Research Journal of Applied Sciences, Engineering and Technology 10(3): 328-337, 2015
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 29, 2014 Accepted: February 5, 2015 Published: May 30, 2015

A Survey Paper on Privacy Issue in Cloud Computing

[1, 2]Yousra Abdul Alsahib S. Aldeen, [1]Mazleena Salleh and [1]Mohammad Abdur Razzaque
[1]Faculty of Computing, Universiti Teknologi Malaysia, UTM, Skudai, Johor, Malaysia
[2]Department of Computer Science, College of Education_Ibn Rushd, Baghdad University, Baghdad, Iraq

Abstract: In past few years, cloud computing is one of the popular paradigm to host and deliver services over Internet. It is having popularity by offering multiple computing services as cloud storage, cloud hosting and cloud servers etc., for various types of businesses as well as in academics. Though there are several benefits of cloud computing, it suffers from security and privacy challenges. Privacy of cloud system is a serious concern for the customers. Considering the privacy within the cloud there are numerous threats to the user's sensitive data on cloud storage. In this study, we give a survey on numerous works on cloud computing, provide a survey on several research on cloud privacy issues, classify current solutions for privacy issues in cloud environments as architectures, approaches and methods and the advantages and disadvantages of current studies are tabulated. Moreover, it also discusses open research challenges and recommends future research directions. The main goal of this study is to offer a better understanding of the privacy challenges of cloud computing and to focus on current gaps to fulfil the privacy issue.

Keywords: Cloud computing, cloud privacy

INTRODUCTION

The significance of cloud computing is increasing and is getting a rising attention in the scientific and industrial communities. Cloud computing is considered as the first among the top 10 most vital technologies and with a better view in consecutive years by companies and organizations by studying of Gartner. cloud allows ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that could be rapidly provisioned and released with negligible management effort or service provider interaction. It seems as a computational model as well as distribution architecture (Hashizume *et al*., 2013).

Customers of cloud can use computational resources which are including software, storage and processing capacities belonging to other companies (cloud service providers). Cloud services comprise Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as shown in Fig. 1.

Amazon, Google and Microsoft are Great companies that are providing cloud services in numerous forms. Amazon Web Services (AWS) delivers cloud services that include Amazon Elastic Compute Cloud (EC2), Simple Queue Service (SQS) and Simple Storage Service (S3). Google offers Platform as a Service (PaaS) known as Google App Engine (GAE) and eases hosting web applications (+Sun™ Storage J4200/J4400 Array System Overview). Microsoft also offers cloud services in the form of Windows Azure, SQL Azure, Windows Intune etc. Clients can use the advantage of mass storage and processing capacity at a low cost by depending on services. These services can be used by developers to evade the form overhead cost of buying resources, e.g., processors and storage devices (Dev *et al*., 2012).

Five essential characteristics are summarized by the cloud security alliance (Kumar *et al*., 2013) that exemplify the relation to and changes from, traditional computing model:

On-demand self-service: A cloud client may get computing capabilities, similar the practice of numerous servers and network storage, as on demand, without interacting with the cloud provider.

Broad network access: Customers can access the services through heterogeneous thin or thick client tools due to services are brought across the Internet via a standard device that allows.

Resource pooling: The cloud provider services a multi-tenant model to help multiple clients by pooling computing resources, which are dissimilar physical and virtual resources dynamically allocated or reassigned according to client demand.

Rapid elasticity: Capabilities might be rapidly and elastically provisioned to quickly scale out or rapidly released to quickly scale in.

Corresponding Author: Yousra Abdul Alsahib S. Aldeen, Faculty of Computing, Universiti Teknologi Malaysia, UTM, Skudai, Johor, Malaysia

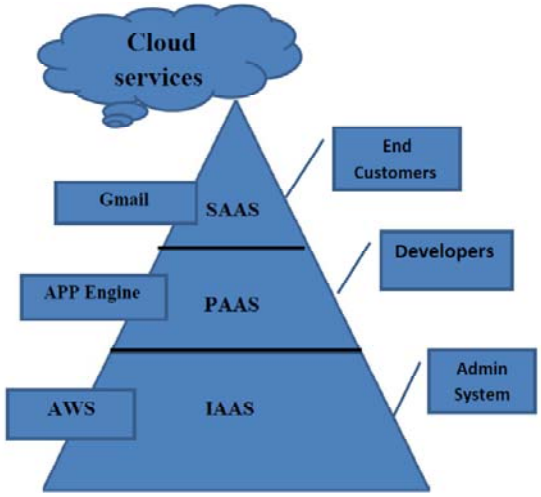

Fig. 1: General architecture of cloud services

Measured service: The service bought by clients can be counted and measured. For both the provider and clients, resource usage will be checked, controlled, metered and reported. For that, cloud computing becomes an attractive field to many companies and organization.

