International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Surveying Personal Information, Privacy and Security in Cloud Computing

Priya Dhingra[1], Shakti Nagpal[2]

Computer Science and Engineering, Geeta Engineering College, Panipat, India

Abstract: ***Cloud computing is certainly revolutionary model which enables flexible, on-demand and low-cost usage of computing resources. Benefits of Cloud Computing are the sources of privacy and security problems, which emerge since the data owned by different consumers are kept in some cloud servers instead of under their own control. To handle security problems, numerous schemes in line with the Encryption algorithms have been proposed recently. However, the privacy issue of cloud computing is actually yet getting fixed. The privacy challenge is to design cloud services in such a manner as to decrease privacy risk and give compliance that is legal. For example, a business storing data about individual consumers using the cloud that is prominent company is sometimes high-risk. Clients may not be in a position to sue enterprises if their privacy rights tend to be violated. This paper surveys privacy issues and security in cloud computing.***

Keywords: Cloud Computing, Security, Privacy Preserving, Information sharing.

1. Introduction

Cloud computing provides reliable services above the Internet, is one of the Top 10 Crucial Technologies. Recently, countless intellectual and manufacturing associations have commenced investigating and growing technologies and groundwork for cloud computing. The representative cloud periods contain Amazon Elastic Cloud (EC2) [1], Google App Engine and Microsoft Live Network.

A user stores his confidential files in a cloud, and retrieves them wherever and whenever he wants. A user pays a Cloud provider for a storage ability in order to store his email memos, and afterward he wants to reclaim merely emails encompassing precise keywords after he is voyaging alongside a client, such as a wireless PDA and a mobile phone. It is trivial to do so after the email memos are stored in the form of a plain-text that will familiarize unwanted protection and privacy risks. For example A user is technician in Firm who seizes in price of after-sale services. He stores all the emails dispatched from the clients in a cloud after he is in his workplace alongside a desktop, and retrieves them to tackle the customer's ability demands after he is out alongside a PDA. An attacker who intercepts and arrests the contact is able to understand the customer's privacy data as well as company's secrets. What is inferior is that an untrustworthy cloud provider is able to facilely attain all the data and send it to the biggest match of Firm A. As delineated in there are two main aggressions below such a circumstance beyond aggressions commenced by unauthorized outsiders and inner aggressions commenced by untrustworthy cloud providers. In such cases, we couldn't fully belief a cloud provider, but yet demand its service. Therefore, the company needs to furnish a little mechanism to protect the user data privacy and the user queries privacy in cloud environment.

The simplest resolution is to encrypt the emails beforehand storing them in a cloud and dispatch queries in the form of encrypted keywords. For example, a user could use his area key to encrypt the email memo body and its keywords beforehand dispatching it to a cloud provider, and next sends queries in the form of encrypted keywords to reclaim the email. As the hidden key is merely recognized to the user himself, an attacker has no believed of the encrypted files and the user queries patterns. Though, such a easy encryption scheme could familiarize supplementary problems:

1) It depletes too much CPU and recollection of the client across the encryption and decryption;
2) The cloud provider couldn't ascertain that emails encompass keywords enumerated by a user if the encryption is not searchable.

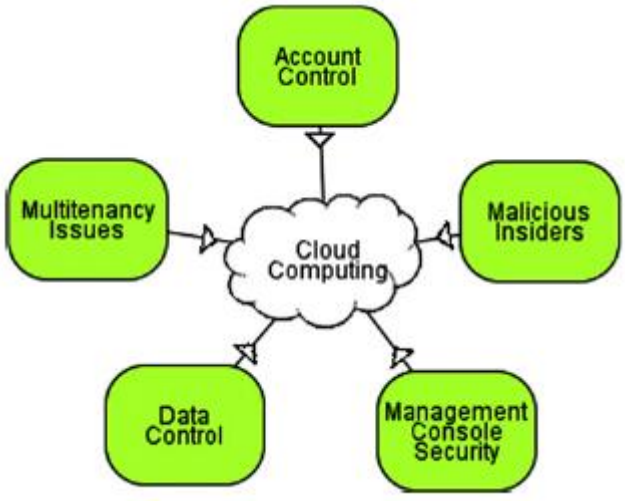

Figure 1: Categorization of Cloud threats

Therefore, it can merely revisit back all the encrypted emails. Usually articulating, a slender client has merely manipulated bandwidth, CPU and memory; consequently a easy encryption scheme couldn't work well below these circumstances.

