Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.146 – 156

AN CLOUD APPROACH FOR PRIVACY PROTECTION USING NOISE GENERATION STRATEGY

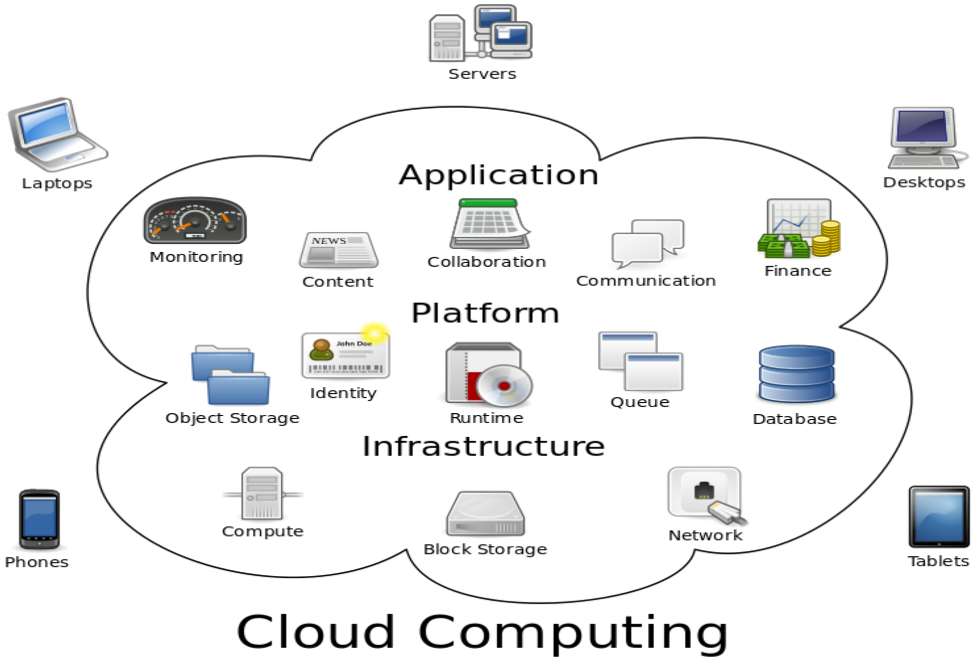
D.Jayakumar[1], R.Priyadharshini[2], S.Rajeswari[3], P.Sharmila[4]
[1]Assistant Professor, Dept. of IT, Prathyusha Engineering College, India
[2,3,4]Student, Dept. of IT, Prathyusha Engineering College, India
[1] jkjayakumard2010@gmail.com, [2] dharshinirajagopal23@gmail.com,
[3] rajeswari8483@gmail.com, [4] sharmirenu24@gmail.com

ABSTRACT:

Cloud computing is an evolutionary domain, which many IT companies prefer to store huge investment of data. It involve a practice of using a network of remote servers hosted on internet to store, manage and process the data rather than a personal computer. One of the serious issue in cloud computing is security. In Cloud Computing, there is a great deal of uncertainty about how security at all levels can be achieved. We have adopted a noise generation strategy to protect customer privacy. Noise obfuscation is an effective approach which utilize noise data. Example, noise service requests can be generated and injected into real customer service requests so that malicious service providers would not be able to distinguish between the original and noise request. Service provider is generally used to collect the information and process the service request. Due to rapid development of cloud, large number of malicious service provider exist in cloud environment. We also provide an additional security enhancement to service provider so it won't allow malicious service provider to access the request. First, we analyze a novel cluster based algorithm to generate time intervals dynamically. Then, based on these time intervals, we analysis probability fluctuations and propose a novel time-series pattern based forecasting algorithm. Finally, novel noise generation strategy can be presented to withstand the probability fluctuation.

INTRODUCTION:

Cloud computing is a kind of Internet-based computing, where data, information and shared resources are provided to computers and other devices on-demand. Cloud computing has now become a highly demanded service or utility. Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and smartphones. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, the cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.



