Design of Security & Privacy Issues for Cloud Computing

[1]Emrah Dönmez
[1]Faculty of Engineering and Architecture, Department of Computer Engineering
Bingöl University, Turkey

Abstract

Data privacy is one of the most significant issues in web environment. Users surfing on the Internet always want to be invisible from any aspect of web environment. Because of the importance of the privacy, designs should be considered and implemented as block boxes for web applications. Users want to take full control of their privacy but web applications become more and more public and transparent and as a result, privacy control becomes a challenging issue. Privacy in cloud is under pressure by both legal and commercial domains. Therefore privacy primitives should be defined as clearly as possible and management rights of privacy related to the end users should be handed over to them completely. On the other hand, there is another issue which is mostly related to the privacy, and known as security. It is a common sense issue between users and developers in terms of all kind of applications especially for web applications. Security in cloud is the most critical issue which should be increased as maximum as possible. User data are hold or processed in cloud servers, therefore data corruption or loss give rise to high costs if it is not prevented through security precautions, such as; backup modules, secure proxy channels, alternative communication lines (satellite etc.), and cryptographic security modules. In this study major privacy and security problems are defined and possible solutions are proposed, and as future concepts which are related to the privacy and security in cloud are introduced.

Key words: Cloud computing, Data security, Data privacy.

1. Introduction

Data privacy in cloud issues are among the key concerns for institutions and organizations moving to the cloud. In mainly countries and industries, data privacy regulations implement whenever personally identifiable information (PII) is collected and stored. When this information resides in the cloud, it exhibits a unique challenge since cloud computing resources are distributed, making it difficult to know where data is rooted and who has access at any given time [1]. A great number of cloud providers ensure services requiring sensitive data such as bank or payment operations especially in financial services. To regulate data privacy in cloud while performing such operations well defined laws are certainly needed. In addition to law regulations, audit units controlling cloud service providers whose numbers increase day by day, are needed. Because of the virtualized computing, storing and servicing environment of cloud, service providers should concentrate on how the user data can be stored and isolated from each other in distributed resources of cloud while ensuring privacy and as well as security demands requisitioned by organizations, institutions and individual end users. Privacy and security shall be designed with respect to user necessities by considering several fundamental cloud issues; availability, integrity, confidentiality, accountability, and privacy-maintainability. There are

*Corresponding author: Address: Faculty of Engineering and Architecture, Department of Computer Engineering Bingöl University, 12100, Bingöl TURKEY. E-mail address: emrahdonmez@msn.com, Phone: +90(542)309 9325

several ways to provide high level privacy and security in cloud environment, these ways have been introduced in subsequent sections. In section 2, several prominent studies have been mentioned, section 3 describes the most conspicuous privacy and security problems and solution recommendations for these problems, section 4 includes several analysis and observation results about privacy and security actualized in cloud environments, and finally the conclusion of general situations and future expectations have been emphasized in section 5.

2. Related Works

There are a number of study examining both privacy and security issues in cloud. These studies mainly focusing on data privacy regulations in laws, security challenges, optimizing cloud services in terms of security and privacy barriers. Hamouda [2] focuses on securable cloud in terms of security and privacy and mentions several challenges and recommendations. Xiao et al. [3] identify confidentiality, integrity, availability, accountability, and privacy-preservability as five general security and privacy attributes. Tianfield [4] introduces challenges and security issues in cloud computing in terms of fundamental cloud issues. Astrova et al. [5] discuss the current situation in cloud computing by giving benefits and drawbacks.

3. Privacy and Security in Cloud

Cloud services (these services can be infrastructure; IAAS, platform; PAAS, software; SAAS, or security; SeAAS) kept in servers can be located as distributed resources manner in all over the world. Security and privacy focused cloud environment is designed according to these service models in cloud. Each of these model has different necessity in terms of security and privacy. Therefore, cloud designers determine the security and the privacy necessities by determining the service scope of the cloud. Cloud providers wants easy management of their whole cloud environment, since as increasing the rate of distribution of resources, the complexity of management become more challenging and as well as this situation, the cost of these resources also go up. But, in the end, users want to see strong privacy and security in cloud.

