EVALUATION OF THE DATA SECURITY METHODS IN CLOUD COMPUTING ENVIRONMENTS

Farhad Soleimanian Gharehchopogh [1] and Meysam Bahari [2]

[1] Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran.
Bonab.farhad@gmail.com, farhad@hacettepe.edu.tr
[2] Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran.
baharicom1@gmail.com

ABSTRACT

Cloud computing is an expression which is used by IT server companies to exchange computing needs as an asymmetrical service of relation for the final receivers of these services. All the models of the cloud computing depend on the resource sharing on the network due to regarding access integrity economic scale. Generally, in most technologies related to the IT, the most important challenge is security. It is particularly more emphasized in cloud computing as the inaccessible control of the final user data cause that the user needs more assure to use and accept this technology. In this case , a lot of efforts are done from service providers (servers), scientific association and so on … in facilitating security issues. In this paper, the methods of data security in cloud computing are discussed by using particular ways. The main goal of this research is to provide strategies for solving related issues and problem of data security which is one of the main goal of sub-structures of data security in cloud computing.

KEYWORDS

Cloud computing, confidentiality, privacy, authentication, encryption.

1. INTRODUCTION

In recent year the cloud computing one of famous term which has emerged since 2006. The Cloud allows users to use and sharing a mass of software and hardware as well as data resource regarding their applications and services[1].The main idea of passing data computing system such as Client/Server and distributed system to cloud computing were the advantages which include reducing costs, more flexibility, automation promotion, integrating data and security[2]. Of course, passage of this term not only mean that the technology of cloud computing doesn't completely put aside the old computing methods such as Grid, Autonomic, Client/Server model, Main Frame, Utility or even Peer to Peer computing systems, but also in most cases, it uses to cooperate these old technologies for making main structure. Lary Alison, the chief executive offices of Oracle Co. noted that " cloud computing is something which we already use without applying any effect on it, except the changes of words in our ads"; It confirms this claim[3]. At the other side, it needs hard work and attempt to remove and substitute old technologies with new and modern ones. Nowadays, in IT world, one of the most prominent security issues in different levels is software and hardware, so, due to the expansion of cloud computing system, the needs for security in different levels is necessary. So, in this article, we discuss about one of the branches of the security and privacy of data by using several particular methods.

The security is referred to data confidentiality or security, data accuracy, integrity and availability which considered important issues for servers. Without proper security considerations very high probability fiasco; Therefore, security issues should be clearly defined in a cloud to avoid the problems that arise [4]. The feature of data security is one of the most challenging and in-process research processes in cloud computing. If hosted-data trade existed in Cloud Service Provider (CSP), we need to make control on data toward the external server by relative security. There are methods to keep main data secure which rely on encrypting techniques and also increase confidence. However, these encryption techniques cause the increase of overload computing. This overhead would increase as data was distributed among several CSP [5]. When security term is discussed in cloud computing and its involved fundamental parts, integrity, data confidentiality and accuracy, many questions would be provided to achieve above-mentioned goals which include as follow:

Which agency and organization is responsible for addressing the failure of commitments of servers? Where must be placed the data and is there a relationship between the sensitivity of data and the type of encrypting and data place? Is data protected due to the paid costs? Is the cloud provider the only responsible for maintaining security and does anyone else in cloud user, country or even international institution responsible in this issue? Which mechanisms and lines can provide access to remote data for users? Is there balance between imposed overhead, financial costs and data importance due to the imposed additional overhead and to maintain security? And finally which mechanisms and policies will be done about trade off? Is data stored as integrated and in a particular place or in different domains? How the security limitations and conditions are be considered in each cases? Which mechanisms will be used for encrypting and security of data? And whether mechanisms will guarantee security?In this article we're going to answer some of these questions.

2. LAYERS OF CLOUD AND IMPLEMENTATION MODEL

The CL-ACC providers provide their services according to 3 models: Interface as a service (Iaas), platform as a service (Paac), and software as a service (Saas) (Figure.1).

