheme is computationally expensive, then the client will use it less frequently and as a result unbounded challenge frequency would suffer.

3) Soundness: property of data integrity schemes ensures data reliability. The nature of a data integrity schemes is tamper evident, not tamper resistant. Therefore, if metadata are tampered with, or data get corrupted intentionally by the CSP [80] or unintentionally, this should be timely distinguished by a data integrity scheme. If the CSP can pass a challenge request without holding the data or with corrupted data, then a client will never be able to identify data corruption promptly, and the value of the data will be lost. Therefore, the reliability of data directly demands the soundness of a data integrity scheme for cloud storage [81][82].

4) Robustness: Data integrity schemes of deterministic nature have a limitation of computational efficiency and are not applicable for large datasets. To overcome these limitations, a probabilistic approach is adopted. Probabilistic data integrity schemes work on randomly chosen samples of data for integrity verification, which raises the issue of identification of small (bit or byte level) corruptions. Robustness property enhances the soundness of data integrity schemes by providing the identification of minor level corruptions in data.

5) Data recovery: For a data integrity scheme, it is not sufficient just to identify the misbehavior by the remote storage server. As cloud users are also interested in, complete data recovery to avoid an unpleasant situation. Data integrity schemes are divided into two categories depending on their tendency. Usually, error-correcting codes (ECC) are used by the schemes providing data recovery.

6) Dynamic data handling: Data can be either static i.e. backup or archival data or dynamic nature i.e. supporting operations like - insertion, deletion, and modification. Providing data integrity for dynamic data is more challenging than for static data or append-only data. Most of the schemes proposed in the literature are not capable to handle dynamic data.

7) Privacy preserving: Privacy concerns are introduced due to public verifiability. As the data owner will not allow the disclosure of his private data [83][84] to a third-party auditor, the privacy preservation property demands that a third party auditor should not obtain any confidential information about the users data but can still verify the integrity of outsourced data.

B. Design challenges

Some of the notable design challenges are listed below -

1) Computation and Storage efficiency: All data integrity schemes preprocess the data before outsourcing it to a cloud storage server, similarly, at the cloud storage server [41][85][86]; metadata are generated from original data. The overhead of performing such processing may affect the computation efficiency of data integrity schemes. Computation efficiency of preprocessing phase does not matter for small datasets, but it has a serious impact for large datasets. Computation cost on the server side for the proof generation limits on how frequently user can verify the integrity of outsourced data. Primitives used by the data integrity scheme as metadata also impact computation time.

For integrity verification and data recovery by any data integrity scheme, additional metadata is required along with the original data. Furthermore, data de-duplication plays a significant role in the reduction of storage [87][88] though will incur some cost.

2) Communication efficiency: In the case of dynamic data, this communication overhead also includes the updates verification. Primitives used for metadata have an impact on the communication cost [89][90]. Three aspects describing the communication efficiency of data integrity schemes are (1) Overhead of the initial data transfer along with metadata, (2) challenge requests for possession verification by data owner [91][92] and (3) challenge response for proof of possession sent back by the cloud storage server [93].

3) Security challenge: Data integrity schemes are vulnerable to a variety of attacks. Therefore, care must be taken in designing such a scheme. Following are the possible attacks that may be launched against a data integrity scheme:-

- Data deletion attack
- Tag forgery attack
- Replace attack
- Replay attack
- Data leakage attack

While designing a data integrity scheme, care must be taken so that the metadata used for verification may not result in leakage of original data during the verification protocol. Modern cryptographic techniques [6][7][94] such as ”Multi-Prover Zero-Knowledge Proof System” can provide protection against tag forgery attack and data leakage attack. Using homomorphic verifiable responses and hash index hierarchy ”Collaborative PDP” ensures that any adversary capable of eavesdropping the communication channel will not be able to extract any information from data exchanged in verification protocol [95][96].

4) Reduced disk I/O: Disk I/O efficiency of a data integrity scheme is derived by the overhead in block access and metadata access for proof generation on cloud storage server. Accessing all blocks for proof generation impacts the efficiency of a scheme and makes the scheme impractical for large datasets.