Though cloud computing is an influential means of attaining high storage and computing services at a low cost, big organizations are still worried about privacy and also hesitate to move their data to cloud. Privacy issues have been made many limitations to extensive use of cloud computing. There are three main challenges for structure secure and trustworthy cloud systems which are including outsourcing, multi-tenancy and massive data and intense computation (Xiao *et al*., 2012). Also, users' data are analyzed by cloud providers for a long time. Furthermore, outside attackers who achieve to get access to the cloud can also analyze data and disrupt user privacy. Cloud is not only a source of huge static data, but also a provider of high processing volume at low cost. This makes cloud more susceptible as attackers can use the raw processing power of cloud to analyze data (Chow *et al*., 2009). Especially, there are multiple data analysis are available that effectively extract valued information from a large volume of data. Researches on cloud privacy issues are either cited as general researches, but within a conversation related with privacy, or linked to the privacy issues that are labelled in the own subsections. This study presents a survey on numerous research on cloud computing, provides a survey on several research on cloud privacy issues, categorizes current solutions for privacy issues in cloud environments as architectures, approaches and methods and the advantages and disadvantages of current studies are tabulated. Furthermore, it also discusses open research challenges and recommended future research directions. The main goal of this study is to offer a better understanding of the privacy challenges of cloud computing and to emphasis on current gaps in order to protect privacy of customers in cloud computing.

CLOUD COMPUTING

Cloud computing is recognised by Williams (2010) and Beloglazov *et al*. (2012) as an abstraction which is based on pooling physical resources notions and presented as a virtual resource. It is also identified as a technology which is considered as the next big step towards the development and implementations of an increasing number of distributed applications, (Marinescu, 2012). Cloud computing systems are typically homogeneous and the same level of security, resource management, cost and other policies are shared by all the users. The could computing can be described by term an umbrella which defines a category of sophisticated on-demand computing services offered by commercial providers, for example Amazon, Google and Microsoft, (Rajkumar *et al*., 2011). Sadeghi *et al*. (2010) has defined the cloud computing system as infrastructure and computational services on demand for different clients on shared resources or network such as Amazon EC2 (computation) or S3 (storage), over platform services such as Microsoft's database service SQL Azure or Google App Engine.

National Institute of Standards and Technology (Mell and Grance, 2011) defines Cloud Computing as characteristic to deliver and deployment of specific models. Pearson and Charlesworth (2009) has listed the key characteristics defined by NIST as including the sharing of resources and resource pooling technology such as multi-tenancy and virtualization. Cloud computing offers reliable and customized computing environments for extensive internet users due to it has a very great computing paradigm (Gong *et al*., 2013). They provided survey on cloud computing, which highlight its key ideas, architecture, state of the art application and some main challenges. They aimed is to

provide a good guidance of the design challenges of cloud computing and also explained numerous significant research directions in this field. Consequently, cloud computing system has become a necessity and attractive computing paradigm which can provide customized and reliable computing system for extensive Internet users. In future, it can be considered as one of the basic utility following water, electricity, gas and telephone. So, it is being accepted widely and utilized in business industry. Though, there are multiple advantages of cloud computing systems but it also brings number challenges such as security and privacy which are needed to be settled.

Privacy challenges in cloud computing: Sun *et al*. (2011) have presented and discussed the key issues related to security, secrecy and reliance on cloud computing systems (Sun *et al*., 2011; Gellman and Forum, 2009; Chow *et al*., 2009). The tangible and intangible threats related to cloud systems have been discussed in details so that clients can understand these types of threats such as security, privacy and trust. The authors have analyzed the different mechanism used to eliminate the privacy, security and trust threats and provide a secure, trustworthy and dependable cloud computing system. Tchifilionova (2011) has described that the Security and privacy would be a persisting threats on cloud systems until clients fully understand the cloud system i.e., who manages the system, how it works and whether the company can afford to "leak" their private information decision that can only be used after a careful risks analysis and policy considerations otherwise they may simply get lost in the cloud. Xiao *et al*. (2012) have discussed the five most representative attributes related to security and privacy of cloud system such as accessibility, secrecy, accountability, reliability and privacy-preservability. The relationships among these parameter, the vulnerabilities misused by attackers, the threat models and existing defense strategies in a cloud scenario have been described. It has been suggested that the privacy should not be separated from security due to its importance particularly in cloud system. Privacy is as strongly related to security, as well as the security attributes have positive or negative impact on privacy. Porwal *et al*. (2011) and King and Raja (2012) have described the issues regarding to data protection on cloud computing system and pointed out some privacy laws which should be enforced in the EU. It has been concluded the cloud system should include high level regulatory recommendations data protection, security, transfer, confidentiality and non-disclosure, intellectual property, law enforcement access, risk allocation and limitation of liability change of control, audit. Wayne and Hafner (2012) have successfully developed a measurement system based on standardized dimensions to assess privacy risks in cloud environments and described in details the drawbacks of current techniques which are applied in cloud computing systems. Svantesson and Clarke (2010) have identified the cloud computing systems with serious risks to privacy and consumer rights and that current privacy law may able to settle some of these threats.