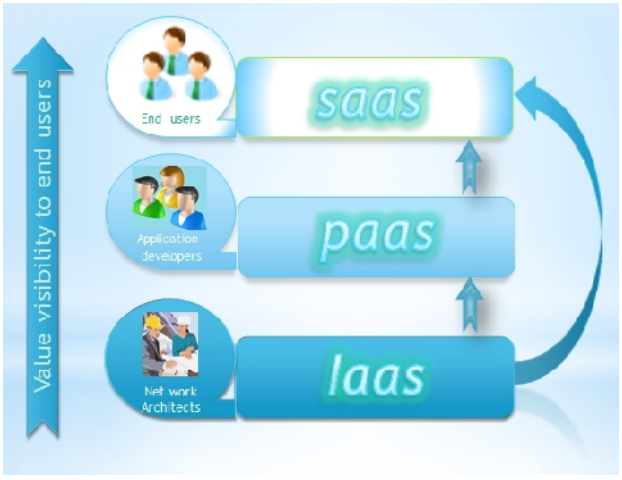


Figure 1. Levels of cloud computing

2.1. Interface as a service (IaaS)

Infrastructure is used as the basic model of cloud service. Cloud servers provide storage media, firewalls, computing load balancing and networks in a virtual context. The providers of this model provide demand resources in a large database. The local network which includes IP address can be used as a secure computing space domain. For doing cloud computing in expanded networks, it can be used internet context and VPN lines as well [6, 7, 8, 9].

2.2. Platform as a Service (PaaS)

In this model, cloud providers produce a computing platform or a mass of solutions which include operating system, programming language runtime environment, database and web service provider to the final user [6,7,8,9]. The developers of applied programs can promote or apply their software in a cloud platform without cost and marketing difficulties and management software and hardware levels. Under a platform as a service, the scale of computing and storage resources are done as automatic in accordance to the users demands, so , the user doesn't do it manually[6,7,8,9].

2.3. Software as a Service (SaaS)

In this model, the cloud computing providers installed and run the applications inside the cloud and the users may have access to the software through the cloud client. By eliminating the needs to install and run applications in the cloud, it is easy to maintain and support computer systems of the users. However, the difference between cloud applications and the other usual programs are their flexibility [6,7,8,9]. This can be done either by dividing the tasks in the number of virtual machines during running time to apply requested changes or by using a load balancer in cloud computing which distributed on a series of virtual machine and resulted in reducing traffic [6,7,8,9]. This process will be clear for the user who perceived just a single access point. For using more users, the cloud application can be used in multipurpose, as each machine provides service for more than one user [6,7,8,9].

In the mentioned level, the levels of security in the cloud computing at different points the users and the service providers should be responsibilities for them [10]. According to National Institution of Standard and Technology (NIST) definition,, cloud settlement models are divided to four main subgroups:

-Public Cloud

Public cloud represents its main and traditional meaning which leased to the users in a limited scope by using dynamic internet lines, in order to have access to cloud [11,12,13]. In public cloud such as public computing model, the user of public services (such as phone and electricity lines) uses a specific services a specified fee [11,12,13].

-Community Cloud

In some cases, as a full-service provider can't meet its obligations, it will be used by community cloud model and other cloud facilities and infrastructures to the final users fee [11,12,13]. As the number of users is usually less than costs, so it is more expensive than public cloud but at the same time, it has high privacy, compliance and security [11,12,13].

-Private Cloud

It is a part of public clouds which is provided for meeting the clouds computing needs in institutions and organizations. And as the facilities, infrastructures and communication lines are controlled by organization, they have more security. But the main problem in this model is to provide and maintain it which can be solved by using virtual private clouds [11,12,13].

-Hybrid Cloud

Which is a combination of public and private clouds. In some necessary times in the one or more domains may use combination of the public cloud and private cloud [11,12,13].

3. SECURITY

The protective goals are often the basis of security requirements which must be done by IT systems as general and cloud computing systems as specific. This security purposes are generally performed due to the user needs from service providers. There are 3 basic goals which include protection or confidentiality, integrity and data accuracy. These include the components of security. As these are used in cloud based computing, the user data are almost out of reach and these 3 components must provide relative security for the final user (Figure. 2).

Figure. 2. Goals of security in cloud computing

Some believe that data inside the organization has more security than outside, but the others believe that the external companies are more motivated in keeping and attracting clients. However, whether the data is external or internal, these 3 components are still having virtual importance. These are described as follow:

3.1. Confidentiality

Confidentiality of a system is to ensure the gathering of confidential data and must be defined in data security system as the confidentiality characteristics such as reviewing to make sure that data

can't be available by inconsistencies [14, 15 ,16]. Of course, it must be considered that there are differences between access t the data which allowed by the user and those which communicate through network. And, it means that confidential data must be kept secure not only in storage but also exchanging along network. Anyways, it must be possible to recognize and take the data which are completely accurate for its data processing and also running review process (the purpose is to send info in network besides security issues. It must be exchanged real and accurate data which is inevitable) [14, 15, 16 , 17].