3.1. Cloud Servers Location

To convince them about these two critical issues, the data moved to the server farms of cloud can be constructed in location where users contact to the system. Namely, data can be stored or processed in specific locations like a country or city where user belong. For example if a user want to move his data to the cloud he should be able to choose where it will be stored, or processed. This property can be integrated to the cloud provider's service interface. By this way, user's privacy domain are constricted to only a specific geographic location instead of an expanded privacy domain where the location of user data isn't known. This property brings additional cost to the cloud service provider (CSP). Even if total number of servers isn't changed, the cost will still increase. Because the server may transport different locations and each of these servers have to be controlled by a local management system. Therefore, at first step such additional functions can be seen as a disadvantages in aspect of CSPs. But, they will turn to the advantages in the long run.

3.2. Legal Regulations

In addition to cloud center locations, there will appear another problematic issue local laws and regulations about user privacy and data security. Because of laws and regulations can be differentiate from country to country, cloud providers cannot maintain static privacy and security rules. Therefore, providers have to build a dynamic rules cluster of privacy and security that can be easily harmonized to statutes of related country or states. Then, rules are chosen in cluster according to the obligations. Management of these rules for each location separately will be an intensive task itself. Cloud provider can service to a large scope points geographically. Therefore, a large scale resource distribution is formed, and controlling of the whole cloud in one point is not practical. Instead of one point management rights can be distributed to the clustered cloud resources. According to the resource size and geographical conditions, the size of clusters can be determined. If it is necessary, these clusters can be divided into sub-clusters (cluster Middle-East to sub-cluster Turkey e.g.). Management of rules can be easily done through these clusters and sub-clusters. Each sub-cluster creates its own rule pool with respect to laws and regulations of related location. These rules are also added main rules cluster. Aim of this main rule cluster is observation of whole rules and management of sub-clusters from one point.

3.3. Data Transportation between Cloud Providers

Data transportation between cloud providers is an important issue. Since users may want to move their data to another cloud provider because of several problems. For example a small scale provider can stop service and shut down, or user dissatisfied with services of cloud provider, and so on. Then users ask that "is it possible to moving data from one cloud provider (source) to another (target)?" If it can be, then how can one sure that the moved data completely removed in servers of first cloud provider (source). The data can be moved if cloud provider allow this operation. If moving process is allowed data can be transported in several stages. Firstly, it can be done via high speed bands between cloud providers. To implement such data transportation both source and target provider should negotiate. After negotiation and before starting of transfer process the source must be in ready state to communicate with target via port by opening secure channels, then target must notify the source about its ready state to communicate via secure port by reserving an isolated space for user according to the data size or user preferences. Finally, the source observing target as ready should start to transfer user data. After the data transportation, user checks accuracy of the data. If there is a problem, before the predefined service period is not exceed, the problem have to be notified to the source and data transfer must be actualized over problematic part(s) of the data. If any recourse not come in this predefined period, user data must be removed from source provider completely at the end of the this period following data transfer.

3.4. Accountability

If user data is breached in cloud servers or while data in communication process, there will be trouble for both provider and cloud user. Since the breached data can be precious in aspect of cloud user and prestige of cloud provider would suffer as a commercial corporation. Because of this breaching, there can be financial sanctions or penalty according to laws and regulations in aspect of cloud provider, on the other hand there will be able to occur financial and non-

pecuniary loss in aspect of cloud user. To overcome this problem servers of cloud providers can be constructed and configured according to geographic location serviced. The advantage of this situation is the data can be reachable physically under the law. Otherwise, because of data corruption, bankrupting of cloud provider, corruption of connection, service stopping and so on, data could be loss completely. Another solution for data loss using different cloud providers especially for sensitive data at the same time. If user don't store owned data in a reachable physical environment, then the data can be stored in two cloud provider at the same time. If one is corrupt, the data are recovered from other. This solution increases the cost of the cloud in terms of users, however, this operation can be done for only a part of the data that are the most critical ones.