Chadwick and Fatema (2012) have presented an infrastructure service run on authorization infrastructure. The proposed infrastructure ensures the users' privacy policy and access would always be monitored and managed by the policies even for the transferring of data between cloud providers or services. Adrian (2013) have determined whether or not a cloud computing infrastructure can provide privacy regulation. The issues regarding to the privacy and personal information, privacy and the Internet, privacy and cloud computing have been discussed in details.

Hou *et al*. (2011) have addressed the issues regarding to the forensic investigation and employed homomorphic encryption and commutative encryption to solve the problem. By using the proposed method the investigators can extract the required evidences without exploiting the privacy of other users. At the same time, the service provider cannot identify in what sort of information the investigators are interested. Pearson *et al*. (2009) have presented a co-regulation strategy which involves the corporate responsibility model. The model is underpinned primarily by contract which places the onus upon the data controller to follow a more proactive technique to ensure compliance. But at the same time, it encourages cloud service providers and their subcontractors to compete in the service provision arena, at least in part, on the basis of at least maintaining good and ideally evolving better, privacy enhancing mechanisms and processes.

Khan *et al*. (2012) have illustrated the data privacy related issues on cloud computing system (Chen and Zhao, 2012). A concise analysis has been presented on data security and privacy protection problems related to cloud computing for all different stages of data life cycle. Some solutions related to such data security issues have also been discussed such as Decentralized Information Flow Control (DIFC), fully homomorphic encryption scheme, differential privacy protection technology, a mathematical way to verify the integrity of the data, Data Integrity (PDI) solution and client-based privacy management. For the issues related to privacy protection techniques for instance K anonymous, Graph anonymization and data pre-processing methods, a privacy protection model using Information Accountability (IA) components have also been presented and discussed. Patel *et al*. (2013) have surveyed and described the latest developed Intrusion Detection and Prevention Systems (IDPSs) and alarm management techniques by describing a comprehensive taxonomy and exploring possible solutions to identify and avoid intrusions on cloud computing environments. By assuming the required features of IDPS and cloud systems, a list of germane requirements are described

and presented the four concepts of autonomic computing self-management, ontology, risk management and fuzzy theory to fulfil these requirements. Itani *et al*. (2009) have proposed PasS set of security protocols to ensure the secrecy of client data on cloud infrastructure. The security solution depends on cryptographic coprocessors which provide a trusted and isolated execution environment on the cloud. The PasS protocol system and the privacy enforcement mechanisms supported by these protocols have been discussed in details. The description for the proof of concept implementation has also been presented.

CURRENT SOLUTIONS OF PRIVACY ISSUES IN CLOUD COMPUTING

This section will discuss the current solutions for privacy issues in cloud. It classified into three subsections which are including architecture, framework, approach and method to become more attractive from the reader.

Architecture and framework for solving privacy issue in cloud: Nandipati and Sridevi (2013) have investigated a new cloud framework known as Data Protection as a Service, which is able to reduce the per-application development efforts dramatically which are required for data protection and mean time it also allows the rapid development and maintenance. The DPaaS paradigm offers logging and auditing at the platform level to share the advantages of all applications running on top. Sykes *et al*. (2013) have presented a model acting by three distinct logical components: the Privacy Service Mediator (PSM) Mobile Device Agent (MDAg) and cloud services. Using the PSM, the communication between mobile applications and cloud services have been proposed. It analyzed the exchange of information in privacy perspective. Using a command design pattern, the mobile application could bundle the cloud-service calls into a chain of command objects which are linked and sent to PSM for execution via MDAg.

Ke *et al*. (2013) built a privacy negotiation model between service provider and user on the basis of description logic, transforming the pre-negotiation of privacy policy for decidable issue of Tableau algorithm. The privacy policy negotiation is composed of two steps:

Step 1: With Tableau algorithm of description logic, by detecting the conflicts of privacy attribute collections, they can obtain the Privacy Knowledge Base (PKB) that satisfy user requirements.

Step 2: Through ordinal exchange of privacy disclosure assertion based on privacy attribute sequences between user and service provider, they obtain the privacy policy that meet both user and service provider privacy requirements. Pearson *et al*. (2009) have discussed a privacy managing system for cloud computing environment, which decrease the risk of user's private information being misused and also helps the cloud systems provider to ensure the privacy laws. The different possible framework for cloud system to manage privacy of clients has been discussed in details such as algebraic description of obfuscation which is one of the important features of privacy manager. The authors have also described how these manages might be employed to protect the clients private metadata of online photos on cloud system. The issues related to privacy manager have been addressed, which can help cloud system clients to manage the privacy of own data on cloud environment.

Two types of the Secure Cloud Computing (SCC) systems are proposed by Yang and Lai (2013). One of them is with Trusted Third Party (TTP) and the other is without TTP. The main objective of their schemes is to protect the data privacy and security in the cloud server. They added the symmetric property in secret sharing to successfully reduce the cost to share the shares between the client and the server. Also, by the homomorphism property of secret sharing, they extend SSC to Multi-server SCC (MSCC) fitting the multi-server environment. As compared to the previous data Privacy by Authentication and Secret Sharing (PASS), their schemes have the better security and performance. Santos *et al*. (2009) have presented a new design for a reliable Cloud Computing Platform (TCCP) which provides IaaS services as Amazon EC2 for closed box execution environment. TCCP ensures the trustworthy execution of guest VMs and permits clients to verify the IaaS provider and able to know if the service is safe and secure before the clients launch their VMs.