Generally, for protecting confidentiality of data, encryption and control techniques are used based on strong authentication on data. Data are often moving along dynamic systems (such as hoc networks) and systems which are open essentially (such as systems which are in the platform of internet) [14, 15 , 16]. A cloud service provider or server must be able to store data on its server. It must also be allowed to rewrite and copy of data to optimize infrastructure capacities and ensure from necessary efficiency [14,15,16]. The processes are usually out of reach of clients and this can be resulted in confidentiality issues and problems. For example, if information were available in different places or stored in domains with security rate, it must be applied suitable security overhead to reach them resulted in improving confidentiality condition.

3.2. Integrity

As system guaranteed the integrity of data, it doesn't manipulate without permission or by using unauthorized method. In another word, an integrated system defines as trusted data and messages which are not revealed by a potential interfere [12, 14, 17 , 18]. A cloud computing system should be protected from variability by a third party which pose a risk to the integrity [12, 14, 17 , 18]. If integrity is determined as a good for cloud services, not only the cloud system appearance which is accessible by final users but also the internal part must follow it. In a complicated system such as cloud computing system, integrity can be considered a heavy burden for severs who are responsible for meeting the needs of users [12, 14, 17 ,18].

3.3. Accuracy

The accuracy of a subject is perceived by tools which determined assurance and validation. It can be considered assurance and validation based on a single identification characteristics. The info is valid in the case that can be identified secure by sender and also can be approved that the changes were impossible as the information are created and distributed [14, 15]. Using security techniques to determine the communication patterns and mechanisms to assure the accuracy of cloud computing are among the basic components of this system. These mechanisms must be able to accept or reject the accuracy of the protected information. None of these shared systems can create or distribute message or data beyond the objects (e.g. protected info) [14, 15]. As the economical agency begins to use cloud services, it must be assured from final users' credibility which is one of the basic and important needs. The issues related to different identification management, is a public issue which must be considered [14, 15].

4. THE METHODS OF INFO SECURITY

Suppose that we want to fragment and divide the available data of a database by using particular methods and also considering their security rate in it. After that the data are put in different domains, we begin to exchange data by using safe communication methods which resulted in increasing security and data confidentiality. It is clear that if data fragmentation is done by considering database analyzing points, it deletes the redundancy. Moreover, we can access to the

desired data by using compound techniques. In the later paragraphs, we note to the methods which include discussed issues about security.

4.1. Data Fragmentation

Suppose a relational database which includes several tables. We want to fragment it by using methods and distribute them in different domains by special mechanisms. The reason is that: the fragmentation of relational database resulted in decreasing in the time of data processing, ease of data manipulation, decrease of complexity, data process distribution and facility of data exchange and distribution [5]. Although, this action will impose additional overhead by considering technical and security matters both for data base server and network for exchanging data technically. But, we do it in order to preserve confidentiality and increase user trust [5]. Here, the fragmented tables are divided in 2 groups:

1- Main data tables.
2- Tables which determine communications (relations).

The relationship among tables is done by external or main keys. The fragmented data must meet 3 main needs before they are stored and distributed in different places [5].

1- Data base must be 3nf before any process. So, each table can be appeared as an independent fragment.
2- The level of confidentiality in tables will determine the importance of available data.
3- The user needs will determine the additional demands related to fragment distribution which can be selected by the user.

In the first item, database normalization process is provided to ensure that non-communication and independency is vital. So, each table must have an independent subject, no redundancy in the stored data, extraneous characteristics which are dependent to the main key and also integrity and compatibility.

In this suggested method, the second important item is to determine the security level which depends on the content that is stored in tables.
Here are the 3 different levels of security (Table 1 , Table 2 , Table 3)[5]:

Table 1: with high security

Emp ID	**Credit Card Number**
Ep151	2001 1111 1111 1111
Ep226	2003 1111 1111 1114
Ep212	3123 1111 1111 1114
Ep114	4563 3333 3333 3332
Ep167	3454 2222 2222 2212

Table2: with medium security

Project No	**Project Budget**
EN302	10.000.000
EN505	21.000.000

EN211	8.000.000
EN326	321.000.000
EN400	2.000.000

Table 3: with low security

ZIP	**City**
EN302	City A
EN505	City B
EN211	City C
EN326	City D
EN400	City E

Tables with high security level include date with high sensitivity such as social security numbers, personal ID numbers or credit card numbers which must be properly secured. In order to decrease security actions, we do the followings:

We store the data in a secure space (local domain) without concealing (means that undoing additional actions on data is performed to preserve them) or put them in an external source while we apply concealing actions on them. In the second item, we apply concealing in all columns. Even the names of entities are stored in as codes to stay away. For example, a user can store different kinds of data as encrypted and with high security. In this case, the invaders wouldn't be able to understand whether the database includes credit card numbers or the other data which have low security level. As the hidden feature is used, its keys must be stored in (domain) space and become available. The problem is that it increases the costs of computing as it must be spent time for revealing before query process for each data [5].