3.5. Data Back-up and Recovery

Data back-up in cloud is an important security issue in terms of preventing data loss by using data recovery from back-up. Since user can feel comfortable with such back-up mechanism in cloud. Otherwise data loss can give rise to big costs for both user and provider. Before the data moved to the cloud, users should check whether the cloud provider have a data back-up system or not, then data moving should be determined. Preventing the data loss while providing the data security are critical points in cloud servers. Cloud providers must construct back-up servers in each geographic location where main servers are resided. When a data loss or corruption occurs, the data can be easily recovered from back-up servers. To increase the potential and strength of the back-up mechanism cloud provider can demanded disk space from user. This disk space is used for sensitive user data determined by users. And size of allocated disk space is decided by users. This disk space size can be either a static size (20GB e.g.) or dynamic size (10% of total disk space or a partition). Control of this disk space can be given to the cloud provider or before any action, disk owner and cloud user can be informed to maintain back-up processes. At the same time this three disk space holding user data can be synchronized automatically or manually. Manually means that when a user changes data in this allocated disk space cloud provider can ask to the user whether the changes should made or not in cloud servers and in addition user can prefer don't change anything or make changes automatically like an OS update. Thanks to this donated disk space sensitive user data are protected at least. If the cloud server holding the user data corrupt the back-up server takes over the recovery duty and user is informed about situation. If the back-up server does not response, then the users informed again. This informing processes at each step ensure a trusted communication between user and cloud provider.

3.6. Confidentiality

Users may want to move their sensitive data to the cloud. It is another security challenge for cloud provider. Since sensitive data protection increases cost of management and maintain for cloud providers. Users may want to know how their critical data is protected in cloud servers. To implement trustworthy cloud environment providers can use data encryption techniques in cloud servers. These encryption techniques or methods should be chosen carefully according to user's profile. Since each user has different necessaries in terms of data security. One can want to access as rapid as possible with light security precautions, on the other hand other can want to see highly reliable data protection with strong security precautions. To provide such operations in cloud

servers, security preferences can be selected by users via cloud interface. Namely there can be security levels like light, medium and heavy protection for data security. For example if user selects light security protection cost of data security is less than other choices and data access is fastest compared to other choices, since to provide light protection fastest and weak (weak means that it may be strong but it is weak compared to the other protection choices) encryption techniques (DES, Blowfish e.g.) can be used. On the other hand, if user selects heavy protection, then cost of data security is more than other choices and data access may be a bit slower compared to others, for to ensure heavy protection slowest but strong encryption techniques (AES, RC6 e.g.) can be used. Of course there are several parameters that affect the durability and speed of encryption techniques (like key size, block size etc.). However for the sake of this paper, encryption techniques are not examined deeply. By allowing users to make preferences for their data security, trustworthy of the cloud environment will increase.

3.7. Integrity

In terms of security cloud providers must take precautions against to data leakage. Data leakage may occur in servers, if there are insufficient security measures. Cloud users enter the cloud spaces allocated for them and they change, delete or add files to these spaces. However cloud provider is not be able to know whether these cloud operations done by real cloud owner or not. To make sure whether real cloud owners done these cloud processes e-mail notification and getting approval mechanism can be used. For instance, when a user make major actions in his allocated space, a mail include messages like "These changes were actualized in your cloud drive. If you don't know please click the below link to undo these changes." from server is sent to the user. After this step, if user undo his actions then he is guided by cloud interface to make password changes. In addition to e-mail notification mobile checking system can also be implemented. If major changes or changes in sensitive data parts take place, then notification about this situation is sent to the cloud user mobile phone as message. For approval a code can be sent to the users and then it is wanted that the code have to be entered to the system with a message and user may notified with a message like "Hello (user ID) cloud user. The code sent by system have to be entered to the cloud interface to make these changes" via cloud interface. Finally, user enters the code to the interface, if code is true, than approval is granted else changes are revoked after three unsuccessful code entry attempt. To increase the level of security in defined period any change in space cloud user is not allowed. If cloud users may make confirmation about these actions done by them, they may select the notification systems (e-mail or mobile) and which part of their space must be notified can be selectable at the same time. Namely, they may want to select only sensitive data (which located into a folder, a file or etc.) in their total data as partially. Cost of these e-mail notification or mobile checking can be externalized to these users as customers. According to their notification preferences, costs changes to downward or upward, and these costs can be calculated according to the file number, file type or file size.

3.8. Availability

Cloud services have to run 7/24 while ensuring access to the cloud processes. Service availability is a critical issue in aspect of user access to the cloud. If a cloud service stops, then user cannot

maintain cloud processes properly. There can be several reasons related to the service stopping. Server connection to the Internet environment can be corrupted by a physical or software-related distortion. Service can include a software-bug that internally resides in any service modules. An external attack to the server can give damage to the server connections, or services. A hardware-related problem like memory or disk reading error can occurs in server, so it can adversely affect the services, and then service(s) could run in unstable state. The first solution that comes to mind is a duplicate server which takes over all tasks from the unstable server. This duplicate server includes all services of original one's. Moreover, this server is connected to the Internet from a separate network line. A proxy computer can be used to fulfill external requests between the server and the Internet. These request are examined for their approval. Another solution is that the service can be reset and then restart. Duplicate service in same server can be used, when service corrupts this duplicate service is awakened from the suspend state and started to take over processes. Server can be protected by extra firewall and system security programs. Server ports should be carefully monitored by an agent to detect abnormal communication patterns like bandwidth saturation.

