2015 IEEE 7th International Conference on Cloud Computing Technology and Science

Security and Privacy in Cloud Computing via Obfuscation and Diversification: a Survey

Shohreh Hosseinzadeh*, Sami Hyrynsalmi*, Mauro Conti† and Ville Leppänen*
*Department of Information Technology, University of Turku, Finland
Emails: {shohos, sthyry, ville.leppanen}@utu.fi
†Department of Mathematics, University of Padova, Italy
Email: conti@math.unipd.it

***Abstract*—The development of cloud computing has facilitate the organizations with its services. This makes the security and privacy of the cloud even more significant. Diversification and obfuscation approaches are of the most promising proactive techniques that protect computers from harmful malware, by preventing them to take advantage of the security vulnerabilities. There is a large body of research on the use of diversification and obfuscation techniques for improving the security in various domains, including cloud computing. Cloud computing provides an excellent setting for applying diversification/obfuscation, as the computing platforms (virtual machines) are implemented in software.**

The main objective of this study is to determine in what ways obfuscation and diversification techniques are used to enhance the security and privacy of the cloud computing, and discover the potential avenues for the further research. To achieve this goal, we systematically review and report the papers that discuss/propose a technique to enhance the security and privacy of the cloud, using diversification and obfuscation techniques. As the result of the search we collected 43 papers published on the topic. In this report we present the process of data collection, analysis of the results, and classification of the related studies. The classification is done based on how the diversification/obfuscation techniques are used to enhance the security in cloud computing environment. The presented study gives a clear view of the state of the art of the existing works in the field, and sheds light on the areas remained intact which could be avenues for further research. The existing works cover surprisingly a small set of the wealth of opportunities for diversification/obfuscation.

***Index Terms*—cloud computing, security, privacy, obfuscation, diversification, systematic literature review**

I. Introduction

With the changes in the business models, new technologies have been adopted such as cloud computing. Furthermore, companies and organizations, these days, are dealing with more users and information. This makes the organizations more exposed to security risks. Enterprise security encompasses different aspects including: information security, business security, physical security, and operational risk management. In this paper, we focus on securing the information and data which is a crucial need for the organizations that lay their services over cloud environments.

Cloud computing is a model that enables the service providers to share services and computing resources to the users [1]. The services are offered based on three different models: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS). In IaaS, the service providers offer the services, including storage, processing, computing resources, and virtual machines. In PaaS, the cloud service providers offer computing platforms, e.g., operating system. In SaaS, the cloud service provider offers the applications that run on cloud and the clients access these applications through the client interface, e.g., the web browser. The development of cloud services on one hand has augmented the business, technology and government; on the other hand, has questioned security and privacy. Therefore, there is a significant exigency for the security: a) *for* protecting the cloud from the external intruder that imperils the cloud infrastructure, and b) protecting *from* the malicious/untrusted cloud (the data can be misused by the cloud without the user's consent). For these purposes, obfuscation/diversification techniques are helpful.

Code **Obfuscation** [2] is transforming the code to a semantically identical form. The idea is to make the code more difficult to comprehend by an adversary (even if the attacker has the source code in hand). For instance, in [3], [4], obfuscation is used to make the disassembly of the machine code and the reverse engineering harder.

Malware is malicious software that manipulates the user's computer towards the attacker's desire [5]. To achieve this goal, malware uses knowledge about how to access the computer's resources. Thus, by making this knowledge secret we can make the malware ineffective. Interface **Diversification** [6] is a promising technique for this purpose. The idea is to generate unique secret software interfaces for known reference interfaces, in a way that they appear differently, but function the same. Diversification always involves *propagation* of created secret interface instances to legal parties. Consequently, for the malware, the idea is not to remove the security holes but to prevent the malware to work, as it no longer knows the secret service interfaces of the system. Diversification has been applied previously on various interfaces including, OS kernel and system calls, libraries, functions, protocols, and on hardware platforms at machine language level. System call diversification [7] is an effective way of protecting OS from the intrusions. To protect the OS from buffer overflow attack, Chew and Song propose the randomization of the entry point and also the system call mapping in the kernel [8].

These two potential techniques can be used in cloud computing environment to overcome the possible security threats

978-1-4673-9560-1/15 $31.00 © 2015 IEEE
DOI 10.1109/CloudCom.2015.29

TABLE I
SEARCH RESULTS.