4.2. Data Trust Third Party (TTP)

If server doesn't determine how to access the resources and who has access to the data, they can't properly compute the available capacities for the future users. So, cloud computing providers facilitate user security needs by using a supervision mechanism called third parties on systems and also documentation of the planned procedures to respond data security needs [14].this subject will be more important when the user do not control over cloud infrastructure for example location of data storage and so on[19]. By increasing the use of TTP services in cloud, it is provided the increasing trust in levels and more important layers and also resulted in creating proper solutions to keep security, integrity and accuracy in data and communication validity [20]. Technically and legally, TTP provides reliability which caused desired electronic interactions become extracted, produced and independently documented. It is also provided its service guarantees by legal, technical, financial tools and/or structured income resources [14].

TTP includes the following items:

-Security or confidentiality up and down
-Server/Client authentication
-Creating secure domains
-Distributed data encryption
-Authentication based on certificate

4.3. Fragmented data in secure space

In a cloud environment, there are many approaches focus to the problem of data fragmentation security [21]. Providing secure space for data which exchange in network is a complicated and sophisticated process. It is as the attack for creating changes on data and info in one side and applying interval in their exchanges in the other side, are still increasing. For data which become fragmented and put in different domains, we can use Public Key Infrastructure (PKI) which resulted in applying secure communications through IPSec or SSL. IPSec is one of the network protocols which provide the possibility of sending and receiving preserved packages as secure [14]. IPSec often can provide data security and validation and in some cases the possibility of validation [22]. SSL protocol provides point to point encryption by using interactions between two applications. It can also be used TCP/IP protocol for authentication of server and client and encrypted communication channel among them. For connecting applications which situated in different domains, the SSL is anticipated on browsers and there is no need to install applications in client service anymore [14].

In a cloud environment, an authentication server (service provider) is necessary for interaction. It must be involved all levels which included physical infrastructures servers, virtual server, user environment and network facilities. We can use an authentication provider to increase credibility which supports PKI. At the other sides, by using single sign on (SSO) and Light Weight Directory Access Protocol (LDAP), we can use the advantages of top-secured environments to create communication and authentication [14]. In order to use different services, users shouldn't have to authenticate themselves, repeatedly. And, as distributed data are available in different domains, it is highly possible that in a demand, different data were used from different domains. . so, inter-domain servers have to be used SSO techniques to prevent repeated login and log out. Federations will lead us to an efficient secure environment by using PKI and LDAP techniques, simultaneously. Federations are legal entities which applied shared security roles and agreements to access on-line resources. In another words, it is a legal structure which provides authentication and access permission through different organizations [23]. In a presented idea, due to the essence of it which placed different data in different domains by considering their security levels, cloud infra0structures can be organized to domains with separated security issues. The federation clouds are single clouds which can interact with each other. It means that they can exchange data. They can also apply specified connectors to use each other computing resources.

The necessity of different encryption for distributed data cause that data become indiscoverable for those who don't allow having access. In return, this access is provided for the authenticated users. In a cloud environment, the connection between resources and users are often dynamic as ad hoc networks. Most servers, resources and users are not in a secure domain. The users are usually identified by using their features and characteristics instead of their identification before. So, previous identified models which acted based on access control model aren't effective and decision making to control access must be done by features [24].

4.4. Using applied security methods in Client/Server model of database server

As noted before, the cloud computing model is a combination of old computing models. So, by considering this point, we can also apply secure technology and techniques as security strategies. As main database servers provide their services to users by using servers such as Oracle and SQL, we can also use applied security methods in them. An outstanding sample is SQL Azure which most features of it which includes security features was inspired from used SQL server in 2005 and 2008 Windows. For example, it can be noted to the authentication section in which Azure Windows database do authentication in each time of user connection to database (asking for

username and password). Of course, some changes are done based on requirements. In Client/Server model, we can generally use 3 basic parts to create secure space: 1-Security in platform and network 2-Security of database objects 3-Security of the used applications in the environment [25,26].