Song *et al*. (2011) have presented a new framework for privacy-protected private data recovery service known as parity cloud service. Parity cloud service provides solution for all problems related to cloud system such as consistency, economical efficiency, accessibility and confidentiality while developing personal data recovery service. The proposed approach is simple and does not involves any resources for privacy protection. It works on collaboration-based data recovery algorithm in which the data loss rate is very less. Wang *et al*. (2010) have proposed a privacy-preserving public auditing system for security of stored data on cloud system, where TPA (Third Party Auditing) performs audit for stored data without demanding the local copy of data. In the proposed system a homomorphic authenticator and random mask techniques are used to ensure that TPA would not get any information regarding to the data content stored on the cloud system while running the auditing process. The careful security and performance analysis have shown that the proposed frameworks are proved safe and highly efficient. It has believed that the security and

high efficiency of proposed frameworks will shed light on economies of scale for Cloud Computing.

Approach or prototype for solving privacy issue in cloud: Lu and Tsudik (2011) have presented a scheme from avoiding the cloud server to learn any possible sensitive plaintext in the outsourced databases. Furthermore, the proposed scheme also provides private querying so that neither database holder nor the cloud server can access the query details. An additional condition such as client's input is authorized by Cloud Auditing (CA). An encryption scheme has been incorporated to protect data secrecy and permit access control. The scheme is developed to retrieve search token and decryption key for a user from database owner without showing query contents. But their proposal scheme has some limitation such as, it only supports equality testing and hides concrete contents in the conditional expression and does not support the join operations between two tables. Schiering and Kretschmer (2012) presented a prototype of an IaaS cloud service which serves as a basis for Software Services (SaaS) compliant with this European directive. This is achieved by a combination of organizational and technical measures accompanied by auditing and monitoring.

Ranchal *et al*. (2010) have presented a new technique for Identity Management (IDM) systems independent of Trusted Third Party (TTP) and able to utilize identity data for un-trusted hosts. The technique is based on using of predicates over encrypted data and multi-party computing to negotiate use of cloud system.

Chuang *et al*. (2011) have presented an affective privacy protection framework for cloud environment to provide confidentiality to users' data without affecting system performance. The proposed scheme is able to analyze associated information, by picking the most suitable combination of encryption algorithm and number of data division to deliver more safe protection or decrease performance overhead. Their simulation results showed that the proposed scheme satisfies user-demand privacy requirement and offers the better performance at the same time. Mishra *et al*. (2011) have focused simultaneously data confidentiality and harmonizing the relations intact on cloud system. The proposed framework offers data owner to perform computation intensive tasks on cloud servers without unveiling data contents or user access privilege information.

Methods for solving privacy issue in cloud: To tackle security and privacy problems associated to cloud system, Wang (2011) have proposed four effective methods. The proposed methods are based on Role Based Access Control (RBAC). The key parameters in the cloud-based RBAC model are cloud clients, access authorization, role and session. The policy integration method has employed to solve the multi-policy issues. To avoid the unauthorized usage of the cloud data, one identification management method and user control method have been proposed which can be employed to the generalized cloud computing system. Mowbray and Pearson (2009) have developed a privacy manager software which is based on user's assistance i.e., whether the client can protect his secrecy while accessing cloud system. Fundamental feature of privacy manager are based on obfuscation and de-obfuscation service to limit the quantity of sensitive data stored on a cloud. Also, the privacy manager assists cloud's clients to choose privacy preferences about the handling of his private data by different personae, revising and modifying of data stored on cloud system, etc. Obfuscation could obfuscate all or a portion of data structure before transmitting to the cloud server. Guo *et al*. (2010) have developed a technique to produce a rank list of sub-schemas for publishing. These sub-schemas regulate the predictive performance on the target variable, but bound the prediction accuracy against the private attributes. Experiments have been conducted on a financial database to express the efficiency of the strategy. Experimental results have shown that the proposed technique is able to generate sub-schemas which can regulate and maintain high accuracies against the target variables, while keeping the predictive capability low against private attributes.

Ulltveit-Moe and Oleshchuk (2010) have worked on classification of privacy leakages in the Intrusion Detection System (IDS) rules. The Procedure Related to Privacy Leakage (PRILE) is a general procedure which is compatible to any IDS system. Five general classification tasks have been identified which have been analyzed in the PRILE procedure and two of them are investigated based on a Naïve Bayes classifier. The limitation in employed method is that the analysis is snort specific. The employed procedure, PRILE, is still in its initial stages, therefore more investigation are required to realize objective view. Mowbray *et al*. (2010) have discussed the privacy manager issues related to cloud computing system, specifically which controls policy-based obfuscation and de-obfuscation of personal, sensitive, or confidential data within cloud service provision.