Database	Number of search results	Search Strings
IEEEXplore Digital Library	21	**In Title:** "Document Title": cloud AND ("Document Title": obfuscation OR "Document Title": diversification) **In Abstract:** "Abstract": cloud AND ("Abstract": obfuscation OR "Abstract": diversification)
ACM Digital Library	11	**In Title:** (Title: cloud) and (Title: obfuscation or Title: diversification) **In Abstract:** (Abstract: cloud) and (Abstract: obfuscation, or Abstract: diversification)
Wiley Online Library	2	**In Title:** (cloud) AND (obfuscation OR diversification) **In Abstract:** (cloud) AND (obfuscation OR diversification) **In keywords:** (cloud) AND (obfuscation OR diversification)
SienceDirect	12	**In Title, Abstract, and Keywords:** TITLE-ABSTR-KEY(cloud) and TITLE-ABSTR-KEY(obfuscation) TITLE-ABSTR-KEY(cloud) and TITLE-ABSTR-KEY(diversification)
SpringerLink	417	**In Full-text:** search for the exact phrase: cloud obfuscation
Total number:	473	

[9]. For instance, to prevent the data breach, to sufficiently secure the Application Program Interfaces (API), and to secure the shared infrastructures and applications.

The remainder of this paper is structured as follows: Section 2 discusses the method used for data collection. Section 3 includes the results and analysis of the results. Discussion comes in Section 4. Section 5 explains the limitations of the study and presents the conclusion.

II. SURVEY METHODOLOGY

In this study we collected the data using the method suggested by Kitchenham [10], which presents guidelines for conducting a Systematic Literature Review (SLR) in the software engineering domain. In the first phase we conducted an initial electronic search in five large databases in the field (the search was done on March 5th, 2015). Table 1 presents the search strings we used, and the number of hits we got in each database. After removing the duplicates the number of the papers dropped to 463. In the second phase, based on the title and abstract of the papers, we omitted the papers from the list which were irrelevant to our inclusion criteria. The inclusion criteria in this study are as follows: a) the articles written in English language, b) the articles that are in the context of cloud computing, c) the articles that discuss/propose a solution using obfuscation and/or diversification techniques, and d) the articles that aim at enhancing the security and privacy in the domain of cloud computing. After this phase we had 43 unique papers. In the final phase, the selected papers were reviewed, and data extracted from them. According to the extracted data, we classified the papers based on how they were discussing obfuscation/diversification techniques to improve the security and privacy of the cloud.

III. RESULTS AND ANALYSIS

Table 2 lists the selected papers that discuss the concept of "obfuscation" and "diversification" in the domain of security and privacy in cloud computing environment. Figure 1 depicts the classification of the selected papers based on: how the papers study/discuss the obfuscation and diversification techniques to enhance the security and/or protect the privacy in cloud computing environment. In the figure, the numbers between the parentheses shows the frequency of each category, i.e., the number of papers discussing the term. Literally, the techniques, obfuscation and diversification, were used in nine various ways with the aim of protecting the security and privacy, including: 1) noise obfuscation, 2) client-side data obfuscation middleware, 3) general data obfuscation, 4) source code obfuscation, 5) location obfuscation, 6) file split and stored on different clouds, 7) obfuscation through encryption, 8) diversification, and 9) cloud security through securing the browser. In the following we explain the presented terms in detail.

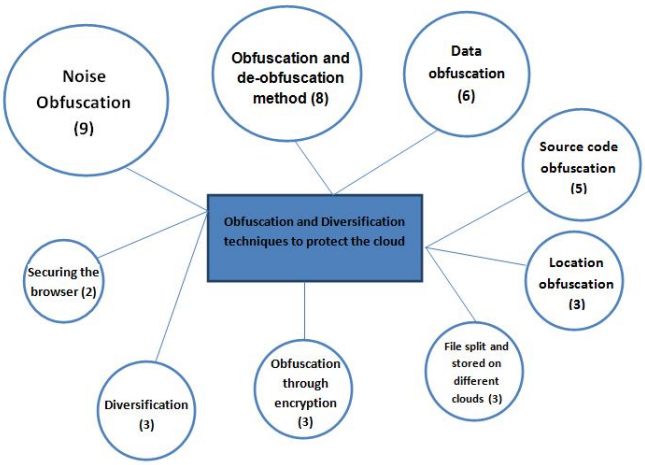

Fig. 1. Classification of the published papers on security and privacy through obfuscation and diversification, and frequency of each category.

1) **Noise obfuscation:** In this type of approach the aim is to confuse the malicious service provider by injecting noise requests into the customer's requests. The idea in this strategy is to make the occurrence probability of the noise and the real requests the same, so that they will not be distinguishable. In this way, it is difficult for the service provider to distinguish the original requests [11]–[18].

TABLE II: List of the selected papers. Based on how the papers use the obfuscation/diversification, they fall into nine different categories.