Personal Information

'Personal information' is a term that can be utilized in a way that is somewhat different individuals, but in this document, we mean by this term privacy sensitive and painful information that includes the following:

- **Personally identifiable information** (PII): any information that could be accustomed recognize or locate a person (e.g. name, address) or information that may be correlated with other information to identify an individual (e.g. bank card quantity, postal code, Internet Protocol (IP) address) [4].
- **Sensitive information**: information on religion or race, wellness, intimate orientation, union account or other information that is considered private. Such information requires safeguards which can be extra. Other information that may be considered delicate includes personal information that is job performance information that is economic. - Information considered being PII that is sensitive and painful. biometric information or collections of surveillance camera images in public areas.
- **Usage data**: Usage data collected from computer devices such as printers; behavioural information such as watching habits for electronic content, users' recently visited websites or product usage history.
- **Unique device identities**: Other types of information that might be uniquely traceable to a user unit, e.g. IP addresses, Radio Frequency Identity (RFID) tags, unique hardware identities.

Challenges to Cloud Privacy

The privacy challenge for software engineers is to design cloud services in such a means as to diminish privacy danger, and to ensure compliance that is legal. Laws placing geographical as well as other limitations on the collection, processing and transfer of personally recognizable and information that is use that is sensitive of services as currently designed. For instance, a UK business storing data about individual customers with the cloud that is prominent provider Salesforce.com could find itself in breach of UK data protection legislation. Customers may have the ability to sue enterprises if their privacy rights are violated, and in any case that is complete enterprises may face injury to their reputation. There is a true range that is wide of privacy breaches in the news recently. It can also be essential to allay users' fears about usage of cloud solutions. Concerns arise when it's not clear to individuals why their information that is personal is or just how it is used or passed on to other parties: this absence of control results in suspicion and finally distrust. There are also concerns that are security-related whether the information that is personal the cloud will be adequately protected.

2. Cloud Confidentiality Issues

Confidentiality issues in Cloud information mining is a serious topic. A problem that is key arises in virtually any masse that is en of information is the fact that of confidentiality. The necessity for privacy may also be due to law (e.g., for medical databases) or can be inspired by business interests. However, there are situations where the sharing of data can lead to gain that are mutual. A utility that is key of databases today is research, whether it be scientific, or financial and market oriented. Thus, for instance, the field that is medical much to gain by pooling data for research; as may also competing businesses with mutual interests. This could be not feasible because of the confidentiality issues which arise despite the prospective gain. We address this question and show that extremely solutions that are efficient possible. Our scenario is the immediate following:

Allow P1 and P2 be parties owning (large) personal databases D1 and D2. The parties wish to share information that is joint without revealing any unnecessary information about their individual data. That is, the information that is only by P1 about D2 is that which can be discovered through the production associated with information selection, and vice versa. It is not assumed that any "trusted" 3rd party who computes the output that is joint. Huge databases and efficient computation that is secure is very difficult. A model is need exactly that utilized multi-party computation.

It is clear that any solution that is reasonable have the parties that are individual the most of the computation individually. option would be based on this principle that is guiding in fact, the amount of bits communicated is based on how many transactions by a logarithmic factor only. We remark that a condition that is necessary obtaining such a protocol that is private the existence of a (non-private) distributed protocol with low interaction complexity is need.