RESEARCH GAB IN CLOUD PRIVACY ISSUE

In summary, this literature review addresses the definitions of privacy and how the risk of privacy exposure has grown in terms of importance to the enterprise. It also presents authors who searched in this manner. Some researchers are believed to separate privacy from security due to its significance particular for cloud systems. Privacy is considered as highly related to security, also other security attributes have positive or negative impact on privacy of the system. A number of Cloud Computing system providers have concerned about security and privacy problems and they are unable to sort out appropriate solution in five aspects (i.e., availability, confidentiality, data integrity,

Table 1: Summary of literature review of cloud computing

References	Cloud computing
Williams (2010) and Beloglazov *et al*. (2012)	Identified cloud as an abstraction based on the notion of pooling physical resources, presented the NIST draft definition and described five essential characteristics
Marinescu (2012)	Identified cloud in other way as the next big stage in the development and deployment of an increasing number of distributed applications
Rajkumar *et al*. (2011)	It presented on demand computing services that provided by cloud providers including Amazon, Google, and Microsoft
Sadeghi *et al*. (2010)	Presented cloud services
NIST (2009)	Defined cloud computing and presented its characteristics, specific delivery models and deployment models
Pearson and Charlesworth (2009)	Listed the key characteristics defined by NIST
Gong *et al*. (2013)	Provided survey on cloud computing, which highlight its key ideas, architecture, state of the art application, and some main challenges

Table 2: Summary of literature review of cloud privacy

References	Analysis of privacy issue including survey, architecture, framework, approach and method	Advantages and disadvantages
Sun *et al*. (2011), Gellman and Forum (2009) and Chow *et al*. (2009)	Presented the major security, privacy and trust issues in cloud computing	Adv. Identified the most threats in current existing cloud computing
Tchifilionova (2011)	Explained the fact that security and privacy will remain a major concern in cloud	Adv. Identified the most threats in current existing cloud computing
Xiao *et al*. (2012)	Stated five most representative security and privacy attributes which are confidentiality, integrity, availability, accountability, and privacy-preservability	Adv. Presented the vulnerabilities, the risk models, as well as existing defense strategies in a cloud scenario
Porwal *et al*. (2011) and King and Raja (2012)	Discussed data protection issues related to cloud computing and identified privacy laws enforced in the EU that can be applied to this model	Adv. Give high level regulatory recommendations about data protection, data security etc
Wayne and Hafner (2012)	Creating a measurement system to assess privacy risks in cloud	Adv. Focusing on the weakness of weaknesses of current methodologies
Svantesson and Clarke (2010)	Highlighted current privacy law may struggle to address some of those risks	Adv. Stated the cloud providers should follow the law of other countries
Chadwick and Fatema (2012)	Described a policy based authorization infrastructure that a cloud provider can run as an infrastructure service for its users	Adv. Ensured that the users' privacy policies are stuck to their data
Adrian (2013)	Aimed to determine whether or not cloud computing infrastructure can support privacy regulation yet remain practical	Adv. Analysis the relationship between privacy, cloud and internet
Hou *et al*. (2011)	Focused on the problem of forensic investigation	Adv. Provided two forensically sound schemes to solve the problem
Pearson *et al*. (2009)	Supported a co-regulation strategy based on a corporate responsibility model	Adv. Focused on hybrid accountability mechanism
Khan *et al*. (2012) and Chen and Zhao (2012)	Identified different data protection models and techniques	Adv. Analyzing the risks related to data privacy in cloud
Patel *et al*. (2013)	Surveyed, explored and informed researchers about the latest developed IDPSs and alarm management techniques	Adv. Provide comprehensive taxonomy and investigating possible solutions to detect and prevent intrusions in cloud computing systems
Itani *et al*. (2009)	Presented PasS, a set of security protocols	Adv. Ensure the privacy of customer data in cloud computing infrastructures
Nandipati and Sridevi (2013)	Architecture, explored a novel cloud platform architecture called data protection as a service	Adv. Provides logging and auditing at the platform level
Sykes *et al*. (2013)	Architecture, proposed model acting by three distinct logical components: the Mobile Device Agent (MDAg), the Privacy Service Mediator (PSM) and cloud services	Adv. This drives the communication between mobile applications and cloud services
Ke *et al*. (2013)	Architecture, built a privacy negotiation model between service provider and user	Adv. Reaching the privacy policy that meet both user and service provider privacy requirements
Pearson *et al*. (2009)	Architecture, described different possible architectures for privacy management in cloud computing	Adv. Help the user manage the privacy of their data in the cloud
Yang and Lai (2013)	Architecture, proposed two types of the Secure Cloud Computing (SCC): one is with Trusted Third Party (TTP) and the other is without TTP	Adv. Have the better security and performance
Santos *et al*. (2009)	Architecture, presented the design of a Trusted Cloud Computing Platform (TCCP) that enables IaaS services	Adv. Guarantee confidential execution of guest VMs, allow users to attest to the IaaS provider and determine the security of service
Song *et al*. (2011)	Architecture, proposed a novel privacy-protected personal data recovery service framework on the cloud computing	Adv. It is simple and does not require many resources for privacy protection
Wang *et al*. (2010)	Architecture ,a privacy-preserving public auditing system for data storage security in cloud computing	Adv. Secure and highly efficient