No.	Description of how the paper uses the "obfuscation" and "diversification" to provide security in cloud environment.
	Category 1: Noise Obfuscation
1	Noise obfuscation confuses the cloud by injecting noise requests in customer's requests and making it difficult to distinguish the original requests. The paper considers the privacy-leakage-tolerance in the process of noise obfuscation. [11]
2	For protecting the privacy in the data statistics and mining domain, this paper proposes obfuscation and noise generation techniques. In this obfuscation approach, the data is obfuscated without changing the characteristics. [12]
3	In order to preserve the privacy of the user and protect the data from the malicious cloud, Time-series Pattern Strategy Noise Generation (TPNGS) is proposed to make the client's real requests vague. The idea is to generate a pattern out of the previous requests and forecast the occurrence probability of the future ones. [19]
4	The noise obfuscation technique is proposed to deal with the privacy concerns about the customer's data. In this work, the occurrence probability fluctuation is taken into account. [13]
5	With a view to privacy protection, the paper considers the noise injection as a way to confuse the malicious cloud. [14]
6	The paper focuses on the obfuscation through noise generation to confuse the cloud to distinguish the real requests of the user. The proposed strategy attempts to make the occurrence probability of the noise and the real requests the same, so that they will not be distinguishable. [15]
7	In order to protect the privacy of the information sent from the user to the cloud, this paper proposes enabling oblivious transfer, homomorphic encryption, and query obfuscation schemes in the proxy. Query obfuscation refers to generating noisy or fake queries randomly to confuse the cloud provider. [16]
8	The privacy of the personal information of the user is protected via noise generation. The idea is to conceal the occurrence probabilities of the service requests. [17]
9	Noise generation into the real requests of user is discussed as a way to protect the privacy. [18]
	Category 2: Client-side data obfuscation middleware
10	Confidentiality of the data is achieved by encrypting or obfuscating the data (depending on the type of data) on the client side, before sending the data to the cloud. Encryption is applied on the alphabetics and tries to make the text unreadable; while the obfuscation is applied on the numerical types of data. [20]
11	The personal data of the user is encrypted and then sent to the cloud. Thus, all the processing is done on the encrypted data. In the end the result is sent back and de-obfuscated on the client side, and the user receives the plain result. [21]
12	They propose a way to ensure that the user's data is protected from the service provider, while the data is stored or being processed. For that purpose, they are using information hiding, data obfuscation, and separating the infrastructure service provider from the SW service provider in the cloud. In this approach the Data Obfuscator is a middle-ware provided by a user. It obfuscates the sensitive data using a secret key chosen by the user. The data is being processed in the obfuscated format on the cloud. Then the processed data is de-obfuscated on the user side by the Data De-obfuscator, so that the user can see the plain data. [22]
13	The paper presents a privacy manager for protecting the personal and confidential data. The data is obfuscated using a key selected by the privacy manager before being sent to the cloud, and the processed data is de-obfuscated on the user's side using the same key. It is called obfuscation rather than encryption because some of the original data is still present in the obfuscated version. the paper also presents an algebraic representation of the obfuscation. [23]
14	The paper presents a mathematical formulation of the obfuscation. Also introduces a privacy manager that relies on obfuscation and de-obfuscation technique. [24]
15	In the proposed privacy manager approach, obfuscation and de-obfuscation are used on the client side to control the amount of sensitive information sent to the cloud. The data is obfuscated before being sent to the cloud using a key chosen by the user. The key is kept secret from the service provider, i.e., the data is not de-obfuscated on the cloud. [25]
16	To protect the user's sensitive data from the service provider, the paper proposes to use obfuscation of the data on the client side before transmitting it to the cloud. The outcome of the processed data by the cloud is sent back to the user, and de-obfuscated there using the user's secret key. [26]
17	This paper proposes the privacy manager software that works on the client side. This software obfuscates some of the sensitive data of the user before sending to the cloud, according to the preferences of the user. [27]
	Category 3: General data obfuscation
18	The approach is called systematic obfuscation and tries to protect the personal data. The following obfuscations are proposed to be applied to the data-types: a) Transformation: replacing the information in a different format, b) aggregation, c) sub-setting: selecting a certain part of the data, and d) culling: omitting a certain part of the trace data. [28]