V. OPEN ISSUES AND RESEARCH DIRECTIONS

How to protect customers confidential data (e.g. Business financial records, personal research data etc.), which has to be prepared and generated during the computation is becoming the major security concern [21][97]. So to protect this data from unauthorized use, customers need to encrypt their data prior to outsourcing, but further performing the computations on this encrypted data makes a very hard problem for the cloud server [98][99]. Some open issues and our future research directions are discussed as follows:-

A. Problem Identification

Most of the users favor to store their data inside cloud environment [57][100] in an unoriginal form to decrease the security concerns [101]. However, to execute any operation on the data, which is residing at server, cloud needs to first decrypt the data. This operation might create the confidentiality and privacy issues of data stored in the cloud. Homomorphic encryption is a kind of encryption mechanism that give ability to users for computations to be prosecuted on cipher text itself, thus producing an unoriginal result when decrypted it shows similarity on the result of operations prosecuted on the plain text.

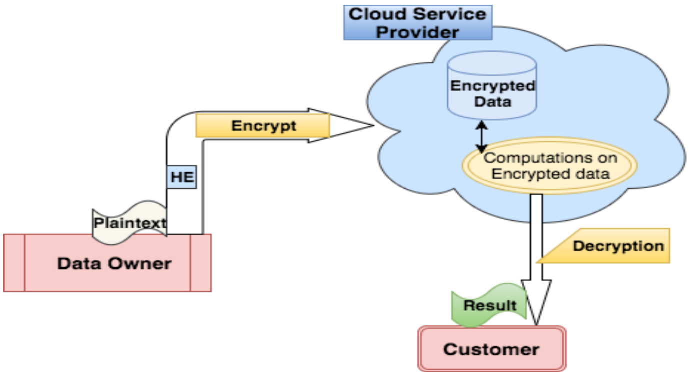


Figure 5: Secure Computations on Encrypted Data

While on another point of view, the operations which are being performed may not transparent to customer, so customer needs to verify the result of the outsourced problem after the computation is performed. Most significantly, security is a prime concern that prevents the adoption of computation outsourcing in the cloud.

B. Future Research Directions

The aim of the research is to develop new practically secure and efficient schemes for the data security in cloud. This aim is fulfilled by using the following objectives -

- We will come up with optimal Homomorphic encryption (HE) schemes and apply it to secure computation in cloud. Homomorphic encryption is a way to perform processing and computations on the encrypted data in cloud environment, which is being used by any third parties without the knowledge of private secret key.
- We will also present the practical applicability and security analysis of the proposed schemes.
- One limitation of homomorphic encryption is that it does not support for multiple users. We will come up with the possible ways to solve this problem.
- In our implementation, we may work on a virtual platform as a Cloud server, a VPN network that links the Cloud with the customer and then simulate the different scenarios. We can connect to the AWS DynamoDB service through the Eclipse IDE. Further we can build our own AWS model for proposed system and will try to implement the proposed FHE scheme, and later perform simulation over it. OpenNebula, Eucalyptus types of open source tools can be utilized for virtual cloud environment experiments.

VI. CONCLUSIONS

Customers need to outsource their problem to the cloud server for computation in a secure manner that brings new challenges for customer's data privacy and confidentiality. This paper started with the discussion of introduction to the entire problem domain, security and privacy challenges involved in it. Then we have presented an extensive review of work done in past years. We have mentioned the significant characteristics of robustness of schemes along with its design challenges. Further, we have listed some vital issues in this domain and our future research directions.

REFERENCES

[1] Cong Wang, Kui Ren, Jia Wang, Karthik Mahendra Raje Urs. ”Harnessing the Cloud for Securely Outsourcing Large-scale Systems of Linear Equations”, IEEE Transactions on Parallel & Distributed Systems, vol. 24, no., pp. 1172-1181, June 2013, doi:10.1109/TPDS.2012.206.

[2] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, Athanasios V. Vasilakos. ”Security and privacy for storage and computation in cloud computing”, Information Sciences 258, 2014, 371-386.

[3] Cong Wang, Kui Ren, Jia Wang. ”Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming”, IEEE Transactions on Computers, Vol. 65, No. 1, January 2016.