Table 2: Continue

References	Analysis of privacy issue including survey, architecture, framework, approach and method	Advantages and disadvantages
Lu and Tsudik (2011)	Approach, proposed scheme prevents the cloud server from learning any possibly sensitive plaintext in the outsourced databases	Adv. Protects data privacy, allow access control and allow user to retrieve search token and decryption key from database owner Dis. adv. It only supports equality testing, hides concrete value in the conditional expression and join operations between two tables is not supported
Schiering and Kretschmer (2012)	Approach, presented a prototype of an IaaS cloud service which serves as a basis for Software Services (SaaS)	Adv. Compliance with the data protection European directive
Ranchal *et al*. (2010)	Approach, proposed an approach for Identity Management (IDM) systems	Adv. It ensures privacy policies
Chuang *et al*. (2011)	Approach, proposed an effective privacy protection scheme in cloud to secure the confidentiality of users' data	Adv. Ensures user-demand privacy requirement and provides the better performance at the same time
Mishra *et al*. (2011)	Approach, achieved data confidentiality while still keeping the harmonizing relations intact in the cloud	Adv. Allowed the data owner to representative most of computation intensive tasks to cloud servers without user access privilege information
Wang (2011)	Method, Role Based Access Control (RBAC)	Adv. Applied to the generalized cloud computing
Mowbray and Pearson (2009)	Method, proposed privacy manager software on the client	Adv. Helped the users to choose privacy preferences about the treatment of their personal information
Guo *et al*. (2010)	Method, proposed a method to generate a ranked list of sub-schemas for publishing	Adv. High accuracies against the target variables Dis. adv. Lowering the predictive capability against confidential attributes
Ulltveit-Moe and Oleshchuk (2010)	Method, presented privacy leakage in the Intrusion Detection System (IDS) rules method	Adv. It should be applicable to any IDS system Dis. adv. Their methodology, PRILE, is needed to more study and more experts
Mowbray *et al*. (2010)	Method, proposed a privacy manager for cloud computing	Adv. Helped the users to choose privacy preferences about the treatment of their personal information

Table 3: Presents the categorization of current studies

References	Issues	Architecture and framework	Approach or prototype	Method	Parameters
Sun *et al*. (2011), Gellman and Forum (2009) and Chow *et al*. (2009)	√				Security and privacy
Tchifilionova (2011)	√				Security and privacy
Xiao *et al*. (2012)	√				Security and privacy
Porwal *et al*. (2011) and King and Raja (2012)	√				Security and privacy
Wayne and Hafner (2012)	√				Privacy
Svantesson and Clarke (2010)	√				Privacy
Chadwick and Fatema (2012)	√				Privacy
Adrian (2013)	√				Privacy
Hou *et al*. (2011)	√				Privacy
Pearson *et al*. (2009)	√				Privacy
Khan *et al*. (2012) and Chen and Zhao (2012)	√				Privacy
Patel *et al*. (2013)	√				Privacy
Itani *et al*. (2009)	√				Privacy
Nandipati and Sridevi (2013)		√			Privacy
Sykes *et al*. (2013)		√			Privacy
Ke *et al*. (2013)		√			Privacy
Pearson *et al*. (2009)		√			Privacy
Yang and Lai (2013)		√			Privacy
Santos *et al*. (2009)		√			Privacy
Song *et al*. (2011)		√			Privacy
Wang *et al*. (2010)		√			Privacy
Lu and Tsudik (2011)			√		Privacy
Schiering and Kretschmer (2012)			√		Privacy
Ranchal *et al*. (2010)			√		Privacy
Chuang *et al*. (2011)			√		Privacy
Mishra *et al*. (2011)			√		Privacy
Wang (2011)				√	Privacy
Mowbray and Pearson (2009)				√	Privacy
Guo *et al*. (2010)				√	Privacy
Ulltveit-Moe and Oleshchuk (2010)				√	Privacy
Mowbray *et al*. (2010)				√	Privacy

control and audit) for privacy. Some of them have found that for some information and business clients have concerned about sharing as government agencies and private litigants may hack their private data more easily from a third party as compared to the creator of the data. Analysis has shown that privacy is a complicated issue and that there is requirement to merge different approaches in order to generate a comprehensive solution that does not compromise client's privacy. Table 1 presents summary of literature review of cloud computing and Table 2 presents current studies on cloud privacy as well as it presents their advantages and disadvantages. Table 3 presents the categorization of current studies. Therefore, it is needed to propose strong, efficient and scalable model that overcomes these issues. It is still needed to further research in this area of study.

