AN IRREVERSIBLE TRANSISTION TOWARDS BIG DATA CLOUDS: CHALLENGES OF DEPLOYING SECURITY AND PRIVACY SCHEMES

[1]S.Jayaprakash, [2]C. S. Rajarajeswari, [3]V.M.Suresh
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor
[1]Department of Computer Science,
[1]Sir Issac Newton College of Arts & Science, Nagapattinam, Tamilnadu, India

Abstract-Cloud technology is a compelling paradigm in digital universe to provide massive-scale computing and storage services. It excludes the need to preserve powerful computing devices, dedicated storage medium, and software tools. The customers are allowed to move their application software and data to the network and use higher-level services on-demand. Of late, it has been observed that enormous development in the scale of Big Data (BD) produced through cloud technology. The security and privacy issues are important barriers to cloud adoption. Transmitting data outside the organizational limits and access them over the internet creates complete loss of the owner's direct control. Hence, when storing and transferring sensitive information using public clouds, cyber threats in any form are expected in cloud computing. Therefore, cloud customers need to cognize the adoption of the service delivery model and the risk of security threats during implementation. In this article, we investigate the security requirements and different methods for protecting data. This study deeply covers data security and privacy challenges in an attempt to scholars can design the consistent security application models on cloud computing.

Keywords - Cloud computing, Cryptography, Data privacy, Group signatures, Security.

I. INTRODUCTION

Two information technology initiatives are the greatest concerns for industries across the world uses of Cloud Computing and BD manipulation. In the last two decades, the unremitting growth of computational capacity has generated vast data streams in unstructured, semi-structured and structured forms [1]. For instance, current high-energy physics experiments with high-level computing requirements like [2], usually capable of producing over 1TB of information day by day. The popular social media, Face book, notches over 540M unique visitors per month, serves a whopping 570B page views monthly, process 3B pictures, and copes 25B pieces of content (like status updates and comments) per month.

The hasty development of social media, sensors, network traffic, and surveillance maneuvers along with their wide spread usage results in generation of big data. BD is pigeon holed by the amalgamation of massive set of digital information with different data types and data structures which cannot be managed by conventional database software tools [3]. Since enormous data sets in unstructured (e.g., Audio files, video files, pictures, e-mail messages, word processing documents etc) and semi-structured (e.g. XML files, JSON documents, No SQL databases etc) formats are being produced from several sources, frameworks, different platforms and methods are mandatory for efficient data manipulation and management.

The torrent of unstructured and structured data pouring into the enterprise is astounding and the organizational data approximately doubles in size every years and expected to touch 44ZB in 2020[4]. For the enterprise to capitalize on it the infrastructure has to be able to integrate, associate and retrieve information at lightning speeds. Furthermore, as data is conserved longer, storage requirements increase. Conventional software tools and data manipulation schemes cannot store, manage, and manipulate that massive data.

Cloud computing offers scalable compute and storage resources over different service models on a pay-per-use basis with high performance and efficiency[5] as compared to conventional paradigms, the cloud technology is extensively employed for BD. Cloud technology has features such as omnipresent network access, on-demand self-service, load balancing, resource scheduling, usage-based pricing and the transference of risk. Cloud enables enterprises to support a larger number of mobile customers since data manipulation and storage are managed outside the mobile devices. These benefits have enticed considerable interests from both the industries as well as academia.

Cloud computing is now changing every aspect of the way to do business. Yet, there are some issues to be resolved for individual customers as well as organizations to save information and implement right services in the cloud. The data leakage and security breach are the most significant issues in the cloud owing to its open environment with restricted customer-side control [6]. Particularly on the cloud computing environment, there are two significant characteristics of BD security as (i) in what way to secure BD, (ii) in what way to exploit the data manipulation method to improve security of the entire cloud. Recent research only emphasis on major techniques for mining and processing. Nevertheless, BD security and privacy are important issues which have received comparatively little research attention.

In this article, we target to address these problems. Accordingly, the study presented in this article delivers a succinct yet appropriate discussion of security and privacy concerns with some basic strategies that should be used by IT industries, stepping into a cloud environment. This survey explores that as computing resources move from on the premise to cloud computing, security and privacy disputes are aggravated. This further thwarts decision making for or against cloud implementations. Subsequently, probing these concerns has the ability to pay considerably to the development of knowledge on cloud computing. Basically this article deals with one as data privacy and security challenges in cloud environment and two is Study of effective methods to secure organizations from threats.