Continued on next page

TABLE II – continued from previous page

No.	Description of how the paper uses the ”obfuscation” and ”diversification” to provide security in cloud environment.
19	The paper presents a solution to protect the data privacy by securing the data stored in the cloud databases. The solution presented in this paper is the obfuscated access pattern leakage. [29]
20	Data obfuscation in this paper is introduces as a way of hiding the real identity of the user, to protect the privacy. After the identity is obfuscated, it can only be deciphered by the user himself. [30]
21	Data obfuscation is the technique suggested as a way to protect the data privacy is SaaS. [31]
22	In CNF (Conjunctive Normal Form) formula there exist some confidential information, e.g., circuit structure that should be protected from the unauthorized access. To this end an algorithm is proposed based on the obfuscation technique. [32]
23	User's behavior usually follow a pattern, which can be captured, analyzed and used for predicting the future behavior. This raises security and privacy issues. This paper proposes obfuscating this behavioral patterns of the users. [33]
24	Image obfuscation is one of the techniques proposed in this paper to hide an image (either by hiding the colors or position of the pixels). It integrates the compression with the secret sharing and generates n number of shadow images. [34]
	Category 4: Source code obfuscation
25	By development of cloud computing, new web services are being used more and more. JavaScript is a common language used in these services. In this paper an obfuscation technique is proposed for protecting the JavaScript code. [35]
26	The framework presented in this paper is based on evolutionary heuristics and is designed transform the C program's source code into an unintelligible form, to make it harder to reverse engineer. [36]
27	This paper surveys the obfuscation methods to make the software harder to reverse engineer. [37]
28	This work adds additional source code transformations to the JSHADOF framework. JSHADOF is a source to source transformation framework to obfuscate the JavaScript code in the web services of Cloud Computing environment. [38]
29	The paper proposes a threat-base obfuscation technique, using control-flow obfuscation and dummy code insertion. [39]
	Category 5: Location obfuscation
30	The paper discusses the identity privacy, content privacy and, location privacy to protect the private information of the user from being disclosed. Location obfuscation is the technique used to hide the location information of the user. [40]
31	The Location Services (LS) provide their services by accessing the user's location, which raises some privacy issues. This paper proposes the location obfuscation to imprecise the precise location of the user. [41]
32	In order to preserve the privacy of the user, this paper proposes the location obfuscation as a technique to hide the real location of the user and confuse the server. [42]
	Category 6: File split and stored on different clouds
33	The files are divided and stored on multiple cloud providers. This is considered as a way of data obfuscation because each of the service providers has a partial view of the whole file. [43]
34	In this work data obfuscation refers to splitting and storing the data on geographically separated data stores. [44]
35	In order to preserve the confidentiality of the data, they propose an obfuscation technique, in which the idea is to spread the data into various cloud providers. [45]
	Category 7: Obfuscation through encryption
36	Cryptography is discussed as the most common approach to achieve obfuscation. It can be done via secret sharing. [46]
37	Obfuscation in this paper is achieved through homomorphic encryption. [47]
38	The paper proposes the point function obfuscation which is based on one way hash function. [48]
	Category 8: Diversification
39	The paper proposes diversifying the cloud execution environment. The idea behind the moving target defense is to randomly and continuously alter the execution environment and configurations, to make it difficult for the attacker to discover the execution environment and its vulnerabilities. [49]
40	In this approach the execution environment and the type of platforms used to run them are continuously changing, so that by the time the attacker discovers the vulnerabilities of the execution environment, it has already altered. Additionally, to tolerate the possible attacks, they introduce hardware redundancy. [50]
41	The paper proposes the design diversity in the cloud. It studies the diversification of the configurations of virtual replicas to enhance the resiliency of the service in the presence of attacks. [51]
	Category 9: Cloud security through securing the browser
42	In this paper a web-browser plug-in is proposed to provide better security and privacy for the data on the cloud through double authentication and hybrid obfuscation techniques. The idea is to keep the data and the keys into different clouds with no direct relation between them. [52]
43	Obfuscation in this work is used to increase the session's life time. [53]

2) **Client-side data obfuscation middleware:** This method ensures that the user's data is protected from the service provider, while stored or being processed. In this regard, a privacy manager is designed as a middleware to obfuscate the sensitive data using a secret key chosen by the user. The data is sent to the cloud in the obfuscated format. Since the key is always kept secret on the client's side, the data is never de-obfuscated on the cloud. The result of the processed data is sent back to the user, and is de-obfuscated on the user side using the secret key, so that the user can see the plain data [20]–[27].
3) **General data obfuscation:** Obfuscation in this category is used to make the data hard to read, for instance, obfuscating the user's identity, the data stored on the cloud's database, and the behavioral pattern of the user (Related to the category 2) [28]–[34].
4) **Source code obfuscation:** In order to protect the cloud's software from the reverse engineering, source code obfuscation makes the code for the attacker harder to understand [35]–[39], [53].
5) **Location obfuscation:** Some services are provided based on the location information of the users; however, revealing this information raises privacy concerns. Obfuscation could be used as a technique to make the exact location of the user imprecise (Related to the category 3) [40]–[42].
6) **File split and stored on different clouds:** In this obfuscation strategy the data/files are divided into different parts and spread over different cloud providers. This approach is beneficial to assure the availability and the security of the data [43]–[45]
7) **Obfuscation through encryption:** Obfuscation could be achieved using cryptographic techniques, e.g., homomorphic encryption and one way hash function (Related to the category 2, 3) [46]–[48].
8) **Diversification:** Diversifying the cloud's execution environment continuously, shortens the chance and the time for the attacker to discover the execution environment and its vulnerabilities. Before the attacker acquires the knowledge about the execution environment it has already changed to a new one [49]–[51].
9) **Cloud security through securing the browser:** A plug-in on the web browser of the user can address the security and privacy of the data, through obfuscation and hybrid authentication [52], [53].