CLOUD SERVICES:

Software as a Service (SaaS):

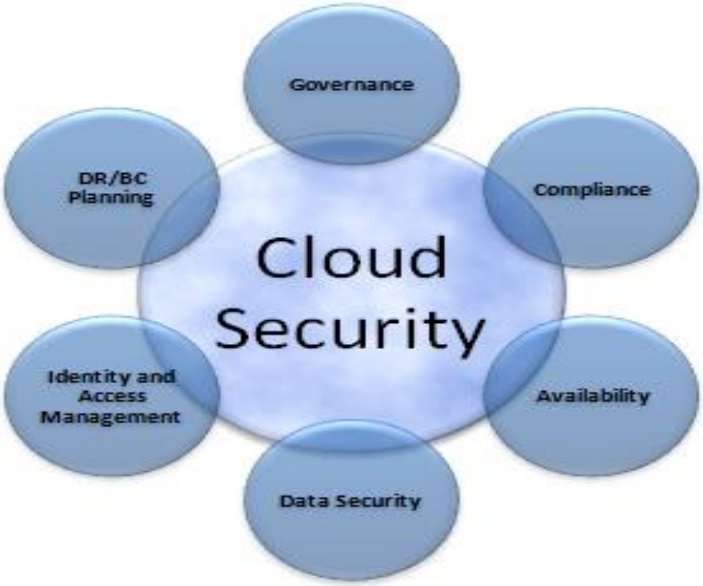
Software as a service (or SaaS) is a way of delivering applications over the Internet as a service. Instead of installing and maintaining software, you simply access it via the Internet, without managing software and hardware configuration.
The feature provided to the consumer is, allowing application to be executed in cloud infrastructure. The applications are accessed through various client devices like web browser.

Platform as a Service (PaaS):

The feature provided to the consumer is effective implementation of application in cloud infrastructure without installing any platform or tools. PaaS provide platform resources like operating system management, memory management .When analysing and selecting PaaS provider, we have to take consideration of programming languages and technologies need to be used. Developer tools and applications integration is also very important because it implements the way how application in the PaaS will integrate with other applications.

Infrastructure as a Service (IaaS):

The feature provided to the consumer is, processing, storage, networks, and other fundamental computing resources where the consumer wants effective implementation of software, which can include all the necessary requirements of application which include operating system etc. IaaS platforms provide high scalable resources where it can be adjusted on demand. This makes IaaS well-suited for workloads that are temporary, experimental or change unexpectedly. IaaS customers pay on a per-use basis, typically by the hour, week or month.



CHALLENGES IN CLOUD COMPUTING:

A cloud computing is a important solution that offer enterprises a cost effective model to satisfy their computing needs. Because of this emergence technologies, cloud computing has placed many challenges in different aspects. Some of these challenges are:

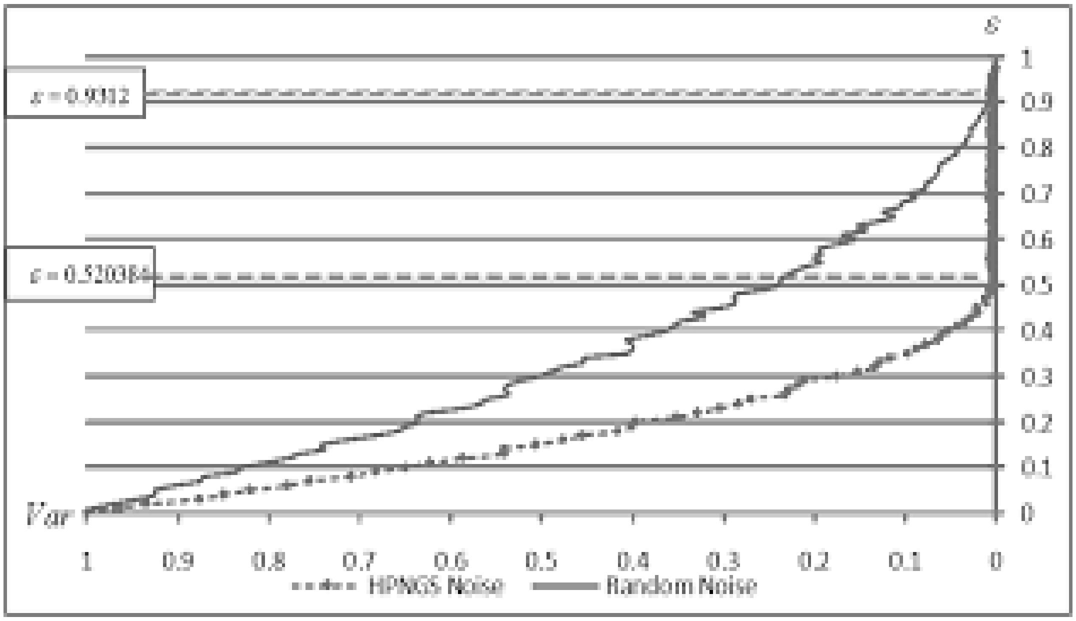
- **Security and Privacy:** This aim is to provide security and protection to data through cloud. This security and privacy issues can be overcomes by employing encryption, security hardware and security application.
- **Portability:** It the ability to move applications and its associated data between one cloud provider and another or between public and private cloud environments.
- **Interoperability:** Application on one platform should be able to incorporate services from another platform. The incorporation is made possible through web services.
- **Performance and Cost:** cost is spent for the bandwidth rather than the hardware. In order to deliver data intensive applications on cloud requires high network bandwidth, which results in high cost.

SECURITY AND PRIVACY ISSUES:

We have multiple security issues that need to be analysed in cloud computing scenario. A public cloud acts as a host of a number of virtual machines, virtual machine monitors, and supporting middleware etc. The security of the cloud depends on the behaviour of these objects as well as on the interactions between them. Moreover, in a public cloud enabling a shared multi-tenant environment, as the number of users increase, security risks get more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanism. Various cloud service providers adopt different technologies to safeguard the data stored in their cloud. But the question is: Is the data stored in these clouds really secure? The virtualized nature of cloud storage makes the traditional mechanisms unsuitable for handling the security issues. These service providers use different encryption techniques such as: public key encryption and private key encryption to secure the data stored in the cloud. Trust based methods are useful in establishing relationships in a distributed environment. A domain based trust-model has been proposed in to handle security and interoperability in cross clouds.