3.9. System Observation

Cloud users may want to see the cloud server situation in terms of hardware, heating, bandwidth etc. Server situations can be showed periodically to the cloud users in this case. Server situation can be sent in predefined period determined by users. This information service can be run through service agents (tiny programs) in each server. When there are major changes like disk replacement in server or bandwidth increment in network should be also reported to the users. This reporting mechanism should also be selectable via cloud interface. If user don't see such reports, he can switch of reporting service. On the other hand, what kind of information exist in report should be preferable via interface. For instance; while one only concern about hardware changes, other can only concern about network changes or server heating. These server situation reports are also logged in servers to provide statistical data about cloud servers. By referencing these reports cloud providers can determine their next move better. Namely, according to these reports, cloud provider can ensure more efficient cloud services by regulating system periodically.

3. 10. Privacy-Maintainability

Before moving data to the cloud users want to know that what kind of data are collected on cloud server which will hold user data and how these data will be protected. Since one can think that other data in server will be able to affect owned data. Thus, isolation of user data from each data on same cloud server is another challenge. To overcome this situation a protection system is needed. This protection system should control both intrusions and data backup on cloud servers. This Intrusion Detection System with Backup (IDSB) unit should backup the user data while observing system against intrusions. If even data loss or corruption occurs, it can be easily recreated from back-up data. There can be additional precautions; A three layered back-up structure (main server, back-up unit1, and back-up unit2) for instance a second back-up unit can be constructed against to the breakdown of the first back-up unit; since if the data corruption actualize in main server and backup unit does not response because of any problem, second

backup unit can quickly response the data request done by users. This three layered mechanism is good for users, but it is not good for providers, since cost of cloud environment will increases.

3.11. User Agreement

Cloud usage increases day by day. Therefore user requirements increase and diversify in parallel to this advancement. User agreement mostly done by SLA known as service level agreement. This process done by a specialized service is developed as a shadowed structure to general cloud users. But in practice properties of service quality, performance issues, service time warranty, and recovery principles have to be clearly defined through SLA. SLA component periodically should examine requirements for new users and requirements demanded afterwards for old users to create a dynamically adaptive environment. Besides, SLA describes how the offered service being sold. There can be different level of SLA on the same SLA component. SLA can be employed to corporate level to satisfy especially service level management (SLM) requirement of such organizations and it is called corporate-level SLA. On the other hand SLA can be employed to meet user level requirements known as customer-level SLA. Lastly, SLA can be utilized as on service level to cover all of the SLM issues. In conclusion, whether corporate, customer or service level, a SLA should carefully designed to isolate different users in terms of service components and parameters offered, and such layered structure should be designed as a block-box structure that hides the general complexity of SLA mechanism.

4. Analyses and Results

In order to determine the priorities of both cloud providers and users, a small scale survey is performed on 42 cloud providers and approximately 700 cloud users consists of individual and foundational users. In table 1 results of this survey is demonstrated. Although there may be significant number of properties expected from a cloud computing infrastructure, mostly known six properties of cloud are selected. The survey is performed through e-mails (generally for providers and foundations) and face to face interviews (generally for individual users and foundations). As demonstrated in following table cost is the most important property of cloud for providers, then we can say that cloud providers generally consider commercial part of cloud servicing. On the other hand, cloud users mostly concern about privacy. Privacy is higher than security in this survey, main reason of this result is surveyed users have mostly consisted of individual users. If only foundations, organizations and institutions part of these total users are taken into consideration, then the security emerges as higher than privacy.