In database object security such as security methods which are used in database server of Client/Server model, it can be used its optimized forms in cloud computing and note to the followings:

4.4.1 User management

In this part, it can be noted to the security items such as choosing secure password (choose passwords by considering related issues such as compound using of characters), centralized user management, strong authentication, proxy authentication and secure configuration basics which each of the above-mentioned can increase the level of security and its sub-groups [27,28,29].

4.4.2 Access Control

Access control is one of the important issues related to the security in different cases which include subjects such as privileged user controls, controlling database, when, where, who and how to access data and related applications to database, determining row and column level security, multi-level security and data classifications which can do changes based on cloud environment needs and optimized use of previous achievement [27,28,29].

4.4.3 Masking and Encryption

Procedures related to encryption are popular from ancient era to keep the data secure. A lot of works had been doing in this issue, from Cesar encryption method which already decode in a twinkling of an eye to the most modern of them which takes a million years to reveal.

It can also be noted to the cases such as data such as data encryption in network space (input and output data of database which exchange based on encryption standards such as RC4, DES, AES and also SSL techniques), data masking (when we want to transmit sensitive data from an environment which created to the other one to improve applications, test and data analyses) [30], export encryption (in most database server , the possibility of data input and output as encrypted is provided which can be used in credit cards) and back up encryption (not only the data must be encrypted during usage but also when backing up in external storage of media , they must be encrypted) [27,28,29].

4.4.4 Monitoring

Monitoring is one of the main involved parts of the data base server. This service provides the possibility of monitoring of the related applications and interactions on data base effectively [30]. It can be noted to the main parts of monitoring such as database auditing (which usually include auditing records such as auditing procedures, users actions, time and date), fine grained auditing (this technique was introduced by Oracle9i for the first time and provide auditing based on security), audit consolidation, reporting and alerts (considering authentication, priorities, the possibility of access to data auditing, reports and messages will be available) and secure configuration scanning [27,28,29].

5. CONCLUSION

As we noted, one of the most important reason of efforts for promoting security in cloud computing is to assure final users to use resources in a secure and trusted environments. The final user can be a real person, institution or a legal organization. At the other hand, the citizens of a country have more trust to their governments psychologically as the governments have legal commitments toward their nations. So, it must be an idea here, if the main server is out of a geographical border of a country, it can be reached an agreement (creating cloud federation) to input high secured data in internal domain and output lower secured data in external domain(between internal and external server of that country). In some cases, it is possible that dominated rules and regulations on cyber space of a third country made more support of data security than the country itself or the country in which the server is situated (e.g. Switzerland Banks in banking issues). In these cases, if the server company and the company located in the third country are in a same federation, they can exchange data with each other. Any ways, as in most countries, there is a national intranet network, putting all data or data with high importance in internal domain can provide security in maximum level physically. And finally, putting data in security ranking domain along with preferable private and trusted lines and also using encrypted protocols will guarantee integrity, accuracy and data confidentiality. In all these cases, we need fragmented data in different spaces, so after distributing data with noted methods, we can have the secure connection by using secure connection techniques. Consequently, using applied secure features in old computing systems, we can multiply the trust of cloud computing usage for the final users.

REFERENCES

[1] J. Che, Y. Duan, T. Zhang, J. Fan," Study on the security models and strategies of cloud computing", Procedia Engineering, Vol. 23, pp586-593, 2011.

[2] S. Marston, Z. Li, S. Bandyopadhyay , J. Zhang , A. Ghalsasi, "Cloud computing — The business perspective", Decision Support Systems,vol. 51, pp176-189, 2010.

[3] N. Sultan, "Cloud computing for education: A new dawn", International Journal of Information Management , vol. 30, pp109 – 116, .2010.

[4] F..S. Gharehchopogh, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", International Journal of Scientific & Technology Research (IJSTR), ISSN 2277-8616, Vol. 1, Issue. 6, pp 49-54 , 2012.

[5] A. Hudic, S. Islam, P. Kieseberg, E.R. Weippl, "Data Confidentiality using Fragmentation in Cloud Computing", MSc degree, University of East London, pp1-10, 2012.

[6] R. Aoun, Chinwe E. Abosi, Elias A. Doumith, R. Nejabati, ,M. Gagnaire, D. Simeonidou," Towards an optimized abstracted topology design in cloud environment", Future Generation Computer Systems,vol.29, pp46-60,2012.

