Journal of Engineering and Applied Sciences 14 (2): 539-544, 2019
ISSN: 1816-949X

Cloud Security and Forensic Awareness Survey: An Empirical Analysis

[1]Sugandh Bhatia and [2]Jyoteesh Malhotra
[1]Department of Computer Science, Guru Nanak Dev University, 143005 Amritsar, India
[2]Department of Computer Science and Engineering GNDU Regional Campus,
144007 Jalandhar, India

Abstract: Cloud computing has become extremely popular technology for the allocation of resources dynamically. New technologies, performance measurements and improvements for the extension and expansion of the cloud services are being developed. In this research, the researchers discuss the outcome and analysis of a survey that had been conducted among cloud computing users, information technology experts and researchers on cloud security, privacy and forensic proficiency in order to analyse the principal issues of cloud computing based on 105 responses of the survey.

Key words: Investigation, survey, digital forensics, security and privacy, computing, proficiency

INTRODUCTION

Cloud computing furnishes through a progressive way of delivering IT services in form of computing, storage, analytics, machine learning, network security and IoT. In addition to the many benefits of providing such resources, the issues related to data security and privacy is pivotal. The study of Crisp research, Germany reveals that 40% of the study participants refused to avail the cloud services due to the reason of security and privacy of data. Development and execution of cloud involves high running cost. Moreover, cloud security, data privacy, compliance readiness and cloud forensic are those research and development areas in computer science which requires huge investment and deployment of highly skilled computer scientists and engineers. The outcome of these research projects is not definite. Therefore, less cloud companies are interested in these projects. The major concentration of cloud service providers is to give more and more services to their clients. The overall emphasis of the cloud company should be on data privacy and security, rather than increase in the number of clients. To protect data and resources in cloud computing various mechanisms or techniques are available and will be discussed in the section 2 of this study entitled as literature survey. Cloud security and forensic perform the important role in the successful execution of cloud system. To provide the security and privacy, different methods can be applied and to find out the lapse occurred in the system, cloud forensic perform a significant role.

Literature review: Some of the advised methods have been explained in the literature survey for managing and organizing security issues in the cloud computing. Munoz *et al.* (2013) recommended the strong contextual nature of the concept of security and privacy in cloud computing. The researcher emphasized on the division of cloud security mechanisms and generation of taxonomy in terms of threats, risks and vulnerabilities in the cloud.

Fehling *et al.* (2014) suggested a cloud application and the cloud environment. Both these entities denoted the diversions between the cloud service provider and customer. Moreover, the focus of the researchers was on cloud computing patterns which include presentation layer, data layer, memory and virtualization.

Soares *et al.* (2014) discussed another security mechanism which is dependent on the classification of previous solutions and their use. This method was practically oriented and developed to execute secure cloud systems.

Popovic *et al.* (2011) explained the privacy and security issues in the cloud system along with the pre requisites and threats that are confronted by the service providers in the cloud system during the services. Juels and Parno (2013) suggested "Proof of Retrievability" model which is based upon technique of correcting codes. These correcting codes are applied while retrieving the data. It is not feasible for the user to examine the data every time. Therefore, there is a dire need of a mechanism which can be applied at any level or application in the cloud computing environment.

Corresponding Author: Sugandh Bhatia, Department of Computer Science, Guru Nanak Dev University, 143005 Amritsar, India

Malozemoff *et al.* (2014) suggested a framework for attribute based encryption that reduces overhead effectuated by ABE decryption process. The required time for the conversion of plain text in to cipher text and vice-versa is dependent upon the complexness of retrieval mechanism. The researchers framework can convert the ABE cipher text into the fixed size cipher text and the major advantage is that no message is explored by the cloud during this process.

MATERIALS AND METHODS

The survey was conducted by the researchers of Guru Nanak Dev University, Amritsar, India. Total number of participants are 105. Data regarding the demography of the participants is collected initially. The major components of the survey are classified into four categories:

- Section 1 demographic information
- Section 2 cloud computing, models and its types along with applications
- Section 3 cloud security, privacy and forensic readiness
- Section 4 cloud security and forensic capabilities, tools and techniques

In section 1, the details are taken regarding the age, sex, qualification, department and nature of job or work of the participant. In section 2, the significance of cloud computing, its terminology, impact, models and services are discussed along with difference between traditional approach and modern approach of computing.