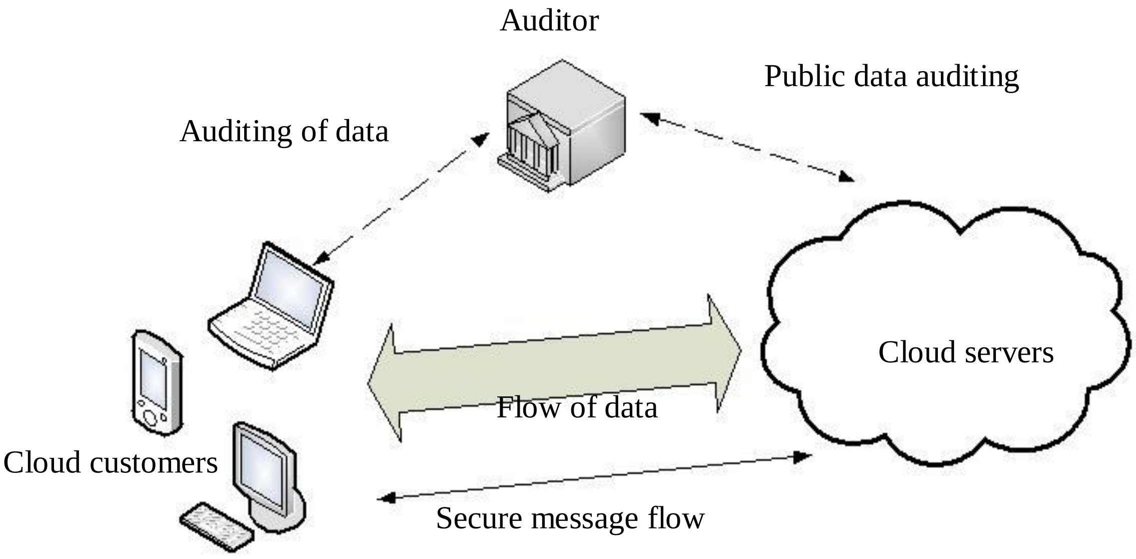
HISTORICAL PROBABILITES BASED NOISE REQUEST*:*

This strategy generates noise requests based on their historical occurrence probability so that all requests including noise and real ones can reach about the same occurrence probability and then service providers would not be able to distinguish in between. Our strategy can significantly reduce the number of noise requests over the random strategy, by more than 90% as simulation evaluation. It generates noise requests based on their previous occurrence probabilities, i.e. historical probabilities, so that all requests including those noise ones and real ones can reach about the same occurrence probabilities. This would confuse service providers. Therefore, customers need to take certain actions to protect their privacy without the need for the service providers' cooperation, since noise request is generated by server. The major disadvantages in this paper is, Noise request generate in unequal time intervals, so that malicious provider can guess the probability fluctuation. It generates noise request based on historical occurrence probability. It can reach same occurrence probabilities of final request in entire time period, but not same in all time intervals Malicious service provider can deduce the customer privacy from these fluctuations.



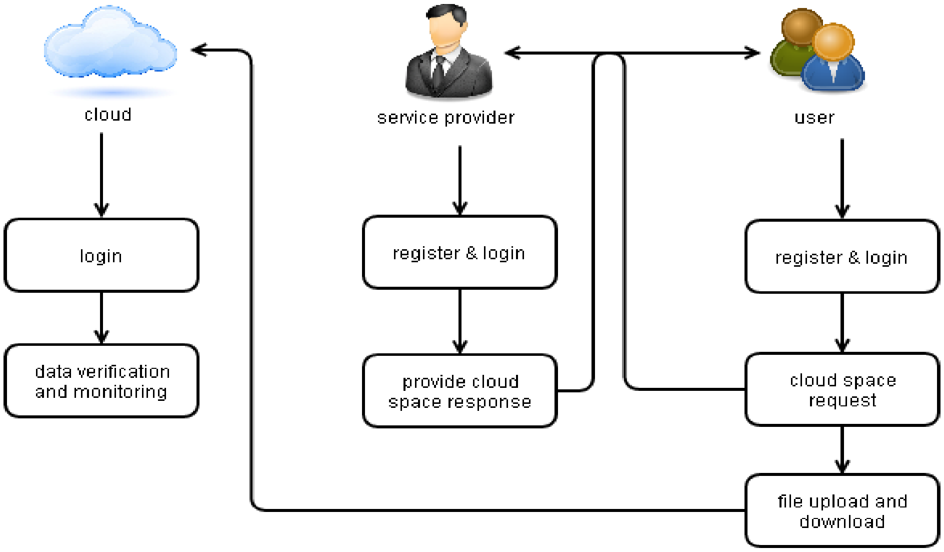
THIRD PARTY AUDITORING:

Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data .To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we propose a secure cloud storage supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. The advantage is, it uses a technique of public key based homographic linear authenticator. It enables TPA to perform the auditing without demanding the local copy of data. It reduces the communication and computation overhead as compared to the straightforward data auditing approaches. The major disadvantages is the number of times a particular data file can be audited is limited by the number of secret keys .The TPA also has to maintain and update state between audits, i.e., keep track on the revealed MAC keys.