[7] S. Islam , J.C. Gregoire, "Giving users an edge: A flexible Cloud model and its application for multimedia", Future Generation Computer Systems, vol. 28 , pp823–832, 2012.

[8] W.A. Jansen, "NIST, Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, HI, 4-7 January 2011.

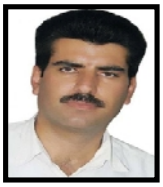
[9] F. B. Shaikh, S. Haider, "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates,11-14 December 2011 .

[10] Z.A. Khalifehlou, F.S. Gharehchopogh, "Security Directions in cloud Computing Environments" , 5th International Conference on Information Security and Cryptology (ISCTURKEY2012), Ankara, Turkey, pp327-330, 17-19 May 2012.

[11] K. ˙Inc ki , ˙I. Arı , H. S¨ozer, "A Survey of Software Testing in the Cloud", IEEE Sixth International Conference on Software Security and Reliability Companion, TUBITAK BILGEM, Kocaeli, Turkey ,pp 18 – 23, 20-22 June 2012.

[12] M.A. AlZain, E.Pardede, B. Soh, J.A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences, Melbourne, VIC, Australia, pp 5490- 5499 , 4-7 Jan. 2012 .
[13] H. Takabi, J.B.D. Joshi, G..J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, Vol: 8, No:6, pp24-31, 2010.
[14] D. Jamil, H. Zaki, "Security Issues in Cloud Computing and Countermeasures", International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp 2672-2676, 2011.
[15] Sambhaji Sarode, Deepali Giri, Khushbu Chopde, " The Effective and Efficient Security Services for Cloud Computing", International Journal of Computer Applications, Vol:34– No.9,pp42-48, 2011.
[16] S. Subashini n, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, pp1-11, ,2010.
[17] B. Gowrigolla, S. Sivaji, M..R. Masillamani, "Design and Auditing of Cloud Computing Security", Dept of Computer Science and Engineering, Hindustan Institute of Technology and Science, pp 292 – 297, 2010.
[18] M.A. AlZain, B. Soh, E. Pardede, "MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing", Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, Sydney, Australia,pp784-791, 12-14 December 2011.
[19] J.R. Winkler, "Securing the Cloud: Cloud Computer Security Techniques and Tactics", Technical EditorBill Meine, Elsevier Publishing, 2011.
[20] D. Polemi, "Trusted third party services for health care in Europe", Future, Generation Computer Systems, Vol. 14 , pp 51–59, 1998.
[21] V. Ciriani, S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P, Samarati, "Combining fragmentation and encryption to protect privacy in data storage", ACM trans, vol. 13,pp1-30, 2010.
[22] A. Alshamsi , T. Saito. "A technical comparison of ipsec and ssl", In 19th International Conference on Advanced Information Networking and Applications, Tokyo Univ. of Technol., Japan, Vol. 2, pp 395-398, 28-30 March 2005.
[23] UK Federation Information Centre, UK federation information centre, 2007.
[24] B. Lang, I. Foster, F. Siebenlist, R. Ananthakrishnan, T. Freeman, "Attribute based access control for grid computing", pp 1-13 , 2006.
[25] G. Brunette, R. Nagappan,J. Weise, "SPARC SuperCluster T4-4 Platform Security Principles and Capabilities",p 20, July 2012.
[26] McGraw-Hill/Osborne, "Sun Certified Security Administrator for Solaris 9 & 10 Study Guide", p.576, 2005.
[27] P. Huey, "Oracle Database Security Guide 11g Release 1 (11.1)",p.374,October 2007.
[28] Sideris Courseware Corp ,"Oracle Database 11g R2: Encryption & Advanced Data Security",P.322, May 9, 2011.
[29] Osborne/McGraw-Hill ,"Oracle Security Handbook : Implement a Sound Security Plan in Your Oracle Environment",p.624, August 2001.
[30] S. Fogel, J. Stern, C. McGregor , "Oracle Database 2 Day DBA 11g Release 1 (11.1)",p.274, February 2012.

Authors



Farhad Soleimanian Gharehchopogh is currently Ph.d candidate in department of computer engineering at Hacettepe university, Ankara, Turkey. And he works an honors lecture in computer engineering department, science and research branch, Islamic Azad University, West Azerbaijan, Iran. for more information please visit www.soleimanian.com

Meysam Bahari is a M.Sc. student in Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran. Email: baharicom1@gmail.com