From the presented categories, the first seven categories attempt to provide protection *from* the (malicious) cloud, while the last two categories attempt to provide protection *for* the cloud from the possible threats.

IV. Discussion

Due to the fact that the techniques, obfuscation and diversification, are regarded as successful techniques in impeding the malware from making harm in many different domains, we were motivated to answer the question, "how these techniques could be used to boost the security in cloud computing environment". For this purpose, we conducted an SLR to study the existing works, find the gaps, and in the end to identify the the topics missed, which could be an agenda for the further research. As the result of our search we realized that there are fairly decent number of works (43 papers) studying the use of obfuscation and diversification techniques in cloud computing, aiming at enhancing the security and protecting the privacy. The papers were pursuing this purpose through different manners. Thus, we classified them into 9 various categories according to how they were using the aforementioned techniques to reach this goal. The presented categories are: noise obfuscation, obfuscation and de-obfuscation method, data obfuscation, location obfuscation, source code obfuscation, file split and stored on different cloud providers, obfuscation through encryption, diversification, and securing the browser.

Figure 2 presents the distribution of the selected papers published yearly from 2009 to 2015, in conferences and journals. The growing trend in the publishing rate shows the growing interest on using obfuscation/diversification in cloud computing for the security means.

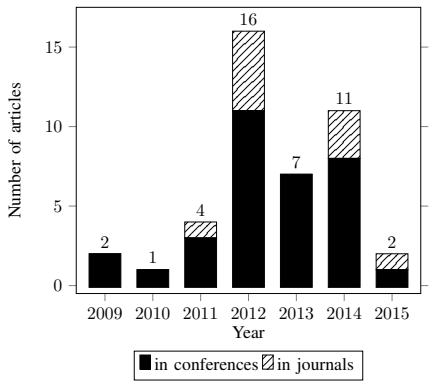

Fig. 2. Number of papers published yearly on the topic of security and privacy through obfuscation/diversification

While literature studies contribute to the field by reviewing and listing existing research, the aim is also to underline existing research gaps for further work. By surveying the selected papers and analyzing the collected data, we reached to several results:

- In most of the studied works, the cloud service provider is an untrusted party who may maliciously deduce the users' data without their consent. Therefore, in these works, obfuscation and diversification techniques are being used to protect the data "from the cloud", so as to preserve the privacy of the users.
- In the majority of the papers, the main objective of using obfuscation and diversification techniques was to preserve the privacy of the users through protecting the data.
- Most of the proposed approaches present their security measure at the client side rather than the server side, e.g, by obfuscating the data before sending to the cloud, and

protecting the web-browser of the user using obfuscation techniques.

- The papers were mostly interested in using the obfuscation method, and only a small number of the papers were discussing diversification in cloud security.

The above results lead us to suggest the following avenues for further research:

1) Using diversification as a security measure: a lot of work has proposed the use of obfuscation in the cloud environment; the use of diversification techniques should be stressed more to enhance the security in cloud computing (e.g., diversifying the machine language level of a virtual machine).
2) Protecting the cloud from intruders: researchers have deeply studied how to secure the data *"from"* the untrusted cloud; nevertheless, there is a lack of approaches that use obfuscation and diversification to protect the cloud itself from the external or internal malicious parties.
3) Server-side approaches to protect the cloud: most of the existing research works rely on the client side approaches. There still is a need to stress more on server side approaches for protecting the cloud.

V. Limitations and Conclusion

We have conducted a review using a revised protocol (manual search was not included) to study the work related to the obfuscation/diversification techniques used for cloud security; however, there were some issues limiting the result of our study. First, we selected the set of search strings manually. Thus, there is a concern that not all the materials in the field are captured. Second, the inclusion or exclusion phases might be biased based on the researcher's knowledge. Third, in some cases the search flow was dictated by limitations of some of the databases. For instance, in SpringerLink database we had to limit our search to (Cloud AND Obfuscation), and skip the (Cloud AND Diversification); since the later one brought up over 2000 false positive results.

In this study, we pointed out the significance of having measurements to boost the security and privacy in cloud computing. More specifically, we focused our research on the two techniques, obfuscation and diversification. By collecting, analyzing and classifying the existing research on this domain, we concluded that: a) privacy protection is the main target of the proposed approaches, b) in most of these studies cloud service provider is assumed as "untrusted" and the data should be protected from the cloud, c) most studies were interested to base their approaches on the client side, rather than the server side, and d) there were small number of studies focusing on interface diversification techniques, and the majority of the studies were interested in obfuscation.