Table 1. Properties of cloud prioritized by providers and end-users

Properties of Cloud	Cloud Providers		Cloud Users	
Cost of the cloud	42.3%	(1)	12.5%	(3)
Privacy in the cloud	10.4%	(3)	33.8%	(1)
Security in the cloud	37.2%	(2)	30.1%	(2)
Usefulness/Practicability of the cloud	3.3%	(5)	7.2%	(5)
Capacity of the cloud (Storage and Computing)	4.5%	(4)	10.6%	(4)
Customizability of the cloud	2.3%	(6)	5.8%	(6)

According to our early pre-researches organizations and institutions generally concern about security of the data moved to the cloud servers, on the other hand, individual end users generally concern about privacy of the data moved/copied to the cloud environment. From these early findings we can say that organizations and institutions pay attention to the security of data more than privacy, since these data can include strategic information, commercial information, or information wanted to be hidden about these foundations. Individual end users pay attention to the privacy of data rather than security, for these data can include personal information, multimedia data like photos, videos, and music and documents like article, business related data, or etc.

According to our researches it can be said that before data moved to the cloud environment, average cloud users pay attention to the trademark value of the cloud provider. They don't deeply examine the opportunities of the cloud or what type advantages or disadvantages does it has. They also don't pay attention to the privacy primitives of the cloud. The more experienced users look facilities, resources of cloud infrastructure besides its trademark value. They compare cloud provider's advantages and disadvantages. It is found that 79.5% of the total users trust a well-known trademark without looking exactly what it present to them. 20.5% of the total users examine what cloud present as well as its trademark and determine by comparing cloud providers. Main reason of this situation is that the word "cloud" pervade, but usage of cloud is still under crawling phase. Of course there are a great number of users especially corporations, institutions, foundations and so on. In the end, we can say that this settling time of the users to the usage of cloud will not be a long period.

5. Conclusion and Future Expectations

Privacy and security are two closely issues that are given weight by both cloud users and cloud providers at most. There are still several problems in cloud privacy and security which are not remedied clearly. In this paper we touch several major problems and present a couple of solutions against to these problematic issues. Location of cloud servers, data transportation in cloud, data breaching and back-up, encryption, data leakage, cloud server situation, sensitive data protection, and data isolation issues have been examined in terms of privacy and security respectively. Possible solutions to these mentioned issues have been proposed. Analyses have been demonstrated that both security and privacy are significant issues which should be developed as strong and flexible as possible. Since 47.6% of the providers and 63.9% of the users have specified their priorities as privacy and security with respect to researches made. As a result cloud providers may ensure a flexible cloud environment that can be customized with respect to user necessities by overseeing both security and privacy.

Because of these major problems related to both individual and foundational users, cloud providers should present data storage and computing processes as transparent as possible. Since this transparent structure of cloud providers gives them comfort. Moreover, privacy properties are allowed to be completely changeable by users, however security preferences can be handed over partially. Because, some static security options must be controlled by cloud itself. Besides, user should be able to make cloud preferences as maximum as possible. Since such customizable environment gives them comfort and increases the potential customer number.

Cloud environment will be used by almost everyone, we will not need to USB storages, instead of them cloud will be used mostly in near future. A number of cloud providers have already ensured free cloud storage and processing services, but cloud is in a new concept for a significant number of users. In near future this providers will ensure more storage capacity with highly customizable environment (tools, virtual software etc.). There will derive third party cloud security programs protecting user data in cloud drives like desktop ones which provides real time protection against harmful software (virus, malware, trojan etc.). Cloud providers will be able to design a multi-level data protection according to user necessities and users pay for these protection system according to preference of data protection level.

Acknowledgments

We exhibit our thanks to the cloud providers, individual and foundational users who participated the survey about cloud privacy and security mentioned in this paper. Furthermore, this study has been supported by IBM Turkey Scientific Activity Support Program.

References

[1] Donald C., Dowling Jr. International Data Protection and Privacy Law. Practising Law Institute treatise International Corporate Practice 2009; Chapter 24

[2] Hamouda S. Security and privacy in cloud computing. Cloud Computing Technologies, Applications and Management (ICCCTAM) 2012, p. 241-245

[3] Xiao Z., Xiao Y. Security and Privacy in Cloud Computing. Communications Surveys & Tutorials. IEEE. vol.15, no.2, 2013, p.843-859

[4] Tianfield H. Security issues in cloud computing. Systems, Man, and Cybernetics (SMC) 2012 IEEE International Conference 2012, p.1082-1089

[5] Astrova I., Grivas S.G., Schaaf M., Koschel A., Bernhardt J., Kellermeier M.D., Nitz S., Scher F.C., Herr M.. Security of a Public Cloud. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference 2012, p.564-569