In section 3, the questions cover the various aspects of security, privacy and forensic readiness. Requirement of privacy models in the cloud computing, service level agreements, cryptography and its types are the prominent areas of discussion at this level.

In section 4, the questions revolved around the tools, techniques, frameworks and architectures of cloud security and forensic capabilities. At this level, guidelines, policies and agreements between cloud service provider and clients are included in the survey.

RESULTS AND DISCUSSION

Section 1-demographic information: The 105 participants are covered in the survey. These participants are classified into three categories on the basis of age. It is shown with the help of Table 1.

Table 1: Categories on the basis of age

Age group	No. of persons
18-25	32
26-31	45
32-40	28

Table 2: Levels of education

Education level	No. of persons
Graduate	42
Post graduate	49
PhD	14

30% participants fall in the category of 18-25 of age group. 43% participants are of the group 26-31 and 27% of the sample size covered in the group of 32-40. These 105 participants can be further classified in to three groups on the basis of level of education. It is shown with the help of Table 2. The 40% of the sample size falls in the category of graduation. The 47% of the participants covered in the category of post-graduation and 13% of the respondents are the research scholars of different faculties. The demographic outcome of the survey reveals that participants are literate and well educated. Moreover, they have experience in the field of cloud computing, information technology and availing the services of cloud computing like SAAS, PAAS and IAAS. The 65% of the participants agree that cloud computing is an emerging and important paradigm of information technology. They are satisfied with the definition of cloud computing given by gartner.

"Cloud computing is a style of computing where scalable and elastic IT related capabilities are provided 'as a service' to multiple external customers using internet technologies." The 35% of the respondents strongly agree with the definition of cloud computing given by NIST (Mell and Grance, 2011). "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable resources".

Since, cloud computing originated as the latest technology and new paradigm of information technology. It has been providing a significant technological change towards furnishing computational capability as a service. Moreover, it provides a huge variety of benefits and advantages compared to earlier or traditional method of computing like cost control, effectiveness and expandability.

Section-2

Cloud computing as a new paradigm of information technology: The 105 participants are involved in the survey and 75% of the respondents strongly agree

that cloud computing is an important paradigm of information technology. Only 25% of the respondents agree that cloud computing is a novel method of providing computing services and it is not a new technology. Cloud computing can be considered as one of the most transformative technology in the modern world. Gartner forecasts that worldwide public cloud services revenue would be more than $ 302 bn by 2021. The idea of cloud computing was given in 1960s from the concept of J.C.R. Licklider, who performed an important role in the deployment of ARPANET and contemplated computation as an universal network. John McCarthy is another person who contributed a lot in the development of cloud computing. He gave the concept of 'Artificial intelligence' based computing. One of the most important advantage of cloud computing is cost reduction but major hindrance in the growth of cloud computing model is the lack of security and privacy models. In every sphere of computing and life, cloud based models have been applied. Some experts believe that cloud computing is the advance phase of computing which leads to more effective and accurate computing. Proper implementation of security, privacy and compliance readiness are the major problems and must be removed.

Cloud forensic definition: The 105 respondents participated in the survey on the basic terminology of cloud forensics. The 74.28% of the respondents strongly agree that cloud forensics is "the application of digital forensics in cloud computing which is based upon computer forensics, hardware forensics and network forensics (Messier, 2017). On the other hand, 25.72% of the participants believe that it is a new area which revolves around traditional computer forensics. NIST cloud computing forensic science working group information technology laboratory has defined cloud forensics as "Cloud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence". The definition of cloud forensics is closely associated with the definition of cloud computing. The outcome of this survey reveals that cloud forensics is an amalgamation of digital forensics, hardware forensics, network forensics and digital device forensics. As the structure or working of the cloud computing is primarily dependent upon internet connectivity and services. Therefore, it can be called as a modern technique which is still evolving and it is possible that cloud forensics would disclose many hidden patterns and areas in the field of digital forensics.