Semi-honest adversaries

A Semi-honest adversary [4] can invariably change its input in any multi-party computation environment. This particular fact can be very damaging because the adversary can determine its input to function as empty database within the data-mining setting. Then, the output obtained is the consequence that is total of algorithm on one other party's database alone. Even though this attack cannot be prevented, you want to prevent an event that is harmful performing some other attack. Nevertheless, because of this work that is assume that is initial the adversary is semi-honest (also known as passive). That is, it correctly follows the protocol specification, yet attempts to learn information that is additional examining the transcript of messages received throughout the execution. We remark that even though the adversarial that is semi-honest is far weaker than the model that is adware a party may arbitrarily deviate from the protocol specification), it is normally a realistic one. That is because deviating from a specified program which might be buried in a complex application is a job that is non-trivial. Semi-honest behavior that is adversarial models a scenario in which both parties that participate in the protocol are honest.

3. Related Work

Secure two party computations were first investigated by Yao and was later generalized to multi-party computation []. These works all use a similar methodology: the functionality f to be computed is first represented as a combinatorial circuit, and then the parties run a short protocol for every gate in the circuit. While this approach is appealing in its generality and simplicity, the protocols it generates depend on the size of the network. This size depends on the size of the input (which might be huge as in a data mining application), and on the complexity of expressing f as a network (for example, a naive multiplication circuit is quadratic in the size of its inputs). We stress that secure two-

party computation of small circuits with small inputs may be practical using the protocol.

Due to the inefficiency of generic protocols, some research has focused on finding efficient protocols for specific (interesting) problems of secure computation.

Ning Cao et al., 2011 [6] In the growing cloud computing paradigm, data proprietors come to be increasingly motivated to outsource their convoluted data association arrangements from innate locations to the business area cloud for outstanding flexibility and commercial savings. For the thought of users' privacy, sensitive data have to be encrypted beforehand outsourcing, that makes competent data utilization a extremely challenging task. In this paper, for the early period, they delineate and resolve the setback of privacy-preserving query above encrypted graph-structured data in cloud computing (PPGQ), and institute a set of severe privacy necessities for such a safeguard cloud data utilization arrangement to come to be a reality. Our work utilizes the principle of "filtering-and-verification". They prebuild a feature-based index to furnish feature-related data concerning every single encrypted data graph, and next select the effectual inner product as the pruning instrument to hold out the filtering procedure. To encounter the trial of upholding graph query lacking privacy ruptures, they counsel a safeguard inner product computation method, and next enhance it to accomplish assorted privacy necessities below the known-background menace model.

Cong Wang et al., 2004 [7] This paper Cloud Calculating has outstanding possible of bestowing robust computational manipulation to the area at decreased cost. It enables clients alongside manipulated computational resources to outsource their colossal computation workloads to the cloud, and frugally relish the large computational domination, bandwidth, storage, and even appropriate multimedia that can be public in a pay-per-use manner. Although the incredible benefits, protection is the main obstacle that prevents the expansive adoption of this enthusing computing ideal, exceptionally for clients after their confidential data are consumed and produced across the computation. Indulging the cloud as an intrinsically insecure computing period from the viewpoint of the cloud clients, they have to design mechanisms that not merely protect sensitive data by enabling computations alongside encrypted data, but additionally protect clients from malicious behaviors by enabling the validation of the computation result. Such a mechanism of finished safeguard computation outsourcing was presently shown to be feasible in theory, but to design mechanisms that are usefully effectual stays a extremely challenging problem.

Shubhashis Sengupta et al., 2011 [8] Cloud Calculating is increasingly becoming accepted as countless enterprise requests and data are advancing into cloud platforms. Though, a main barrier for cloud adoption is real and observed lack of security. In this paper, they seize a holistic think of cloud computing protection - spanning across the probable subjects and vulnerabilities related alongside virtualization infrastructure; multimedia platform; individuality association and admission control; data integrity; confidentiality and privacy; physical and procedure protection aspects; and lawful compliance in cloud. They present our findings from the points of think of a cloud cloud provider, cloud customer, and third-party powers such as Govt. They additionally debate vital research orders in cloud protection in spans such as Trusted Computing, Data Centric Protection and Privacy Maintaining Models. Finally, they draft a set of steps that can be utilized, at a elevated level, to assess protection preparedness for a company request to be traveled to cloud.