The rest of the article is structured follows as we describe the evolution of cloud computing in section II. We discuss the fundamental concepts of big data in section III. In section IV, we present the problems and challenges related with BD. Section V starts with basic concepts of data security and privacy, followed by the phases of data life cycle and the section VI is dedicated to existing solutions to prevent security and privacy problems in the services delivered by cloud technology. Then, we present our conclusion in section VII.

II. OVERVIEW OF CLOUD COMPUTING

Before data security and privacy problems are addressed, the utilities of cloud technology are studied first. In cloud computing, Service Provider (SP) is a company that enables and handles the cloud services. SP provides computing and storage services through the Internet, whereas customers access services for meeting their demands and then pay SP accordingly. Cloud offers two basic services one is computing second as storage systems. In this environment, customers do not need anything and they can obtain rights to retrieve their information and complete their computation works simply over the internet. In the course of the information retrieval and computation processes, the customers do not even aware where the information is stored and which device performs the computation process. In case of storage, data security is the major issues for obtaining the customer's trust and making the cloud effectively implemented. Numerous data security and privacy methods have been suggested in the literature. Nevertheless, more effective solutions need to be implemented urgently to thwarts these issues.

Today, cloud technology is having a seismic effect on IT operations. Business enterprises and other organizations are implementing their business models through cloud computing technology to minimize their initial investment as well as overall cost. By delivering applications, platforms, and infrastructure available as a service, cloud computing has constantly reformed the way computing and storage resources are offered and utilized. The cloud technology is developing constantly since it could provide advanced performance at lower tariffs. Famous corporate enterprises like Amazon, Google, Microsoft, Rake space and IBM have delivered cloud services over the internet. The cloud has numerous applications based on the cloud offerings from SP. For instance, Apps Engine, Amazon Web Services (AWS) and Azure stack are famous service providers implemented by Google, Amazon and Microsoft respectively. Based on the access scope, there are four different clouds are available to users such as

1. Public cloud: It is open to everyone with all the resources and functionalities available to the customer publicly. Usually, it is maintained by a governmental organization and the customers accessed the services on demand.
2. Private cloud: It denotes an enterprise cloud where only the legal customers can retrieve the cloud offerings and resources.
3. Community cloud: The community cloud is a back bone network of clouds shared by more than one organization, having their own access strategies.
4. Hybrid cloud: It is the combinations of multiple clouds work in collaboration to deliver the required services to the customers moving from one place to another, and without requesting the services from cloud to cloud.

Cloud can save a time, capital costs and operational costs of organizations. However, creating trust in the cloud environments is a main challenge since the data of an organization are considered as a tangible asset that they share in the cloud. Cloud technology opens several issues that need distinct effort to make it reliable and trust worthy. The reliability and trust worthiness of the cloud hinges on the security and privacy methods employed in it. Several methods have been proposed and implemented by investigators to thwart these issues. However, there are still gap that requires research effort and effective solutions to make security and privacy methods efficient.