Section-3

Implications of cloud forensics: The 105 participants involved in the survey and answered various questions on the importance and implications of cloud forensics. 81.90% of the participants strongly agree that cloud forensics is the most important element of cloud security and cloud computing model. The 18.10% of the participants agree that cloud forensics is a complex and tedious task to perform and requires more funds for the working, deployment, research and development. Moreover, clients of the cloud service providers are not so aware and never feel the utility for security and privacy, until or unless a security breach happens. Result of this section of the survey divulges that the participants are cognizant of the requirement, importance and implications of cloud forensics. But they are not able to handle or understand the complexities of cloud forensics (Zawoad and Hasan, 2016), security and privacy due to lack of technicalities involved in the mechanism.

Inter-relationship between cloud computing and digital forensics: The 102 participants replied on the questions of inter-relationship between cloud computing and digital forensics. The 64.76% of the respondents agree that it is very difficult to apply the combination of digital forensics and cloud forensics in the cloud computing environment. 28.57% gave the consent in favour of that it is easy to perform digital forensics in the cloud computing model where as 6.66% of the participants were unable to answer any question. Main issues raised by the participants during the survey are discussed below. The issues are classified in to two categories. Here, we are discussing the issues raised by 64.76% of the participants which said that it is difficult to apply digital forensics:

- Non-availability of standard interfaces
- Complex data recovery system
- Limited access to distributed and remote storage, computing resources and infrastructure
- Difficult to control and locate the data
- Due to segregated evidences

Table 3: Cloud basesd system

Challenge	Agreedrespondents(%)
Lack of uniformity of approaches in the cloud computing models	89.52
Terms and conditions in service level agreements are not clear	82.86
Segregated nature of cloud data and availability of multiple users	79.04
Scarcity of personnel in the field of digital forensics	72.38
Gigantic growth in the size of cloud based devices	70.48
Jurisdiction and legislative problems due to structure of cloud system	69.52
Consolidation of log formats	66.67
Lack of co-ordination between CSP and user	62.86
Intrusion detection and prevention mechanisms are not adequate	58.09
Due to awareness of user	57.14

The 28.57% of the participants gave their points in the favour of digital forensics (Gladyshev and Rogers, 2012). According to them, it is easy to control and implement due to the following issues:

- Cloud security and forensics services can be outsourced as per the requirements
- Not possible to destroy or modify the evidences as these may be stored on multiple locations
- Economically it is feasible and favourable for the organization to apply the cloud security and privacy model
- Inter-relationship between the entities in the cloud makes it easy to investigate for investigation team

Section 5

Multifarious aspects of cloud forensics: The 105 participants answered various questions on the topic of aspects of cloud forensics. The 73.33% of the participants strongly agree that the aspects of cloud forensics are multi-dimensional. It includes various aspects like technical, social, legal, organizational, political and personal. On the other side, 26.67% of the respondents did not participated in this section of survey. Lack of knowledge is one of the major reasons of less participation in this section. Basically, the aspects of cloud forensics can be classified in to two categories, first is personal and other is non-personal. Personal aspects can be controlled or managed by the user. In other words, it can be said that over all control of these aspects in the hands of user. Under the non-personal, the major aspects are political, social and legal. User has no control on these aspects. It is need of the hour that the user or client must be aware about all the aspects of cloud forensics.

Cloud forensics applications: Application is the most important criteria to verify the usability of technique or technology. The 105 participants are again questioned on the topic of applications or usability of cloud forensics. The 55.24% of the respondents strongly agree that cloud forensics is an important technique for investigating the digital crimes, privacy or security breach, policy violations and civil or criminal cases. The 44.76% of participants said that besides the investigation, cloud forensics techniques can also be applied for compliance readiness, regulatory compliance, log monitoring and troubleshooting. From the above discussion, it is clear that cloud forensics and digital forensics are interlinked with each other. Sometimes, cloud forensics is considered as an application of digital forensics. Moreover, investigations in the cloud forensics can be classified in to two categories: internal and external investigation. An investigation which is controlled or managed by the cloud service provider itself is covered under the category of internal investigation. It can be initiated for investigating the security or privacy breach, regulate the compliance, policy violations and log monitoring. The whole process of investigation is performed with in the organization without taking any support of external agency. On the other side, in case of external investigation, entire process of investigation is outsourced. One or more agencies can be given the assignment to perform the investigation on behalf of the organization. In this case, it is the prerogative of the external agency to select tools or techniques for the investigation.