The classification of the papers presented in our study clearly illustrated that some areas have gained more attention, while other areas still are potential for further research. This study sheds more light on the areas that remained intact, which gives an agenda for the further research. More studies can focus on the use of diversification technique to provide better security in cloud computing environment. Security should be taken into account not only for providing protection *from the cloud*, but also *for the cloud* itself.

Acknowledgment

Hosseinzadeh, Hyrynsalmi and Leppänen are supported by Cyber Trust research program funded by the Finnish Funding Agency for Innovation. Conti is supported by a Marie Curie Fellowship (PCIG11-GA-2012-321980); EU-India REACH Project ICI+/2014/342-896; TENACE PRIN Project 20103P34XC funded by the Italian MIUR; Project "Tackling Mobile Malware with Innovative Machine Learning Techniques". We also thank Silke Holtmanns for her helpful insights.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing." Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2011.

[2] C. Collberg, C. Thomborson, and D. Low, "A taxonomy of obfuscating transformations," Department of Computer Science, The University of Auckland, New Zealand, Tech. Rep., 1997.

[3] I. V. Popov, S. K. Debray, and G. R. Andrews, "Binary obfuscation using signals." in *USENIX Security*, 2007.

[4] C. Linn and S. Debray, "Obfuscation of executable code to improve resistance to static disassembly," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, ser. CCS '03. New York, NY, USA: ACM, 2003, pp. 290–299.

[5] E. Skoudis, *Malware: Fighting malicious code*. Prentice Hall Professional, 2004.

[6] F. B. Cohen, "Operating System Protection through Program Evolution," *Comput. Secur.*, vol. 12, no. 6, pp. 565–584, Oct. 1993.

[7] S. Rauti, J. Holvitie, and V. Leppänen, "Towards a diversification framework for operating system protection," in *Proceedings of the 15th International Conference on Computer Systems and Technologies*, ser. CompSysTech '14. New York, NY, USA: ACM, 2014, pp. 286–293.

[8] M. Chew and D. Song, "Mitigating buffer overflows by operating system randomization," UC Berkeley, Tech. Rep., 2002.

[9] Top Threats Working Group, "The notorious nine: cloud computing top threats in 2013," *Cloud Security Alliance*, 2013.

[10] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Information and Software Technology*, vol. 55, no. 12, pp. 2049 – 2075, 2013.

[11] G. Zhang, Y. Yang, and J. Chen, "A privacy-leakage-tolerance based noise enhancing strategy for privacy protection in cloud computing," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 12th IEEE International Conference on*, July 2013, pp. 1–8.

[12] P. Yang, X. Gui, F. Tian, J. Yao, and J. Lin, "A privacy-preserving data obfuscation scheme used in data statistics and data mining," in *High Performance Computing and Communications 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC-EUC), 2013 IEEE 10th International Conference on*, Nov 2013, pp. 881–887.

[13] G. Zhang, X. Liu, and Y. Yang, "Time-series pattern based effective noise generation for privacy protection on cloud," *Computers 64(5), IEEE Transactions on*, pp. 1456–1469, May 2015.

[14] G. Zhang, Y. Yang, D. Yuan, and J. Chen, "A trust-based noise injection strategy for privacy protection in cloud," *Software: Practice and Experience*, vol. 42, no. 4, pp. 431–445, 2012.

[15] G. Zhang, Y. Yang, and J. Chen, "A historical probability based noise generation strategy for privacy protection in cloud computing," *Journal of Computer and System Sciences*, vol. 78, no. 5, pp. 1374 – 1381, 2012, {JCSS} Special Issue: Cloud Computing 2011.

[16] D. Lamanna, G. Lodi, and R. Baldoni, "How not to be seen in the cloud: A progressive privacy solution for desktop-as-a-service," in *On the Move to Meaningful Internet Systems: OTM 2012*, ser. Lecture Notes in Computer Science, R. Meersman, H. Panetto, T. Dillon, S. Rinderle-Ma, P. Dadam, X. Zhou, S. Pearson, A. Ferscha, S. Bergamaschi, and I. Cruz, Eds. Springer Berlin Heidelberg, 2012, vol. 7566, pp. 492–510.

[17] G. Zhang, X. Zhang, Y. Yang, C. Liu, and J. Chen, "An association probability based noise generation strategy for privacy protection in cloud computing," in *Service-Oriented Computing*, ser. Lecture Notes in Computer Science, C. Liu, H. Ludwig, F. Toumani, and Q. Yu, Eds. Springer Berlin Heidelberg, 2012, vol. 7636, pp. 639–647.