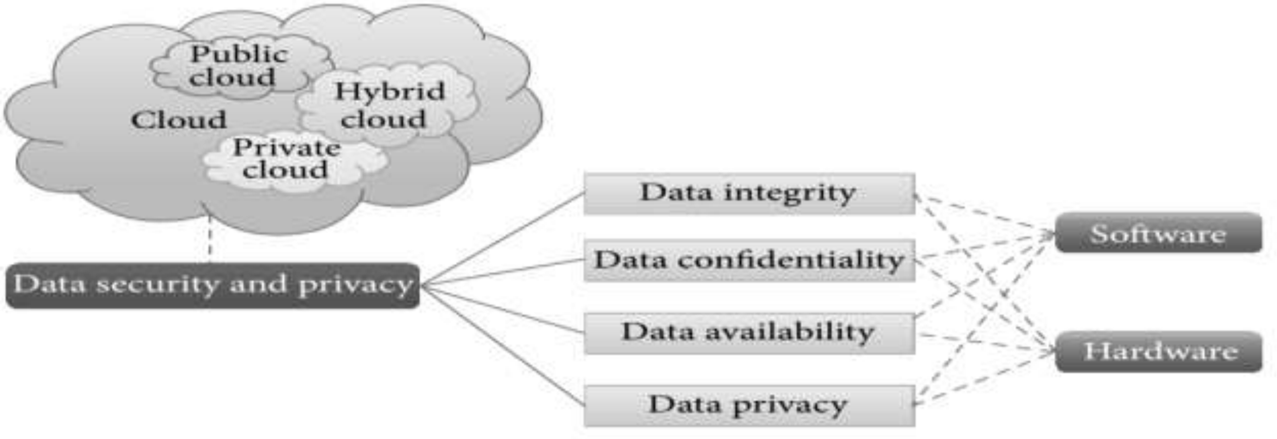

Figure 1. Cloud Computing

As Figure 1 shows, integrity, confidentiality, and availability are essential characteristics of a data. Data integrity indicates the confidence that the information kept in the cloud is not retrieved by illegal users. Confidentiality is associated with data privacy, where it is not revealed to illegal users [7]. Availability denotes the guarantee that whenever the customer requests data, it should be available to them instantly and can't be denied.

III. BIG DATA ANALYTICS

As explained in [8] BD analytics is an important tool for organizations and governmental agencies to manipulate and analyze data. Therefore, there is a fundamental need for breakthrough technology that will aid manipulation and storage system of BD in cloud. References [9] and [10] describe the term big data as extensive and intricate datasets that it becomes very tough to manipulate through conventional database software tools or on-hand manipulation techniques. BD is characterized by variety, velocity, volume, veracity and value [11] as follows:

1. Volume (Data Size): The data volume normally ranges from several terabytes to zeta bytes every month. It is not possible for large enterprises to accumulate a huge amount of secured data on the monthly basis.

2. Velocity (Data generation and manipulation speed): Velocity denotes to fast computation speed. It is defined as time taken for an instant anomaly or real-time response. For example, the potentially valuable data in a surveillance system are processed in simply one or two seconds, which are also very different in nature from the typical database management system.
3. Variety (Data Types): The BD comprises of different data types (i.e., text, image, audio, video etc). While considering security issues, data types could include large files, network log, geographic information, click data, machine and sensor data, video, pictures and social media activities etc. Hence, it is usual for organizations to integrate hundreds of varieties of data for performing security analysis by means of different algorithms.
4. Veracity (Data reliability): BD must be reliable and precise. Since it is associated with the real world entities, the analysis of BD is the process of elucidating and envisaging the real events from the huge network of data.
5. Value (Worth of data): Significant value can be established in BD, including optimizing processes, understanding users better, directing them accordingly, and enhancing business performance. Normally, BD has high commercial value. Through BD analysis, the user can understand how to increase value. Hence, several organizations are already using BD to generate and increase value.

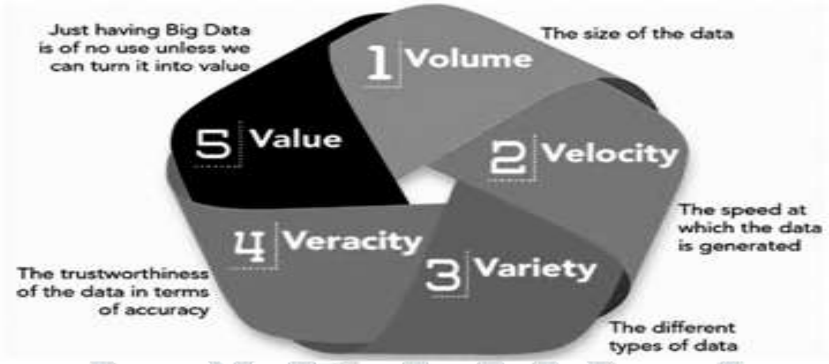

Figure 2. Characteristics of Big Data

IV. BIG DATA IN CLOUD COMPUTING

Massive-scale data usually require powerful processing devices and storage system, which drives the need for cloud technology. Big data enables organizations and enterprises to use cloud, because of its tremendous benefits, like cost saving, reliability, manageability, etc. It also delivers massive computation ability and storage. The important technologies behind the cloud such as virtualization techniques, scalable resource sharing, and worldwide distributed storage system are making it possible to process workloads that had been considered difficult in typical software tools. But, in contrast, cloud computing also causes severe data security and privacy disputes. Users vacillate to store their personal and sensitive information to the cloud unless they are sure that their information will be protected. There are some problems for constructing a reliable and secure BD manipulation and storage structure on cloud which are given below [12].