Dimitrios, Zissis et al., 2012 [9] The present rise of cloud computing has drastically modified everyone's understanding of groundwork architectures, multimedia transport and progress models. Projecting as an evolutionary pace, pursuing the transition from mainframe computers to client/server placement models, cloud computing encompasses agents from grid computing, utility computing and autonomic computing, into an innovative placement architecture. This quick transition towards the clouds, has fuelled concerns on a critical subject for the accomplishment of data arrangements, contact and data security. From a protection outlook, a number of unchartered dangers and trials have been gave from this relocation to the clouds, deteriorating far of the effectiveness of established protection mechanisms. As a consequence the target of this paper is twofold; firstly to assess cloud protection by recognizing exceptional protection necessities and secondly to endeavor to present a viable resolution that eliminates these possible threats. This paper proposes familiarizing a Trusted Third Party, tasked alongside promising specific protection characteristics inside a cloud environment. The counseled resolution calls on cryptography, specifically Area Key Groundwork working in concert alongside SSO and LDAP, to safeguard the authentication, integrity and confidentiality of encompassed data and communications. The resolution, presents a horizontal level of abiility, obtainable to all implicated entities, that realizes a protection mesh, inside that vital belief is maintained.

Md Riyazuddin et al., 2012 [10] This paper In present years, advances in hardware expertise have lead to an rise in the competence to store and record confidential data concerning customers and individuals. This has lead to concerns that the confidential data could be misused for a collection of purposes. In order to lessen these concerns, a number of methods have presently been counseled in order to present the data excavating tasks in a privacy-preserving way. Privacy maintaining data excavating has come to be increasingly accepted because it permits allocating of privacy sensitive data for research purposes. So area have come to be increasingly indisposed to allocate their data, oftentimes emerging in people whichever weakening to allocate their data or bestowing incorrect data. Privacy maintaining data excavating has been learned extensively, because of the expansive blast of sensitive data on the globe source. In this paper, they furnish a study of methods for privacy and examine the representative method for privacy maintaining data mining.

Boyang Wang et al., 2012 [11] This paper alongside cloud storage services, it is commonplace for data to be not merely stored in the cloud, but additionally public across several users. Though, area auditing for such public data — as

maintaining individuality privacy — stays to be an open challenge. In this paper, they counsel the early privacy-preserving mechanism that permits area auditing on public data stored in the cloud. In particular, they exploit ring signatures to compute the verification data demanded to audit the integrity of public data. With our mechanism, the individuality of the signer on every single block in public data is retained confidential from a third party auditor (TPA), who is yet able to openly confirm the integrity of public data lacking reclaiming the whole file. Our experimental aftermath clarify the effectiveness and efficiency of our counseled mechanism after auditing public data.

Ronald Petrlic et al., 2012 [12] This paper they come up alongside a digital entitlements association (DRM) believed for cloud computing and display how license association for multimedia inside the cloud can be attained in a privacy-friendly manner. In our scenario, users who buy multimedia from multimedia providers stay anonymous. At the alike period, our way guarantees that multimedia licenses are attached to users and their validity is checked beforehand execution. They retain a multimedia re-encryption scheme so that computing centers that present users' multimedia are not able to craft user profiles—not even below pseudonym—of their users. They join hidden allocating and homomorphic encryption. They make sure that malicious users are incapable to relay multimedia to others. DRM constitutes an incentive for multimedia providers to seize portion in a upcoming cloud computing scenario. They make this scenario extra appealing for users by maintaining their privacy.