[18] X. Liu, D. Yuan, G. Zhang, W. Li, D. Cao, Q. He, J. Chen, and Y. Yang, "Cloud workflow system quality of service," in *The Design of Cloud Workflow Systems*, ser. SpringerBriefs in Computer Science. Springer New York, 2012, pp. 27–50.

[19] G. Zhang, Y. Yang, X. Liu, and J. Chen, "A time-series pattern based noise generation strategy for privacy protection in cloud computing," in *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on*, May 2012, pp. 458–465.

[20] L. Arockiam and S. Monikandan, "Efficient cloud storage confidentiality to ensure data security," in *Computer Communication and Informatics (ICCCI), 2014 International Conference on*, Jan 2014, pp. 1–5.

[21] Y. Tian, B. Song, and E.-N. Huh, "Towards the development of personal cloud computing for mobile thin-clients," in *International Conference Information Science and Applications (ICISA)*, April 2011, pp. 1–5.

[22] S. S. Yau and H. G. An, "Protection of users' data confidentiality in cloud computing," in *Proceedings of the Second Asia-Pacific Symposium on Internetware*, ser. Internetware '10. New York, NY, USA: ACM, 2010, pp. 11:1–11:6.

[23] M. Mowbray, S. Pearson, and Y. Shen, "Enhancing privacy in cloud computing via policy-based obfuscation," *The Journal of Supercomputing*, vol. 61, no. 2, pp. 267–291, 2012.

[24] S. Pearson, Y. Shen, and M. Mowbray, "A privacy manager for cloud computing," in *Cloud Computing*, ser. Lecture Notes in Computer Science, M. Jaatun, G. Zhao, and C. Rong, Eds. Springer Berlin Heidelberg, 2009, vol. 5931, pp. 90–106.

[25] M. Mowbray and S. Pearson, "A client-based privacy manager for cloud computing," in *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*, ser. COMSWARE '09. New York, NY, USA: ACM, 2009, pp. 5:1–5:8.

[26] K. Govinda and E. Sathiyamoorthy, "Agent based security for cloud computing using obfuscation," *Procedia Engineering(38),125-129*, 2012.

[27] R. Patibandla, S. Kurra, and N. Mundukur, "A study on scalability of services and privacy issues in cloud computing," in *Distributed Computing and Internet Technology*, ser. Lecture Notes in Computer Science, R. Ramanujam and S. Ramaswamy, Eds. Springer Berlin Heidelberg, 2012, vol. 7154, pp. 212–230.

[28] C. Reiss, J. Wilkes, and J. Hellerstein, "Obfuscatory obscanturism: Making workload traces of commercially-sensitive systems safe to release," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 1279–1286.

[29] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient privacy-aware search over encrypted databases," in *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '14. New York, NY, USA: ACM, 2014, pp. 249–256.

[30] M. Vleju, "A client-centric asm-based approach to identity management in cloud computing," in *Advances in Conceptual Modeling*, ser. Lecture Notes in Computer Science, S. Castano, P. Vassiliadis, L. Lakshmanan, and M. Lee, Eds. Springer Berlin Heidelberg, 2012, vol. 7518, pp. 34–43.

[31] L. Li, Q. Li, Y. Shi, and K. Zhang, "A new privacy-preserving scheme dospa for saas," in *Web Information Systems and Mining*, ser. Lecture Notes in Computer Science(6987), Z. Gong, X. Luo, J. Chen, J. Lei, and F. Wang, Eds. Springer Berlin Heidelberg, 2011, pp. 328–335.

[32] Y. Qin, S. Shen, J. Kong, and H. Dai, "Cloud-oriented sat solver based on obfuscating cnf formula," in *Web Technologies and Applications*, ser. Lecture Notes in Computer Science, W. Han, Z. Huang, C. Hu, H. Zhang, and L. Guo, Eds. Springer International Publishing, 2014, vol. 8710, pp. 188–199.

[33] J. Tapiador, J. Hernandez-Castro, and P. Peris-Lopez, "Online randomization strategies to obfuscate user behavioral patterns," *Journal of Network and Systems Management*, vol. 20, no. 4, pp. 561–578, 2012.

[34] K. Kansal, M. Mohanty, and P. Atrey, "Scaling and cropping of wavelet-based compressed images in hidden domain," in *MultiMedia Modeling*, ser. Lecture Notes in Computer Science, X. He, S. Luo, D. Tao, C. Xu, J. Yang, and M. Hasan, Eds. Springer International Publishing, 2015, vol. 8935, pp. 430–441.

[35] B. Bertholon, S. Varrette, and P. Bouvry, "Jshadobf: A javascript obfuscator based on multi-objective optimization algorithms," in *Network and System Security*, ser. Lecture Notes in Computer Science, J. Lopez, X. Huang, and R. Sandhu, Eds. Springer Berlin Heidelberg, 2013, vol. 7873, pp. 336–349.