[4] Susan Hohenberger, Anna Lysyanskaya. ”How To Securely Outsource Cryptographic Computations”, TCC 2005: Theory of Cryptography Conference, pp. 264-282.

[5] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. ”Achieving Secure, Scalable, and Fine grained Data Access Control in Cloud Computing”, IEEE INFOCOM 2010.

[6] Craig Gentry. ”Fully Homomorphic Encryption Using Ideal Lattices”, STOC09, May 31-June 2, 2009.

[7] Manish M Potey, C A Dhote, Deepak H Sharma. ”Homomorphic Encryption for Security of Cloud Data”, 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79, 2016, 175-181.

[8] Khaled Elleithy, Reem Alataas. ”Cloud Computing Algebra Homomorphic Encryption Scheme Based on Fermat's Little Theorem”, ASEE 2013.

[9] Frederik Armknecht, Colin Boyd, Christopher Carr, Kristian Gjsteen, Angela Jschke, Christian A. Reuter, Martin Strand. ”A Guide to Fully Homomorphic Encryption”, IACR 2015.

[10] Ronald L. Rivest. ”On Data Banks and Privacy Homomorphism”, In Foundations of Secure Computation, pp. 169-180, 1978.

[11] Maha Tebaa, Karim Zkik, Said El Hajji. ”Hybrid Homomorphic Encryption Method for Protecting the Privacy of Banking Data in the Cloud”, International Journal of Security and Its Applications, Vol. 9, No. 6, 2015, pp. 61-70.

[12] Khalid El Makkaoui, Abdellah Ezzati, Abderrahim Beni Hssane. ”Challenges of Using Homomorphic Encryption to Secure Cloud Computing”, 2015, International Conference on Cloud Technologies and Applications (CloudTech).

[13] Muhammad Baqer Mollah, Md. Abul Kalam Azad, Athanasios Vasilakos. ”Security and privacy challenges in mobile cloud computing: Survey and way ahead”, Journal of Network and Computer Applications 84, 2017, 38-54.

[14] Faheem Zafar, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed, Adeel Anjum, Majid Iqbal Khan, Nadeem Javed, Masoom Alam, Fuzel Jamil. ”A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends”, computers & security 65, 2017, 29-49.

[15] Changhee Hahn, Junbeom Hur. ”Efficient and privacy-preserving biometric identification in cloud”, ICT Express 2, 2016, 135-139.

[16] Ab Rahman, N.H., Cahyani, N.D.W., Choo, K.K.R., 2016. Cloud incident handling and forensicbydesign: cloud storage as a case study. Concurr. Comput.: Pract. Exp..

[17] Abdalla, A.-k.A., Pathan, A.-S.K., 2014. On protecting data storage in mobile cloud computing paradigm. IETE Tech. Rev. 31, 82-91.

[18] Ahmed, E., Gani, A., Khan, M.K., Buyya, R., Khan, S.U., 2015. Seamless application execution in mobile cloud computing: motivation, taxonomy, and open challenges. J. Netw. Comput. Appl. 52, 154-172.

[19] Alam, S., Sogukpinar, I., Traore, I., Coady, Y., 2014. In-Cloud Malware Analysis and Detection: State of the Art. In: Proceedings of the 7th International Conference on Security of Information and Networks, p. 473.

[20] Ali, M., Khan, S.U., Vasilakos, A.V., 2015a. Security in cloud computing: opportunities and challenges. Inf. Sci. 305, 357-383.

[21] Ali, M., Dhamotharan, R., Khan, E., Khan, S.U., Vasilakos, A.V., Li, K., et al., 2015b. SeDaSC: Secure data sharing in clouds. IEEE Syst. J. 99, 1-10.

[22] Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K., 2016. Authentication in mobile cloud computing: a survey. J. Netw. Comput. Appl. 61, 59-80.

[23] Alizadeh, M., Hassan, W.H., 2013. Challenges and opportunities of mobile cloud computing, in Wireless Communications and Mobile Computing Conference (IWCMC), 2013. 9th International, pp. 660-666.