Ronald Petrlic et al., 2012 [13] In a cloud-computing scenario whereas users buy multimedia from multimedia providers and present it at computing centers, a digital entitlements association (DRM) arrangement has to be in locale to check the multimedia licenses across every single multimedia execution. Though, the exposure of users to privacy conquest in the attendance of DRM arrangements is problematic. They come up alongside a believed that unites multimedia providers' and users' demands for a safeguard and privacy-preserving DRM arrangement for cloud computing. The occupation of proxy re-encryption permits for a prevention of profile constructing (under pseudonym) of users by each party.

Kui Ren et al., 2012 [14] This paper Cloud computing embodies today's most thrilling computing paradigm shift in data technology. Though, protection and privacy are observed as main obstacles to its expansive adoption. Here, the authors chart countless critical protection trials and inspire more investigation of protection resolutions for a trustworthy area cloud environment.

Cong Wang et al., 2012 [15] This paper Cloud storage enables users to remotely store their data and relish the on-demand elevated quality cloud requests lacking the burden of innate hardware and multimedia management. Nevertheless the benefits are clear, such a ability is additionally relinquishing users' physical ownership of their outsourced data, that inevitably poses new protection dangers towards the correctness of the data in cloud. In order to address this new setback and more accomplish a safeguard and dependable cloud storage abiility, they counsel in this paper a flexible distributed storage integrity auditing mechanism, employing the homomorphic token and distributed erasure-coded data. The counseled design permits users to audit the cloud storage alongside extremely handy contact and computation cost. The auditing consequence not merely ensures forceful cloud storage correctness promise, but additionally simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Thinking the cloud data are vibrant in nature, the counseled design more supports safeguard and effectual vibrant procedures on outsourced data, encompassing block modification, deletion, and append. Research displays the counseled scheme is exceedingly effectual and resilient opposing Byzantine wreck, malicious data modification attack, and even server colluding attacks.

Guojun Wang et al., 2013 [16] In the real globe, firms should publish communal webs to a third party, e.g., a cloud cloud provider, for marketing reasons. Maintaining privacy after publishing communal web data becomes an vital issue. In this paper, they recognize a novel kind of privacy attack, termed 1*-neighborhood attack. They accept that an attacker has vision concerning the degrees of a target's one-hop acquaintances, in supplement to the target's 1-neighborhood graph, that consists of the one-hop acquaintances of the target and the connections amid these neighbors. With this data, an attacker could re-identify the target from a k-anonymity communal web alongside a probability higher than 1/k, whereas each node's 1-neighborhood graph is isomorphic alongside k-1 supplementary nodes' graphs. To challenge the 1*-neighborhood attack, they delineate a key privacy property, probability indistinguishability, for an outsourced communal web, and counsel a heuristic indistinguishable cluster anonymization (HIGA) scheme to produce an anonymized communal web alongside this privacy property. The empirical discover indicates that the anonymized communal webs can yet be utilized to answer aggregate queries alongside elevated accuracy

Taeho Jung et al., 2013 [17] This paper Cloud computing is a extreme computing paradigm that enables flexible, on-demand and low-cost custom of computing resources. Those gains, ironically, are the reasons of protection and privacy setbacks, that appear because the data owned by disparate users are stored in a little cloud servers instead of below their own control. To deal alongside protection setbacks, assorted schemes established on the Attribute-Based Encryption have been counseled recently. Though, the privacy setback of cloud computing is yet to be solved. This paper presents an nameless opportunity manipulation scheme Anony Domination to address not merely the data privacy setback in a cloud storage, but additionally the user individuality privacy subjects in continuing admission manipulation schemes. By employing several powers in cloud computing arrangement, their counseled scheme achieves nameless cloud data admission and fine-grained opportunity control. Their protection facts and presentation research displays that AnonyControl is both safeguard and effectual for cloud computing environment.