Challenges in cloud forensics: The 105 participants have given their answers on the objections and challenges of cloud forensics. We included 10 important challenges in the questionnaire for this part of survey. The 87.62% of the respondents strongly agree that all these 10 challenges are really significant. These challenges along with percentage of agreed respondents are discussed in Table 3. With the expansion and extension of cloud based services and applications, more and more challenges are faced by users and cloud service providers. Most of the challenges and objections are related with security, privacy, compliance readiness, service level agreements, policy violations and threats detection in cloud system. It is expressed in an impressive way with the help of Table 3.

Table 3 reveals that among 105 respondents in the survey a large number of participants agreed that cloud computing and forensics is facing various types of challenges and objections at various levels in the cloud based systems. For the proper and perfect functioning of cloud systems, all these challenges should be taken very seriously by the cloud service provider and users.

Growth avenues of cloud forensics: In comparison to the challenges discussed above, 43.81% of the respondents are unaware regarding the new growth avenues of the cloud forensics. The 40% of the participants strongly agree that security as a service and forensic as a service (Eleyan and Eleyan, 2015) can be new avenues of growth in the field of cloud and digital forensics. Moreover, cloud forensic as a service would be cost effective and economically feasible for the organization, if implemented in an effective manner. The 69.52% of the participants believe that the standards and protocols in the cloud security and forensics must be uniform and homogeneous in nature. There is a dire need that cloud security, privacy and forensics models, standards and frameworks must be scalable and extendable, 83.81% of the participants are in favour of this statement.

Main findings of the study: The 90.48% of the respondents strongly agree that methodology performs an important role in the forensic procedure. Methodology includes the selection of models, algorithms, techniques and tools used for cloud forensics. The 82.86% of the participants believe that the source of data and evidence mounts a strong basic structure for the reliable forensic process. The 75.24% of the respondents strongly agree that the methodology along with set of tools and techniques are equally important in the field of cloud forensics and digital forensics. The 94.28% of the participants are in the favour of recruitment of cloud forensic experts in the organizations which are availing and providing the cloud services. Hence, a separate wing or department of cloud forensic must be created in all the organizations which are directly or indirectly associated with cloud computing.

CONCLUSION

The research study is based on the primary data and analysis of the data depicts that nowadays cloud computing is being applied in every field of computing. security, privacy and cloud forensics tools and methods are required in every sphere of cloud application. It is need of the hour that cloud service providers like Amazon, Microsoft Azure, Google, Adobe and VMware should organize seminars, workshops, conferences and technical sessions to train young faculty members and researchers in the Universities and Institutes. More participation must be from the faculties like social science, architecture, natural science and business management as a major portion of the users belong to this category and they have less exposure in the field of cloud security, privacy and forensics whenever compared with the person from the background of computer science and technology. Cloud forensic may be considered as an extension of digital forensic. Digital forensic is a challenging technique itself and therefore, cloud forensic encompasses more challenges than digital forensics. 92.38% of the participants who are using cloud models and applications are unaware regarding the issues, problems and risks of privacy and security in cloud computing. Moreover, 72.38% users said that they have heard about the concept of digital and cloud forensics but they are not able to understand the technicalities and concepts of forensics. On the priority basis, cloud forensics techniques must be imparted through the training and education at the college and university level among faculty members and research scholars. However, cloud forensics accelerates the level of tools, techniques and methods used in the cloud computing at various levels.

LIMITATIONS

This survey is conducted by the researchers of Guru Nanak Dev University, India. Cloud forensics is still an emerging technique and requires more research in this field. Participants covered under this survey tried well to answer the questions as they are using various models and applications of cloud computing, but lack of knowledge in the field of cloud forensics clearly reveals that user must devote some time to learn various tools and techniques which can be useful in securing and protecting data and resources over the channel along with cloud forensics mechanism. Sometimes participants feel fluster and uncomfortable to answer the questions due to the technicalities involve in the survey and size of questionnaire.