[24] Al-Mutawa, M., Mishra, S., 2014. Data partitioning: an approach to preserving data privacy in computation offload in pervasive computing systems. In: Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks, pp. 51-60.

[25] Alqahtani, H.S., Kouadri-Mostefaou, G., 2014. Multi-clouds Mobile Computing for the Secure Storage of Data, in 2014 IEEE/ACM. In: Proceedings of the 7th International Conference on Utility and Cloud Computing, pp. 495-496.

[26] Amin, M.A., Bib Abu Bakar, K., Al-Hashimi, H., 2013. A review of mobile cloud computing architecture and challenges to enterprise users, in GCC Conference and Exhibition (GCC), 2013. 7th IEEE, pp. 240-244.

[27] Azfar, A., Choo, K.-K.R., Liu, L., 2016. Android mobile VoIP apps: a survey and examination of their security and privacy. Electron. Commer. Res. 16, 73-111.

[28] Ba, H., Heinzelman, W., Janssen, C.-A., Shi, J., 2013. Mobile computing-A green computing resource, in Wireless Communications and Networking Conference (WCNC), IEEE, pp. 4451-4456.

[29] Baharon, M.R., Shi, Q., Llewellyn-Jones, D., 2015. A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing, in Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, pp. 618-625.

[30] Bahrami, M., 2015. Cloud Computing for Emerging Mobile Cloud Apps, in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015. In: Proceedings of the 3rd IEEE International Conference on, pp. 4-5.

[31] Bahrami, M., Singhal, M., 2015. A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing, in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015. In: Proceedings of the 3rd IEEE International Conference on, pp. 189-198.

[32] Bouzefrane, S., Mostefa, B., Amira, F., Houacine., Cagon, H., 2014. Cloudlets Authentication in NFC-Based Mobile Computing, in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014. In: Proceedings of the 2nd IEEE International Conference on, 2014, pp.267-272.

[33] Chard, K., Caton, S., Rana, O., Bubendorfer, K., 2010. Social cloud: Cloud computing in social networks,” in Cloud Computing (CLOUD), 2010. IEEE In: Proceedings of the 3rd International Conference on, pp. 99-106.

[34] Chen, M., Zhang, Y., Li, Y., Hassan, M., Alamri, A., 2015b. AIWAC: affective interaction through wearable computing and cloud technology. Wirel. Commun. IEEE 22,20-27.

[35] Chen, M., Hao, Y., Li, Y., Lai, C.-F., Wu, D., 2015c. On the computation offloading at ad hoc cloudlet: architecture and service modes. Commun. Mag., IEEE 53, 18-24.

[36] Chen, X., Jiao, L., Li, W., Fu, X., 2016. Efficient multi-user computation offloading for mobile-edge cloud computing. IEEE/ACM Trans. Netw. 24, 2795-2808.

[37] Chen, M., Li, W., Li, Z., Lu, S., Chen, D., 2014. Preserving location privacy based on distributed cache pushing, in Wireless Communications and Networking Conference(WCNC), 2014 IEEE, pp. 3456-3461.

[38] Dey, S., Sampalli, S., Ye, Q., 2015. A Context-Adaptive Security Framework for Mobile Cloud Computing, in 2015. In: Proceedings of the 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN), pp. 89-95.

[39] Dhanya, N., Kousalya, G., 2015. Adaptive and Secure Application Partitioning for Offloading in Mobile Cloud Computing, Security in Computing and Communications(ed). Springer, 45-53.

[40] Duan, Y., Zhang, M., Yin, H., Tang, Y., 2015. Privacy-preserving offloading of mobile app to the public cloud. In: Proceedings of the 7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud15).

[41] Feng, T., Zhao, X., Carbunar, B., Shi, W., 2013. Continuous mobile authentication using virtual key typing biometrics, in Trust, security and privacy in computing and communications (TrustCom), 2013. In: Proceedings of the 12th IEEE international conference on, pp. 1547-1552.

[42] Gai, K., Qiu, M., Zhao, H., Xiong, J., 2016. Privacy-aware adaptive data encryption strategy of big data in cloud computing, in Cyber Security and Cloud Computing(CSCloud), 2016 IEEE. In: Proceedings of the 3rd International Conference on, pp.273-278.