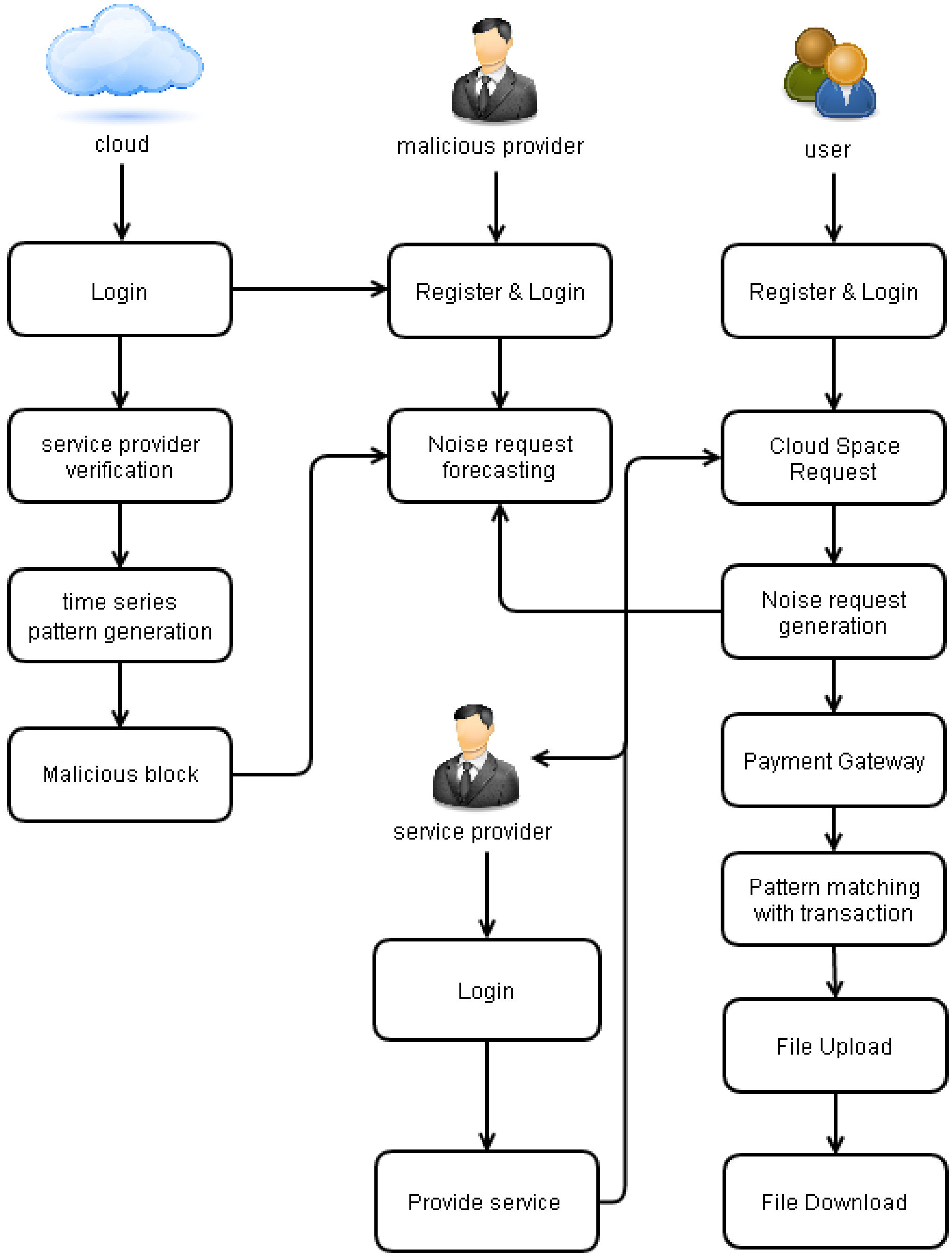
NOVEL PATTERN BASED TIME SERIES PATTERN:

Time related functionalities such as workflow scheduling and temporal verification normally require effective forecasting of activity durations due to the dynamic nature of underlying resources such as Web or Grid services. However, most existing strategies cannot handle well the problems of limited sample size and frequent turning points. To address such problems, we propose a novel pattern based time-series forecasting strategy which utilizes a periodical sampling plan to build representative duration series, and then conducts time-series segmentation to discover the smallest pattern set and predicts the activity duration intervals with pattern matching results. The simulation experiment demonstrates the excellent performance of our segmentation algorithm and further shows the effectiveness of our strategy intervals. The major disadvantage is limited sample size and frequent turning points, potentially affect the effectiveness of conventional time-series models. Limited sample size evidently impedes the fitting of time-series.