Fosca Giannotti et al., 2013 [18] This paper spurred by events such as cloud computing, there has been substantial present attention in the paradigm of data mining-as-a-service.

A firm (data owner) lacking in expertise or computational resources can outsource its excavating needs to a third party cloud provider (server). Though, both the items and the association laws of the outsourced database are believed confidential property of the firm (data owner). To protect company privacy, the data proprietor transforms its data and boats it to the server, sends excavating queries to the server, and recovers the real outlines from the removed outlines consented from the server. In this paper, they discover the setback of outsourcing the association law excavating task inside a company privacy-preserving framework. They counsel an attack ideal established on background vision and design a scheme for privacy maintaining outsourced mining. Their scheme ensures that every single transformed item is indistinguishable, w.r.t. the attacker's background vision, from at least k-1 supplementary transformed items. Their comprehensive examinations on a extremely colossal and real deal database clarify that their methods are competent, scalable, and protect privacy.

Cong Wang et al., 2013 [19] This paper Employing Cloud Storage, users can remotely store their data and relish the on-demand elevated quality requests and services from a public pool of configurable computing resources, lacking the burden of innate data storage and maintenance. Though, the fact that users no longer have physical ownership of the outsourced data makes the data integrity protection in Cloud Calculating a formidable task, exceptionally for users alongside constrained computing resources. Moreover, users ought to be able to just use the cloud storage as if it is innate, lacking fretting concerning the demand to confirm its integrity. Thus, enabling area audit skill for cloud storage is of critical significance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely familiarize an competent TPA, the auditing procedure ought to hold in no new vulnerabilities towards user data privacy, and familiarize no supplementary online burden to user.

Ning Cao et al., 2014 [20] This paper alongside the advent of cloud computing, data proprietors are motivated to outsource their convoluted data association arrangements from innate locations to business area cloud for outstanding flexibility and commercial savings. But for protecting data privacy, sensitive data has to be encrypted beforehand outsourcing, that obsoletes established data utilization established on plaintext keyword search. Thus, enabling an encrypted cloud data find ability is of paramount importance. Thinking the colossal number of data users and documents in cloud, it is critical for the find ability to permit multi-keyword query and furnish consequence similarity ranking to encounter the competent data retrieval need. Related works on searchable encryption focus on solitary keyword find or Boolean keyword find, and scarcely differentiate the find results. In this paper, for the early period, they delineate and resolve the challenging setback of privacy-preserving multi-keyword ranked find above encrypted cloud data (MRSE), and institute a set of severe privacy necessities for such a safeguard cloud data utilization arrangement to come to be a reality.

4. Conclusion

Cloud computing as an growing computing paradigm aiming to allocate storage, computation, and services transparently amid a large users, has gathered outstanding momentum from not merely industry but additionally academia. In core, cloud computing overlaps countless continuing thoughts, such as distributed, grid and utility computing. Though, driven mainly by marketing and ability offerings from large company contestants like Google, IBM and Amazon, cloud computing has evolved out of these thoughts and come to be a new buzz word concentrating on" cloud"—more hypothetical resource and services' delivery. After cloud computing steps into our daily lifetimes, each innately stored data, such as email, word processing documents and spreadsheets, might be remotely stored in a cloud. Then, we can use each terminals, e.g., computer, laptop and PDA etc., to admission these data at anytime, anywhere. Due to these enthusing characteristics, cloud computing has come to be increasingly appealing to the public. In future, we will develop granule access control systems that can facilitate granting disparity based access rights to a set of users and permits flexibility in specifying the access rights of individual users. The data will be stored on the servers in an encrypted form while different users with which the information is share can be allowed to decrypt data sections based upon their identity. This process will effectively get rid of the need to depend on the storage server for preventing unauthorized data access. We will propose a better type of encryption where the authentication mechanisms of different users can be associated with different access structures (granularity).