1). Outsourcing: In order to decrease the initial investment and operational costs, enterprises prefer outsourcing to manage their IT infrastructure. But, data outsourcing means that users will drop physical autonomy on their own data. The loss of physical autonomy on the data is considered as one of the major reasons for insecure cloud environment. This leads to severe harm to the privacy of the user. These disputes can be resolved using secure computing devices and storage system.

2). Multi-tenancy: Storage virtualization in cloud computing allows several independent users or organizations to share the same cloud environment. The information that belongs to various customers may be stored on the same storage medium using appropriate scheduling policies. In virtualization paradigm, it is comparatively easy for a customer to retrieve information illegally. Numerous security problems may arise in cloud (e.g. computation breach and data breach). Hence, it is essential to frame powerful techniques to handle security and privacy threats. Powerful computation: Owing to the competence of cloud technology for managing powerful computations and huge data storage, conventional techniques to secure data privacy are not adequate.

V. BIG DATA SECURITY AND PRIVACY ISSUES IN CLOUDS

Issues related to data security and privacy are most important concerns in information technology. It becomes especially severe in cloud technology, since data are dispersed in various computing devices and storage systems including personal computers, servers and different handheld devices like smart phones and wireless sensors and so on. Security and privacy challenges are augmented by its volume, variety and velocity of BD. Hence, BD security and privacy solutions are more intricate and challenging than traditional mechanisms. The data from customers to service provider and vice versa follow different phases. The main phases of BD life cycle are given below [13]

1. Data in motion: This phase represents the data is transferring from local storage device to cloud storage, between clouds and within the infrastructure, platform as well as software services. In this phase, data can be captured and in turn can distress data security. Advanced encryption techniques are implemented to protect data integrity at this phase.
2. Data in storage: This phase represents the data placed at cloud storages.The SP is responsible to maintain data security and privacy. The service provider needs to ensure data confidentiality, integrity and availability using the security measures such as data encryption and access control.
3. Data in use: This phase denotes the data when retrieved and manipulated by the cloud services. The major issue in this phase is data may be corrupted while manipulation [7].
4. Data remanence : Other significant and ignored issue is data remanence [13]. It is the residual representation of data that remain after deleting files [14]. After reformatting the storage media, there may be some physical properties that enable recovery of the previous contents [14, 15]. Data is securely erased at the end of its useful life by the service provider. In addition to the above phases, data lineage (tracing the data flow) is also essential for compliance analysis and auditing in clouds [13].

With the proliferation of digital devices and social media the size of data generated, integrated, manipulated, analyzed and stored is increasing daily. This poses lots of challenges in the BD security for users and SPs [16]. 80% of large enterprises suffered from major security problems with BD by 2016 [17]. Most of the massive-scale data are not in structured formats which make it more problematic to process with the existing software today [18]. Actually, the modern security tools like DMZs and firewalls cannot be employed in the BD environment since the security tools should be extended beyond the organizational boundary to satisfy the customer/data mobility demands and strategies. Bearing these new scenarios in mind, the relevant question is which security and privacy techniques are more sufficient to meet BD privacy and security requirements [19]. Being BD such an imperative and complex topic, it is usual that several security and privacy issues will arise. These issues have a straightforward effect on the development of solutions that need to manage all the security features and demands.

Big Data Working Group at the Cloud Security Alliance organization (CSA) has focused on the key issues to use secure BD services [19]. CSA has characterized security and privacy issues into four different facets namely (i) infrastructure security (e.g. security for non-relational databases, distributed programming models using Map Reduce), (ii) data privacy (e.g. cryptographic methods for privacy preserving data analytics), (iii) data integrity and management (e.g. data provenance, granular audits, logging transactions) and (iv) reactive security (e.g. end-to-end validation, monitoring the security level in real time). In BD environment, there are some vulnerable areas to security breaches such as data generation and collection process, data lifecycle and the lack of security measures that need to be addressed.