[36] B. Bertholon, S. Varrette, and S. Martinez, "Shadobf: A c-source obfuscator based on multi-objective optimisation algorithms," in *Parallel and Distributed Processing Symposium Workshops PhD Forum (IPDPSW), 2013 IEEE 27th International*, May 2013, pp. 435–444.

[37] M. Hataba and A. El-Mahdy, "Cloud protection by obfuscation: Techniques and metrics," in *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2012 Seventh International Conference on*, Nov 2012, pp. 369–372.

[38] B. Bertholon, S. Varrette, and P. Bouvry, "Comparison of multi-objective optimization algorithms for the jshadobf javascript obfuscator," in *Parallel Distributed Processing Symposium Workshops (IPDPSW), 2014 IEEE International*, May 2014, pp. 489–496.

[39] R. Omar, A. El-Mahdy, and E. Rohou, "Arbitrary control-flow embedding into multiple threads for obfuscation: A preliminary complexity and performance analysis," in *Proceedings of the 2Nd International Workshop on Security in Cloud Computing*, ser. SCC '14. New York, NY, USA: ACM, 2014, pp. 51–58.

[40] K. Karuppanan, K. AparnaMeenaa, K. Radhika, and R. Suchitra, "Privacy adaptation for secured associations in a social cloud," in *Advances in Computing and Communications (ICACC), 2012 International Conference on*, Aug 2012, pp. 194–198.

[41] P. Skvortsov, F. Drr, and K. Rothermel, "Map-aware position sharing for location privacy in non-trusted systems," in *Pervasive Computing*, ser. Lecture Notes in Computer Science, J. Kay, P. Lukowicz, H. Tokuda, P. Olivier, and A. Krger, Eds. Springer Berlin Heidelberg, 2012, vol. 7319, pp. 388–405.

[42] B. Agir, T. Papaioannou, R. Narendula, K. Aberer, and J.-P. Hubaux, "User-side adaptive protection of location privacy in participatory sensing," *GeoInformatica*, vol. 18, no. 1, pp. 165–191, 2014.

[43] A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems," *Journal of Network and Computer Applications*, 2014.

[44] P. Ryan and S. Falvey, "Trust in the clouds," *Computer Law & Security Review*, vol. 28, no. 5, pp. 513 – 521, 2012.

[45] M. Villari, A. Celesti, F. Tusa, and A. Puliafito, "Data reliability in multi-provider cloud storage service with rrns," in *Advances in Service-Oriented and Cloud Computing*, ser. Communications in Computer and Information Science, C. Canal and M. Villari, Eds. Springer Berlin Heidelberg, 2013, vol. 393, pp. 83–93.

[46] R. Padilha and F. Pedone, "Confidentiality in the cloud," *Security Privacy, IEEE*, vol. 13, no. 1, pp. 57–60, Jan 2015.

[47] G. Gao-xiang, Y. Zheng, and F. Xiao, "The homomorphic encryption scheme of security obfuscation," in *Advances in Image and Graphics Technologies*, ser. Communications in Computer and Information Science, T. Tan, Q. Ruan, X. Chen, H. Ma, and L. Wang, Eds. Springer Berlin Heidelberg, 2013, vol. 363, pp. 127–135.

[48] R. Furukawa, T. Takenouchi, and T. Mori, "Behavioral tendency obfuscation framework for personalization services," in *Database and Expert Systems Applications*, ser. Lecture Notes in Computer Science, H. Decker, L. Lhotsk, S. Link, J. Basl, and A. Tjoa, Eds. Springer Berlin Heidelberg, 2013, vol. 8056, pp. 289–303.

[49] C. Tunc, F. Fargo, Y. Al-Nashif, S. Hariri, and J. Hughes, "Autonomic resilient cloud management (arcm) design and evaluation," in *Cloud and Autonomic Computing (ICCAC), 2014 International Conference on*, Sept 2014, pp. 44–49.

[50] Q. Yang, C. Cheng, and X. Che, "A cost-aware method of privacy protection for multiple cloud service requests," in *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conference on*, Dec 2014, pp. 583–590.

[51] M. Guo and P. Bhattacharya, "Diverse virtual replicas for improving intrusion tolerance in cloud," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, ser. CISR '14. New York, NY, USA: ACM, 2014, pp. 41–44.

[52] P. Prasadreddy, T. Rao, and S. Venkat, "A threat free architecture for privacy assurance in cloud computing," in *Services (SERVICES), 2011 IEEE World Congress on*, July 2011, pp. 564–568.

[53] M. Palanques, R. DiPietro, C. del Ojo, M. Malet, M. Marino, and T. Felguera, "Secure cloud browser: Model and architecture to support secure web navigation," in *Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on*, Oct 2012, pp. 402–403.