References

[1] Yi, Sangho, Derrick Kondo, and Artur Andrzejak. "Reducing costs of spot instances via checkpointing in the amazon elastic compute cloud." In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pp. 236-243. IEEE, 2010.
[2] Pearson, Siani. "Taking account of privacy when designing cloud computing services." In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52. IEEE Computer Society, 2009.
[3] Narayanan, Arvind, and Vitaly Shmatikov. "Myths and fallacies of personally identifiable information." Communications of the ACM 53, no. 6 (2010): 24-26.
[4] Brickell, Justin, and Vitaly Shmatikov. "Privacy-preserving graph algorithms in the semi-honest model." In Advances in Cryptology-ASIACRYPT 2005, pp. 236-252. Springer Berlin Heidelberg, 2005.
[5] Pinkas, Benny, Thomas Schneider, Nigel P. Smart, and Stephen C. Williams. "Secure two-party computation is practical." In Advances in Cryptology–ASIACRYPT 2009, pp. 250-267. Springer Berlin Heidelberg, 2009.
[6] Ning Cao, Zhenyu Yang, Cong Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving query over encrypted graph-structured data in cloud computing." In Distributed Computing Systems (ICDCS), 2011 31st International Conference on, pp. 393-402. IEEE, 2011.
[7] Cong Wang, Kui Ren, and Jia Wang. "Secure and practical outsourcing of linear programming in cloud computing." In INFOCOM, 2011 Proceedings IEEE, pp. 820-828. IEEE, 2011.

[8] Shubhashis Sengupta, Vikrant Kaulgud, and Vibhu Saujanya Sharma. "Cloud computing security--trends and research directions." In Services (SERVICES), 2011 IEEE World Congress on, pp. 524-531. IEEE, 2011.
[9] Dimitrios, Zissis and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583-592.
[10] Md Riyazuddin, Dr VVSSS Balaram, Md Afroze, Md JaffarSadiq, and M. D. Zuber. "An Empirical Study on Privacy Preserving Data Mining." International Journal of Engineering Trends and Technology 3, no. 6 (2012): 687-693.
[11] Boyang Wang, Baochun Li, and Hui Li. "Oruta: Privacy-preserving public auditing for shared data in the cloud." In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, pp. 295-302. IEEE, 2012.
[12] Ronald Petrlic, and Christoph Sorge. "Privacy-preserving DRM for cloud computing." In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pp. 1286-1291. IEEE, 2012.
[13] Ronald Petrlic, "Proxy re-encryption in a privacy-preserving cloud computing DRM scheme." In Cyberspace Safety and Security, pp. 194-211. Springer Berlin Heidelberg, 2012.
[14] Kui Ren, Cong Wang, and Qian Wang. "Security challenges for the public cloud." IEEE Internet Computing 16, no. 1 (2012): 69-73.
[15] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou. "Toward secure and dependable storage services in cloud computing." Services Computing, IEEE Transactions on 5, no. 2 (2012): 220-232.
[16] Guojun Wang, Qin Liu, Feng Li, Shuhui Yang, and Jie Wu. "Outsourcing privacy-preserving social networks to a cloud." In INFOCOM, 2013 Proceedings IEEE, pp. 2886-2894. IEEE, 2013.
[17] Taeho Jung, , Xiang-Yang Li, Zhiguo Wan, and Meng Wan. "Privacy preserving cloud data access with multi-authorities." In INFOCOM, 2013 Proceedings IEEE, pp. 2625-2633. IEEE, 2013.
[18] Fosca Giannotti, Laks VS Lakshmanan, Anna Monreale, Dino Pedreschi, and Hui Wang. "Privacy-preserving mining of association rules from outsourced transaction databases." Systems Journal, IEEE 7, no. 3 (2013): 385-395.
[19] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for secure cloud storage." Computers, IEEE Transactions on 62, no. 2 (2013): 362-375.
[20] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." Parallel and Distributed Systems, IEEE Transactions on 25, no. 1 (2014): 222-233.