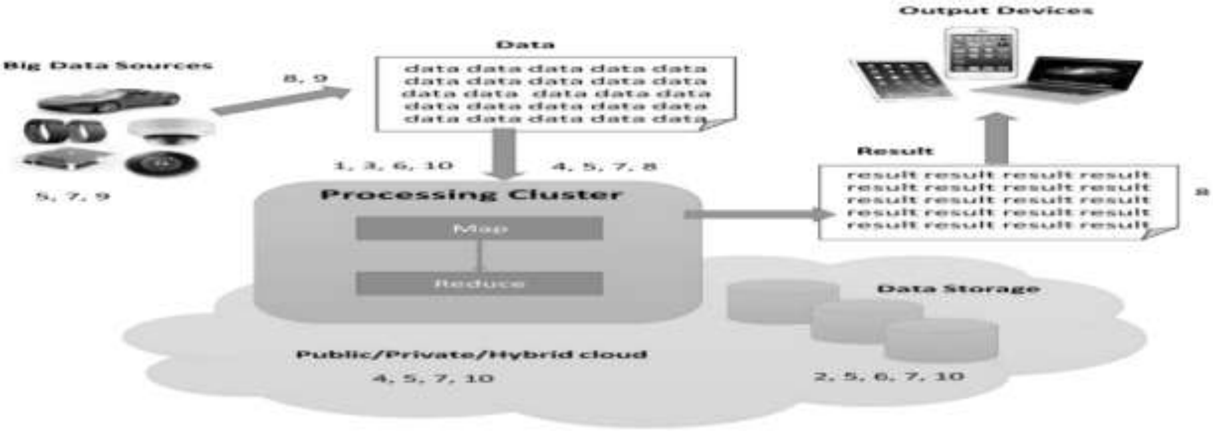

Figure 3. Security and Privacy issues in BD environment

VI. EXISTING SOLUTIONS TO ENFORCE SECURITY AND PRIVACY POLICIES

We cannot expect a single magical solution to resolve all the identified BD security and privacy issues since conventional methods are mostly devoted to secure small size of static information. They are not sufficient to the new rudiments enforced by BD services [19]. Illegal information retrieval to that data to generate new relations, integrate various resources and make it accessible to illegal customers is a severe threat for BD. The simple and more common solution for this issue is encrypting everything to secure data irrespective of where the data exist in (i.e. data centre, PCs, mobile device, or any other).

As BD develops and it's processing gets faster, then encryption, tokenization and masking are critical components for defending sensitive information. Due to these properties, organization essential to take a holistic view to the implementation of security schemes [20]. These projects need to consider the identification of the various sources, producers of data, and who is authorized to retrieve the information. It is also important to implement an accurate classification technique to recognize critical data, and align with the organizational security policies in terms of imposing authorization and data management strategies.

As a recommendation, various security methods should be closer to the data resources and data itself, to provide security control at the data sources, data loss protection and access control should collaborate [21]. Thus, a reliable data provenance technique should be implemented across domains. Furthermore, efficient methods should be implemented to alleviate distributed denial-of-service attacks forced against BD environments [22]. Similarly, BDsecurity and privacy is required to certify data reliability over its complete life cycle. Hasan et al. discussed the customization characteristic of BD services and its influence on the data privacy [23]. The authors address these concerns in the background of EEXCESS project for preserving user privacy. Jutla et al. describes privacy extensions to UML to aid information technologist to rapidly envisage privacy requirements, and develop privacy tools in BD services [24].

While trying to store and use BD, organizations need to certify that they have methods in position which enable them to satisfy legal requirements for data security, particularly for data-at-rest. Applications must comprise of two important points (i) secure encryption method must be implemented to secure all the confidential data such as intellectual property, personal sensitive information, and protected health information; (ii) careful method to control encryption key access which are used to unlock the encrypted data. The effectiveness of these methods depends on its practical transparency and its influence on efficiency and scalability of data [25].

As mentioned earlier, conventional cryptographic and data anonymization techniques are not sufficient to resolve BD complications. They are sufficient to secure data at rest, but are not sufficient when data in motion or data in use [26]. Hence, additional methods need to be employed to secure data in those phases. Modern techniques such as fully homomorphic encryption (FHE) [27], secure function evaluation [28] and functional encryption [29] are implemented to remove the restrictions of conventional security methods.