TIME SERIES PATTERN BASED NOISE GENERATION:

This strategy uses the time series pattern generation for privacy protection of user data. Security is provided to service provider, since it sends intimation to original service provider when malicious service provider try to hack the privacy details of user. Currently, existing representative noise generation strategies have not considered possible fluctuations of occurrence probabilities. In this case, the probability fluctuation could not be concealed by existing noise generation strategies, and it is a serious risk for the customer's privacy. Occurrence probabilities could fluctuate at some time segments of the entire time period, which cannot be concealed by existing noise obfuscations .To address this probability fluctuation privacy risk, we develop a novel time-series pattern based noise generation strategy for privacy protection on cloud. First, we present a novel cluster based algorithm to generate time intervals dynamically. Then, based on these time intervals, we analyze corresponding probability fluctuations and propose a novel time-series pattern based forecasting algorithm. Lastly, based on the forecasting algorithm, our novel noise generation strategy can be presented to withstand the probability fluctuation privacy risk. The simulation evaluation demonstrates that our strategy can significantly improve the effectiveness of such cloud privacy protection to withstand the probability fluctuation privacy risk.


cloud
malicious provider
user
Login
Register & Login
Register & Login
service provider verification
Noise request forecasting
Cloud Space Request
time series pattern generation
Noise request generation
Malicious block
Payment Gateway
service provider
Pattern matching with transaction
Login
File Upload
Provide service
File Download

CONCLUSION:

In an open cloud computing environment, various malicious service providers can exist. Such service providers may record service requests from a customer and then collectively deduce the customer private information. Therefore, customers need to protect their privacy. There is the risk that end users don't understand the issues involved when signing on to a cloud service without reading the terms and conditions. Cloud computing poses privacy concerns because the service provider can access the data at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties for purposes of law and order even without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. The simulation evaluation demonstrated that our novel strategy could cope with these fluctuations very well, i.e., significantly improve the effectiveness of privacy protection.

References:

1 Mr.D.Jayakumar, **“A Resourceful Allocation of Data Storage in Cloud Computing**” International Journal of Advances in Engineering and Emerging Technology,VOL 1,ISSUE 1,MARCH 2013.

2. **“Time-Series Pattern Based Effective Noise Generation for Privacy Protection on Cloud**” IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 5, MAY 2015.

3. C.P. Pfleeger and S.L. Pfleeger, “**Security in Computing**” fourth ed.,Prentice Hall, 2006.

4. G. Zhang, Y. Yang, and J. Chen, “**A Historical Probability Based Noise Generation Strategy for Privacy Protection in Cloud Computing**” J. Computer and System Sciences, vol. 78, no. 5, 2012.

5. Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, “**Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage**,” IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

6. R. Agrawal and R. Srikant, "**Privacy-Preserving Data Mining,**" ACM SIGMOD Record, vol. 29, no. 2, pp. 439-450, 2000.

7. A. Evfimievski, J. Gehrke, and R. Srikant, "**Limiting Privacy Breaches in Privacy Preserving Data Mining,"** Proc. 22nd ACM SIGMOD-SIGACT-SIGART Symp. Principles of Database Systems (PODS '03), pp. 211-222, June 2003.

8. Y. Sang, H. Shen, and H. Tian, "**Effective Reconstruction of Data Perturbed by Random Projections,**" IEEE Trans. Computers, vol. 61, no. 1, pp. 101-117, Jan. 2012.

9. B.C.M. Fung, K. Wang, R. Chen, and P.S. Yu, "**Privacy-Preserving Data Publishing: A Survey of Recent Developments,**" ACM Computing Surveys, vol. 42, no. 4, pp. 1-53, 2010.

10. V.Rastogi, D. Suciu, and S. Hong, "**The Boundary between Privacy and Utility in Data Publishing,"** Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 531-542, Sep. 2007