[43] Guo, C., Zhuang, R., Jie, Y., Ren, Y., Wu, T., Choo, K.-K.R., 2016. Fine-grained database field search using attribute-based encryption for e-healthcare clouds. J. Med. Syst.40, 235.

[44] Han, Y., Chan, J., Alpcan, T., Leckie, C., 2015. Using virtual machine allocation policies to defend against co-resident attacks in cloud computing. IEEE Trans. Dependable Secur. Comput..

[45] Hao, Z., Tang, Y., Zhang, Y., Novak, E., Carter, N., Li, Q., 2015. SMOC: A secure mobile cloud computing platform. In: Computer Communications (INFOCOM), 2015 IEEE Conference on, pp. 2668-2676.

[46] Mollah, M.B., Azad, M.A.K., Vasilakos, A., 2017. Secure data sharing and Searching at the edge of cloud-assisted Internet of Things. IEEE Cloud Comput. 4, 34-42.

[47] Iqbal, S., Kiah, M.L.M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M.K., et al., 2016. On cloud security attacks: a taxonomy and intrusion detection and prevention as a service. J. Netw. Comput. Appl. 74, 98-120.

[48] Jarabek, C., Barrera, D., Aycock, J., 2012. Thinav: Truly lightweight mobile cloud-based anti-malware. In: Proceedings of the 28th Annual Computer Security Applications Conference, pp. 209-218.

[49] Jeong, Y.S., Park, J.S., Park, J.H., 2013. An efficient authentication system of smart device using multi factors in mobile cloud service architecture. Int. J. Commun. Syst.

[50] Jin, Y., Tian, C., He, H., Wang, F., 2015. A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing, in Big Data and Cloud Computing (BDCloud), 2015 IEEE. In: Proceedings of the Fifth International Conference on, pp. 172-179.

[51] Juliadotter, N.V., Choo, K.-K.R., 2015. Cloud attack and risk assessment taxonomy. IEEE Cloud Comput. 2, 14-20.

[52] Khalil, I., Khreishah, A., Azeem, M., 2014. Consolidated Identity Management System for secure mobile cloud computing. Comput. Netw. 65, 99-110.

[53] Khan, A.N., Kiah, M.M., Khan, S.U., Madani, S.A., 2013a. Towards secure mobile cloudcomputing: a survey. Future Gener. Comput. Syst. 29, 1278-1299.

[54] Khan, A.N., Kiah, M.M., Madani, S.A., Ali, M., 2013b. Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. J. Supercomput. 66, 1687-1706.

[55] Kovachev, D., Renzel, D., Klamma, R., Cao, Y., 2010. Mobile community cloud computing: emerges and evolves, in Mobile Data Management (MDM), 2010. In: Proceedings of the Eleventh International Conference on, pp. 393-395.

[56] Kumari, S., Li, X., Wu, F., Das, A.K., Choo, K.-K.R., Shen, J., 2017. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Gener. Comput. Syst. 68, 320-330.

[57] Lei, L., Sengupta, S., Pattanaik, T., Gao, J., 2015. MCloudDB: A Mobile Cloud Database Service Framework, in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015. In: Proceedings of the 3rd IEEE International Conference on, pp. 6-15.

[58] Li, J., Li, J., Chen, X., Liu, Z., Jia, C., 2014. Privacy-preserving data utilization in hybrid clouds. Future Gener. Comput. Syst. 30, 98-106.

[59] Liang, H., Han, C., Zhang, D., Wu, D., 2014. A Lightweight Security Isolation Approach for Virtual Machines Deployment. In: Information Security and Cryptology, pp. 516-529.

[60] Liu, D., Dai, Y., Luan, T., Yu, S., 2015. Personalized search over encrypted data with efficient and secure updates in mobile clouds. IEEE Trans. Emerg. Top. Comput.

[61] Liu, F., Shu, P., Jin, H., Ding, L., Yu, J., Niu, D., et al., 2013. Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. Wirel. Commun. IEEE 20, 14-22.

[62] Liu, L., Zhang, X., Yan, G., Chen, S., 2009. Exploitation and threat analysis of open mobile devices, In: Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, pp. 20-29.