FHE is a cryptographic technique that enables definite forms of calculations to be performed on cipher texts and produce succinct encrypted answer [30, 31]. FHE permits encrypted inputs on databases, which retains personal user data [32]. It allows the customer to submit an encrypted query and the search engine generates a brief encrypted answer without understanding the meaning of the cipher text which could encompass personal sensitive data (e.g. health records). FHE allows a customer to save encrypted data on a remote file server and can access the data later only that meet certain Boolean condition. Processing queries against an encrypted database is one of the fundamental security requirements for

BD. This raises some inquiries like (i) Is the database encrypted using one or more keys? (ii) Do the queries require to be encrypted? (iii) Does the database need to be decrypted prior to its execution? (iv)Who has the authorizations to access the information? and so on.

Of late CryptDB was designed at Massachusetts Institute of Technology to provide provable confidentiality for database-backed applications. CryptDB enables users to execute SQL queries through encrypted data [32] using powerful SQL-aware encryption strategy. CryptDB adopts many types of encryption strategy that enable various kinds of cryptographic calculation on the data [33]. Reliable applications that intent to request encrypted data will transfer their queries to a database proxy (which is placed between the database server and the application server) which rewrites queries to run on encrypted data. The proxy performs cryptographic operations on all the data and changes some query operators, while preserving the semantics of the query.The database directs these cipher texts as a result back to the database proxy server, whose keys will allow decrypting the results, directing the final result back to the application server. Google has designed the Encrypted Big Query Client that will provide client-side encryption for a subset of query types using encryption techniques similar to CryptDB [34].

Besides more precise security references, the security of the organizational infrastructure also need to take into account. The common security practice is to implement security and privacy controls at the edge devices of the networks (which provide an access point to the organization or SP's core networks) but, if an invaders break security rules they will retrieve all the information within it. Hence, a powerful method is essential to shift those security and privacy controls close to the data. Observing, evaluating and learning from data usage are consider as vital features to constantly enhance security of the storage system and control the prevailing security methods[35, 36].

VII.CONCLUSION

This paper provides an elucidation of the research performed to identify the core issues associated to security and privacy in BD, and how investigators are handling these issues. We discovered that those primary issues are interrelated to the intrinsic properties of a BD environment. This study described the fundamental concept, primary challenges, and some security and privacy methods of BD. Our work exhibits that the present existing security and privacy-preserving methods for BD are still not mature. The best way to resolve these issues is to integrate various scientific methods, related policies, and privacy-preserving laws. Then, the issue of BD security and privacy will be explained better.

REFERENCES

[1] Gil,D. Song, I.Y.2016. Modelling and management of big data: Challenges and opportunities. Future Gener. Comput. Syst. 63 (2016) : 96–99.

[2] Big data: science in the petabyte era, Nature 455 (7209): 1, 2008.

[3] Philip Chen, C.L. Zhang, C.Y. 2014. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data, Information Science 275 (2014):314–347.

[4] EMC Digital Universe Study, with data and analysis by IDC, 2014.

[5] Armbrust, M., Fox, A., Griffith, R. et al.2010. A view of cloud computing, Communication ACM, 53 (4) : 50–58.

[6] Zissis, D. Lekkas, D. 2012. Addressing cloud computing security issues, Future Generation Computer.System, 28 (3):583–592.

[7] Worlanyo, E.2015.A Survey of Cloud Computing Security: Issues, Challenges and Solutions.

[8] An Oracle while Paper, "Advanced Analytics in Oracle Database" www.revolution-nalytics.com.

[9] Sophia, Y. Vijay, G. Nabil, S. Emily, S. and Arkady, Y.2014. A Survey of Cryptography Approaches to Securing Big Data Analytics in the Cloud, MIT Lincoln Laboratory.

[10] Rouda, N.,Senior Analyst, White Paper, Getting Real About Big Data: Build Versus Buy Enterprise Strategy Group.

[11] Rouda, N. ,Senior Analyst, ESG White Paper, Getting Real about Big Data: Build Versus Buy, Enterprise Strategy Group.

[12] Xiao,Z. and Xiao, Y. 2013.Security and privacy in cloud computing," IEEE Trans. on Communications Surveys and Tutorials, 15(2) : 843–859.

[13] Bhadauria, R., Sanyal. S,2012. Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. – International Journal of Computer Applications, 47(18): 47-66.

[14] Sabahi, F.2012. Secure Virtualization for Cloud Environment Using Hypervisor-Based Technology. – International Journal of Machine Learning and Computing, 2(1): 39-45.