CONCLUSION

In recent years, the improvement of cloud computing has provided opportunities for investigation in all aspects of cloud computing. Cloud computing is becoming more attractive for many organizations due to fact that it provides multiple computing services as cloud storage, cloud hosting and cloud servers etc. Although, there are numerous benefits of cloud computing, governments and big organizations are concerned about security and privacy issues on cloud. Privacy of cloud system is a serious concern for the customers. The aim of this study is twofold. Firstly, it surveys on cloud computing. Secondly, it surveys on cloud privacy issue and available solutions. Also, a classified of present solutions for privacy issues in cloud environments is provided in this study. The advantages and disadvantages of current studies are tabulated. It also discusses open research challenges and recommends future research directions.

REFERENCES

Adrian, A., 2013. How much privacy do clouds provide? An Australian perspective. Comput. Law Secur. Rev., 29(1): 48-57.

Beloglazov, A., J. Abawajy and R. Buyya, 2012. Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing. Future Gener. Comp. Sy., 28(5): 755-768.

Chadwick, D.W. and K. Fatema, 2012. A privacy preserving authorisation system for the cloud. J. Comput. Syst. Sci., 78(5): 1359-1373.

Chen, D. and H. Zhao, 2012. Data security and privacy protection issues in cloud computing. Proceeding of International Conference on Computer Science and Electronics Engineering, 973: 647-651.

Chow, R., P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka and J. Molina, 2009. Controlling data in the cloud: Outsourcing computation without outsourcing control. Proceeding of the 2009 ACM Workshop on Cloud Computing Security (CCSW, 2009), pp: 85-90.

Chuang, I., S. Li, K. Huang, Y. Kuo and A.C.S. Models, 2011. An effective privacy protection scheme for cloud computing. Proceeding of 13th International Conference on Advanced Communication Technology (ICACT, 2011), pp: 260-265.

Dev, H., T. Sen, M. Basak and M.E. Ali, 2012. An approach to protect the privacy of cloud data from data mining based attacks. Proceeding of SC Companion: High Performance Computing, Networking Storage and Analysis, pp: 1106-1115.

Gellman, R. and W.P. Forum, 2009. Privacy in the clouds : Risks to privacy and confidentiality from cloud computing. Retrieved from: World Privacy Forum: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (Accessed on: August 18, 2012).

Gong, Y., Z. Ying and M. Lin, 2013. A survey of cloud computing. Proceeding of the 2nd International Conference on Green Communications and Networks 2012 (GCN 2012), 2013, 225: 79-84.

Guo, H., H.L. Viktor and E. Paquet, 2010. Identifying and preventing data leakage in multi-relational classification. Proceeding of IEEE International Conference on Data Mining Workshops, pp: 458-465.

Hashizume, K., D.G. Rosado, E. Fernández-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. J. Internet Serv. Appl., 4(1): 5.

Hou, S., T. Uehara, S.M. Yiu, L.C.K. Hui and K.P. Chow, 2011. Privacy preserving confidential forensic investigation for shared or remote servers. Proceeding of 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp: 378-383.

Itani, W., A. Kayssi and A. Chehab, 2009. Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. Proceeding of 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, pp: 711-716.

Ke, C., Z. Huang and M. Tang, 2013. Supporting negotiation mechanism privacy authority method in cloud computing. Knowl-Based Syst., 51: 48-59.

Khan, A.W., S.U. Khan, M. Ilyas and M.I. Azeem, 2012. A literature survey on data privacy/protection issues and challenges in cloud computing. IOSR J. Comput. Eng., 1(3): 28-36.

King, N.J. and V.T. Raja, 2012. Protecting the privacy and security of sensitive customer data in the cloud. Comput. Law Secur. Rev., 28(3): 308-319.

Kumar, S., S.P. Singh, A. Kumar Singh and J. Ali, 2013. Virtualization, the great thing and issues in cloud computing. Int. J. Curr. Eng. Technol., 3(2): 338-341.

Lu, Y. and G. Tsudik, 2011. Enhancing Data Privacy in the Cloud. In: Wakeman, I. *et al*. (Eds.), IFIPTM 2011. IFIP AICT 358, IFIP International Federation for Information Processing, pp: 117-132.

Marinescu, D.C., 2012. Cloud computing : Theory and practice∗, pp: 1-404, Retrieved from: http://www.cs.ucf.edu/~dcm/ LectureNotes.pdf (Accessed on: August 5, 2013).

Mishra, R., D.P. Mishra, A. Tripathy and S.K. Dash, 2011. A privacy preserving repository for securing data across the cloud. Proceeding of 3rd International Conference on Electronics Computer Technology, pp: 6-10.

Mowbray, M. and S. Pearson, 2009. A client-based privacy manager for cloud computing. Proceeding of the 4th International ICST Conference on Communication System softWAre and middleware (COMSWARE '09), pp: 1.

Mowbray, M., S. Pearson and Y. Shen, 2010. Enhancing privacy in cloud computing via policy-based obfuscation. J. Supercomput., 61(2): 267-291.

Mell, P. and T. Grance, 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, Information Technology Laboratory, 145, 7. http://doi.org/10.1136/emj.2010.096966

Nandipati, B.L. and G. Sridevi, 2013. A novel computing paradigm for data protection in cloud computing. Int. J. Modern Eng. Res., 3: 2498-2501.