[63] Louk M., Lim, H., 2015. Homomorphic encryption in mobile multi cloud computing, in Information Networking (ICOIN), 2015 International Conference on, pp. 493-497.

[64] Meilander, D., Glinka, F., Gorlatch, S., Lin, L., Zhang, W., Liao, X., 2014. Using mobile cloud computing for real-time online applications, in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014. In: Proceedings of the 2nd IEEE International Conference on, pp.48-56.

[65] Meng, T., Wang, Q., Wolter, K., 2015. Model-Based Quantitative Security Analysis of Mobile Offloading Systems under Timing Attacks, Analytical and Stochastic Modelling Techniques and Applications (ed). Springer, 143-157.

[66] Mohammad, A.-R., Elham, A.-S., Jararweh, Y., 2015. AMCC: Ad-hoc based mobile cloud computing modeling. Procedia Comput. Sci. 56, 580-585.

[67] Mollah, M.B., Azad, M.A.K., Vasilakos, A., 2017. Secure data sharing and Searching at the edge of cloud-assisted Internet of Things. IEEE Cloud Comput. 4, 34-42.

[68] Qiu, M., Gai, K., Thuraisingham, B., Tao, L., Zhao, H., 2016. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future Gener. Comput. Syst..

[69] Niu, B., Li, Q., Zhu, X., Cao, G., Li, H., 2015. Enhancing privacy through caching in location-based services. In: Computer Communications (INFOCOM), 2015 IEEE Conference on, pp. 1017-1025.

[70] Odelu, V., Das, A.K., Rao, Y.S., Kumari, S., Khan, M.K., Choo, K.- K.R., 2016. Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. Comput. Stand. Interfaces.

[71] Yang, Y., Liu, J.K., Liang, K., Choo, K.-K.R., Zhou, J., 2015. Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data, in European Symposium on Research in Computer Security, pp. 146-166.

[72] [Online: 2016] Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications: < https :==www:itu:int=itudoc=itu □ t=85097:pdf >.

[73] [Online: 2016] US National Security Agency: Information Assurance: < http : ==www:nsa:gov=ia=iaatnsa=index:shtml >.

[74] Osanaiye, O., Choo, K.-K.R., Dlodlo, M., 2016. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. J.Netw. Comput. Appl. 67, 147-165.

[75] Owens, R., Wang, W., 2013. Preserving Data Query Privacy in Mobile Mashups through Mobile Cloud Computing, in Computer Communications and Networks (ICCCN),2013. In: Proceedings of the 22nd International Conference on, pp. 1-5.

[76] Paladi, N., Gehrmann, C., Michalas, A., 2016. Providing user security guarantees in public infrastructure clouds. IEEE Trans. Cloud Comput..

[77] Pasupuleti, S.K., Ramalingam, S., Buyya, R., 2016. An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. J. Netw. Comput. Appl. 64, 12-22.

[78] Tysowski, P.K., Hasan, M.A., 2013. Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds. Cloud Comput. IEEE Trans. 1, 172-186.

[79] Vaezpour, S.Y., Zhang, R., Wu, K., Wang, J., Shoja, G.C., 2016. A new approach to mitigating security risks of phone clone Co-location Over mobile clouds. J. Netw. Comput. Appl.

[80] Wang, S., Tu, G.-H., Ganti, R., He, T., Leung, K., Tripp, H., et al., 2013. Mobile microcloud: Application classification, mapping, and deployment. In: Proceedings Annual Fall Meeting of ITA (AMITA).

[81] Yang, Y., Zhu, H., Lu, H., Weng, J., Zhang, Y., Choo, K.-K.R., 2016. Cloud based data sharing with fine-grained proxy re-encryption. Pervasive Mob. Comput. 28, 122-134.

[82] Yang, Y., Liu, J.K., Liang, K., Choo, K.-K.R., Zhou, J., 2015. Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data, in European Symposium on Research in Computer Security, pp. 146-166.

[83] Yu, Y., Mu, Y., Ni, J., Deng, J., Huang, K., 2014. Identity Privacy- Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage, Network andSystem Security ed.. Springer, 28-40.