[15] Gallagher, P.R.1991. A Guide to Understanding Data Remanence in Automated Information Systems. The Rainbow Books. Chapter 3 and 4. 1991.

[16] VenkataNarasimha Inukollul , Sailaja Arsi1 and Srinivasa Rao Ravuri,2014. Security Issues Associated with Big Data in Cloud , International Journal of Network Security & Its Applications (IJNSA), 6(3).

[17] Elmustafa Sayed Ali Ahmed1 and Rashid Saeed, A. 2014. A Survey of Big Data Cloud Computing Security. International Journal of Computer Science and Software Engineering (IJCSSE), 3(1): 78-85.

[18] Neha Upadhyay , Ajay Kumar.2014. A Framework based on Authentication and Authorization to ensure Secure Data Storage in Cloud, International Journal of Computer Applications, 90 (15): 0975 – 8887.

[19] Cloud Security Alliance. (2013). Expanded Top Ten Security and Privacy Challenges. Retrieved from https:// downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_ Challenges. pdf.

[20] Tankard, C. 2012. Big data security. Network Security, 2012(7): 5–8. doi:10.1016/S13534858(12)70063-6.

[21] Kindervag, J., Balaouras, S., Hill, B., &Mak, K.2012. Control And Protect Sensitive Information In the Era of Big Data.

[22] Luo, H., Lin, Y., Zhang, H., & Zukerman, M.2013. Preventing DDoS attacks by identifier/locator separation. IEEE Network, 27(6): 60–65. doi:10.1109/ MNET 2013.6678928.

[23] Hasan, O., Habegger, B., Brunie, L., Bennani, N., &Damiani, E. 2013. A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case. In 2013 IEEE International Congress on Big Data. IEEE. doi:10.1109/BigData.Congress.(13): 25–30.

[24] Jutla, D. N., Bodorik, P., & Ali, S. 2013. Engineering Privacy for Big Data Apps with the Unified Modelling Language. In 2013 IEEE International Congress on Big Data. IEEE. doi:10.1109/BigData.Congress.2013(156): 38–45 .

[25] Advantech.2013. Enhancing Big Data Security. Retrieved from http://www.advantech.com.tw/nc/newsletter/ whitepaper/ big_data/big_data.pdf.

[26] MIT. 2014. Big Data Privacy Workshop, Advancing the state of the art in Technology and Practice - Workshop summary report. Retrieved from http://web.mit.edu/bigdatapriv/images/MIT Big Data PrivacyWorkshop2014 _ final 05142014. pdf

[27] Gentry, C. 2009. A fully homomorphic encryption scheme. Stanford University. Retrieved from http://cs.au.dk/~stm/local-cache/gentry-thesis.pdf.

[28] Lindell,Y.&Pinkas, B.2002. Privacy Preserving Data Mining. Journal of Cryptology,15(3):177–206. doi:10.1007/s00145-001-0019-2.

[29] Goldwasser, S. Gordon, S. D. Goyal, V. Jain, A. Katz, J. Liu, F.H. Zhou, H.S. 2014. Multi input functional encryption: In Advances in Cryptology EUROCRYPT (2014) : 578–602.

[30] Gentry, C. 2010. Computing arbitrary functions of encrypted data. Communications of the ACM. doi:10.1145/1666420.1666444.

[31] Van Dijk, M. Gentry, C. Halevi, S. and Vaikuntanathan, V. 2010. Fully homomorphic encryption over the integers: In Advances in Cryptology– EUROCRYPT ’10: 24–43. doi:10.1007/978-3-642-383489_20.

[32] Popa, R. & Redfield, C. 2011. Cryptdb: protecting confidentiality with encrypted query processing. Proceedings of the …, 85–100. doi:10.1145/2043556.2043566.

[33] Popa, R. & Redfield, C.2012. CryptDB: Processing queries on an encrypted database. Communications of the …, 55, 103. doi:10.1145/2330667.23306.

[34] Google 2014. Encrypted Big Query Client. Retrieved August 03, 2014, from https://code.google.com/p/encrypted-bigquery-client

[35] Kindervag, J. Balaouras, S. Hill, B. & Mak, K. 2012. Control And Protect Sensitive Information In the Era of Big Data.

[36] Kindervag, J. Wang, C. Balaouras, S. & Coit, L. 2011. Applying Zero Trust To The Extending Enterprise.