Patel, A., M., Taghavi, K. Bakhtiyari and J. Celestino Júnior, 2013. An intrusion detection and prevention system in cloud computing: A systematic review. J. Netw. Comput. Appl., 36(1): 25-41.

Pearson, S. and A. Charlesworth, 2009. Accountability as a way forward for privacy protection in the cloud. In: Jaatun, M.G., G. Zhao and C. Rong (Eds.), CloudCom 2009. LNCS 5931, Springer-Verlag, Berlin, Heidelberg, pp: 131-144.

Pearson, S., Y. Shen and M. Mowbray, 2009. A privacy manager for cloud computing. In: Jaatun, M.G., G. Zhao and C. Rong (Eds.), CloudCom 2009. LNCS 5931, Springer-Verlag, Berlin, Heidelberg, pp: 90-106.

Porwal, S., S.K. Nair and T. Dimitrakos, 2011. Regulatory impact of data protection and privacy in the cloud. In: Wakeman, I. *et al*. (Eds.), IFIPTM, 2011. IFIP AICT 358, Springer-Verlag, Berlin, Heidelberg, pp: 290-299.

Rajkumar, B., B. James and G. Andrzej, 2011. Cloud computing Principles and Paradigms. John Wiley and Sons, Inc., 111 River Street, Hoboken, NJ, pp: 664.

Ranchal, R., B., Bhargava, L.B. Othmane, L. Lilien, A. Kim, M. Kang and M. Linderman, 2010. Protection of identity information in cloud computing without trusted third party. Proceeding of 29th IEEE Symposium on Reliable Distributed Systems, pp: 368-372.

Sadeghi, A.R., T. Schneider and M. Winandy, 2010. Token-based cloud computing. In: Acquisti, A., S.W. Smith and A.R. Sadeghi (Eds.), TRUST 2010. LNCS 6101, Springer-Verlag, Berlin, Heidelberg, pp: 417-429.

Santos, N., K.P. Gummadi and R. Rodrigues, 2009. Towards trusted cloud computing. Comput. Inform. Sci., 10(2): 3.

Schiering, I. and J. Kretschmer, 2012. The infrastructure level of cloud computing as a basis for privacy and security of software services. In: Camenisch, J. *et al*. (Eds.), Privacy and Identity 2011. IFIP AICT 375, IFIP International Federation for Information Processing, pp: 88-101.

Song, C., S. Park, D. Kim and S. Kang, 2011. Parity cloud service : A privacy-protected personal data recovery service. Proceeding of IEEE International Conference on 10th Trust, Security and Privacy in Computing and Communications (TrustCom), pp: 812-817.

Sun, D., G. Chang, L. Sun and X. Wang, 2011. Surveying and analyzing security, privacy and trust issues in cloud computing environments. Proc. Eng., 15: 2852-2856.

Svantesson, D. and R. Clarke, 2010. Privacy and consumer risks in cloud computing. Comput. Law Secur. Rev., 26(4): 391-397, Doi: 10.1016/j.clsr.2010.05.005.

Sykes, E.R., H. Pham, M. Stoica, K. Mahmud and D. Stacey, 2013. A Privacy-enabled Mobile Computing Model Using Intelligent Cloud-Based Services. SmartData, Springer, New York, pp: 107-115, DOI: 10.1007/978-1-4614-6409-9.

Tchifilionova, V., 2011. Security and Privacy Implications of Cloud Computing-Lost in the Cloud. In: Camenisch, J., V. Kisimov and M. Dubovitskaya (Eds.), iNetSec 2011. LNCS 6555, IFIP International Federation for Information Processing, pp: 149-158.

Ulltveit-Moe, N. and V. Oleshchuk, 2010. Privacy violation classification of snort ruleset. Proceeding of 18th Euromicro Conference on Parallel, Distributed and Network-based Processing, pp: 654-658.

Wang, Z., 2011. Security and privacy issues within the cloud computing. Proceeding of International Conference on Computational and Information Sciences, pp: 175-178.

Wang, C., Q. Wang, K. Ren and W. Lou, 2010. Privacy-preserving public auditing for data storage security in cloud computing. Proceeding of the IEEE INFOCOM, pp: 1-9.

Wayne, W.A. and W.L. Hafner, 2012. An empirical study of privacy risk assessment methodologies in cloud computing environments. Ph.D. Thesis, Nova Southeastern University.

Williams, M.I., 2010. A quick start guide to Cloud Computing: Moving Your Business into the Cloud. Kogan Page Ltd., London, 2010, pp: 139.

Xiao, Z., Y. Xiao and S. Member, 2012. Security and privacy in cloud computing. IEEE Commun. Surv. Tutorials, 15(2): 1-17.

Yang, C.N. and J.B. Lai, 2013. Protecting data privacy and security for cloud computing based on secret sharing. Proceeding of the International Symposium on Biometrics and Security Technologies, pp: 259-266.