[84] Yu, Y., Li, Y., Au, M.H., Susilo, W., Choo, K.-K.R., Zhang, X., 2016. Public cloud data auditing with practical key update and zero knowledge privacy. In: Australasian Conference on Information Security and Privacy, pp. 389-405.

[85] Zhang, H., Yu, N., Wen, Y., 2015. Mobile cloud computing based privacy protection in locationbased information survey pplications. Secur. Commun. Netw. 8, 1006-1025.

[86] Zhang, J., Zhao, X., 2015. Efficient chameleon hashing-based privacypreserving auditing in cloud storage. Clust. Comput., 1-10.

[87] Zhang, Y., Su, S., Wang, Y., Chen, W., Yang, F., 2014. Privacyassured substructure similarity query over encrypted graphstructured data in cloud. Secur. Commun. Netw. 7, 1933-1944.

[88] Zhang, X., Schiffman, J., Gibbs, S., Kunjithapatham, A., Jeong, S., 2009. Securing elastic applications on mobile devices for cloud computing. In: Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 127-134.

[89] Zonouz, S., Houmansadr, A., Berthier, R., Borisov, N., Sanders, W., 2013. Secloud: a cloud-based comprehensive and lightweight security solution for smartphones. Comput. Secur. 37, 215-227.

[90] Birk D. Technical challenges of forensic investigations in cloud computing environments. Workshop on Cryptography and Security in Clouds. 2011.

[91] Cachin C, Haralambiev K, Hsiao H-C, Sorniotti A. 2013, Policy-based secure deletion, in ”Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security”, ACM, New York, NY, USA, pp. 259-70.

[92] Calder B, Wang J, Ogus A, Nilakantan N, Skjolsvold A, McKelvie S, et al. 2011, Windows Azure Storage: a highly available cloud storage service with strong consistency, in ”Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles”, ACM, New York, NY, USA, pp. 143-57.

[93] Etemad M, Kp A. 2013, Transparent, distributed, and replicated dynamic provable data possession, in ”Proceedings of the 11th International Conference on Applied Cryptography and Network Security”, Springer- Verlag, Berlin, Heidelberg, pp. 1-18.

[94] Habib A, Khanam T, Palit R. 2013, Simplified File Assured Deletion(SFADE) - a user friendly overlay approach for data security in cloud storage system, in ”Advances in Computing,Communications and Informatics (ICACCI), 2013 International Conference on”, pp. 1640-44.

[95] Khan SM, Hamlen KW. Computation certification as a service in the cloud. Cluster, Cloud and Grid Computing (CCGrid), 2013 13 IEEE/ACM International Symposium on. IEEE, 2013.

[96] Kwon O, Koo D, Shin Y, Yoon H. A secure and efficient audit mechanism for dynamic shared data in cloud storage. Scientific World J 2014;2014:doi:10.1155/2014/820391. Article ID 820391.

[97] Luo W, Bai G. 2011, Ensuring the data integrity in cloud data storage, in ”Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on”, pp. 240-43.

[98] Nabeel M, Bertino E. 2012, Privacy preserving delegated access control in the storage as a service model, in ”Information Reuse and Integration (IRI), 2012 IEEE 13th International Conference on”, pp. 645-52.

[99] Nepal S, Chen S, Yao KJ, Thilakanathan D. DIaaS: data integrity as a service in the cloud. Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, 2011.

[100] Rahumed A, Chen H, Tang Y, Lee P, Lui J. 2011, A secure cloud backup system with assured deletion and version control, in ”Parallel Processing Workshops (ICPPW), 2011 40 International Conference on”, pp. 160-67.

[101] Squicciarini AC, Petracca G, Bertino E. 2013, Adaptive data protection in distributed systems, in ”Proceedings of the Third ACM Conference on Data and Application Security and Privacy”, ACM, New York, NY, USA, pp. 365-76

International Journal of Computational Engineering Research (IJCER) is UGC approved Journal with Sl. No. 4627, Journal no. 47631.

*V. Swathi " Security and Privacy Challenges in Cloud: Survey and Research Directions " International Journal of Computational Engineering Research (IJCER) 7.8 (2017): 63-72