RECOMMENDATION

Future research prospective: Among 105 participants of this survey, 98 respondents participated in this section. The 90.81% strongly agree that cloud forensic is one of the most important and emerging area of research in the field of cloud computing. Cloud forensic model, architecture, cryptography, steganography (Kipper, 2004), compliance readiness, cloud collaboration and cloud security are the important and popular fields of research and development now a days. The 91.84% of the participants agree that there is an exigency of artificial intelligence based applications in the cloud security, privacy and forensics. The domain of cloud forensics must be enhanced and more entities should be covered under cloud forensics. Most of the times, it has been noticed that following major entities are covered under the cloud forensics:

- Cloud service provider
- Cloud user
- Cloud broker
- Law enforcement agencies
- Forensic experts
- Cloud intermediates

REFERENCES

Eleyan, A. and D. Eleyan, 2015. Forensic Process as a Service (FPaaS) for cloud computing. Proceedings of the 2015 European Conference on Intelligence and Security Informatics (EISIC), September 7-9, 2015, IEEE, Manchester, England, ISBN:978-1-4799-8657-6, pp: 157-160.

Fehling, C., F. Leymann, R. Retter, W. Schupeck and P. Arbitter, 2014. Cloud Application Architecture Patterns. In: Cloud Computing Patterns Fundamentals to Design, Build and Manage Cloud Applications, Fehling, C., F. Leymann, R. Retter, W. Schupeck and P. Arbitter (Eds.). Springer, Vienna, Austria, ISBN:978-3-7091-1567-1, pp: 151-238.

Gladyshev, P. and M.K. Rogers, 2012. Digital Forensics and Cyber Crime. 1st Edn., Springer Berlin, Germany, ISBN:978-3-642-35515-8, Pages: 297.

Juels, A. and B. Parno, 2013. Fifth ACM cloud computing security workshop (CCSW 2013). Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, November 04-08, 2013, ACM, New York,USA., ISBN:978-1-4503-2477-9, pp: 1487-1488.

Kipper, G., 2004. Investigator's Guide to Steganography. Auerbach Publications, Boca Raton, Florida, ISBN:9780849324338, Pages: 220.

Malozemoff, A.J., J. Katz and M.D. Green, 2014. Automated analysis and synthesis of block-cipher modes of operation. Proceedings of the 2014 IEEE 27th Symposium on Computer Security Foundations (CSF), July 19-22, 2014, IEEE, Vienna, Austria, ISBN:978-1-4799-4290-9, pp: 140-152.

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing. National Institute of Standards and Technology, Gaithersburg, Maryland. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Messier, R., 2017. Network Forensics. John Wiley & Sons, New York, USA., ISBN:978-1-119-32918-3, Pages: 335.

Munoz, A., A. Mana and J. Gonzalez, 2013. Dynamic Security Properties Monitoring Architecture for Cloud Computing. In: Security Engineering for Cloud Computing: Approaches and Tools, Rosado, D.G. (Ed.). IGI Global, USA., ISBN:978-1-4666-2125, pp: 1-18.

Popovic, O., Z. Jovanovic, N. Jovanovic and R. Popovic, 2011. A comparison and security analysis of the cloud computing software platforms. Proceedings of the 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), October 5-8, 2011, IEEE, Nis, Serbia, ISBN:978-1-4577-2018-5, pp: 632-634.

Soares, L.F.B., D.A.B. Fernandes, J.V. Gomes, M.M. Freire and P.R.M. Inacio, 2014. Cloud Security: State of the Art. In: Security, Privacy and Trust in Cloud Systems, Nepal, S. and M. Pathan (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-38585-8, pp: 3-44.

Zawoad, S. and R. Hasan, 2016. Cloud Forensics. In: Encyclopedia of Cloud Computing, Murugesan, S. and I. Bojanova (Eds.). John Wiley & Sons, Hoboken, New Jersey, USA., ISBN:9781118821978, pp: 233-244.