Received: March 29, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Multilevel Security Framework Based Resource Sharing Using Bilinear Mapping in Cloud Environment

Balamanigandan Ramachandran[1]* **Kamalraj Subramaniam[2]**

[1]*Department of Computer Science and Engineering,*
Karpagam University, Coimbatore, Tamilnadu, India
[2]*Department of Electronics and Communication Engineering,*
Karpagam University, Coimbatore, Tamilnadu, India
*Corresponding author's Email: bala16385@gmail.com

Abstract: During the last decade internet users, researchers and industries have focused on the cloud based technologies. Cloud technology is a distributed and scalable service model and in this model service providers offer the services depending on the cloud users. Security in cloud is a challenge for the service providers , data owners and the service requesters because the cloud providers provide various services such as storage, computing , database and network . All the services focus on data processing in a network to share the information from cloud to users, data owner to cloud and cloud to authenticator. To solve these security issues, in this paper we define a new approach for data sharing issues and service management of Trusted Third Party Authentication (TPA) based on multilevel security framework and bilinear pairing techniques. This framework consists of three modules and these modules are service module, transaction processing module and security module . The next thing is bilinear pairing technique, which uses the pairing techniques to achieve the secure cloud service and improve the computing utility power , store large amount of data and execute the efficient encryption process securely in cloud environment. In this work, the cloud ssecurity requirement has been enhanced using bilinear mapping and multilevel security framework . The result of multilevel security framework is comparatively better than the present day cloud security.

Keywords: Cloud service, Multilevel security framework, Bilinear pairing algorithm.

1. Introduction

Organizations and individual internet users always thought to reduce the time, memory and cost for resource utilization. This type of service oriented computing paradigm are nowadays an on-demand service and users can access the service anywhere and anytime in the universe. Many service providers like Amazon, Google, IBM and Microsoft offering such a kind of services are called as cloud service providers. The service providers (SP) offer the services to the service requesters (SR) based on lease and these services are categorised based on their computation, storage, network and database. Service leasing amount is calculated depending on the usage of infrastructure and time. With rapid growth of cloud consumers and quantity of resource users increasing day by day in the internet market, Specifically in the public cloud which offers the services to SR. In this SR lose the control of data and computing functionalities. So cloud consumers don't know about whether their data and resource are safely protected in the public and hybrid cloud. Security act as a vital role in public as well as hybrid cloud and there are seven major security parameters identified in cloud environment. Within this seven security risk five of them totally focus on cloud data services, which indicated that the resource and data security is the most considerable issue in the cloud computing technology [1].

The major characteristics of public cloud model is its multi-tendency, resource management and distributed computing that could generate various security risks on the resource confidentiality, privacy and integrity. Based on the recent survey calculated, 3000 cloud users show that 84 percentage of users worry about data location and 88 percentage of users worry about storing and retrieving of the data in a cloud [2], [3]. Apart from that, service providers also offer a service called Security as a service (SaaS). In this when SaaS is basically introduced in the market it only deals with protecting the data in the cloud. The problem of cloud security arise because, all the data communication is carried out using remote destination for all computation. Another thing is sending data from cloud to destination in a totally unsecured environment affect the user privacy and lead to more risk [4]. Hence the cloud environment provide less security control in cloud data and resource.

The objective of our proposed work is to improve the security framework in the public cloud environment and it protect data as well as resources. This framework design focuses on a user module, service module, transaction processing module, security functional module and cloud infrastructure. The next thing is bilinear key pairing technique which is used for sharing the data from cloud to consumer and consumer to cloud environment. This bilinear paring algorithm also provide a security for data owners in a cloud, data owners share the encrypted data to service requesters through Third Party Authenticator (TPA). The trusted TPA is a intermediate person between cloud consumer, data owner and cloud service providers.

The rest of the work describe in the following manner: Section 2 fully focuses on the related work. In this related work we will discuss about the cloud security and cloud trust management. Section 3 explains the proposed multilevel security framework and its architecture along with the bilinear pairing algorithm for data sharing. Section 4 describe the implementation and result of cloud security framework .Finally, we conclude how the security framework is adopted with the public cloud environment and the working of bilinear pairing for data sharing to cloud consumers.

2. Related work

2.1 Cloud Security

Cloud security indicates to the wide range of technologies, policies, implemented to provide protection to the data, its oriented applications, and the infrastructure that is associated with the cloud computing. Cloud computing security is the sub-domain of network security, computer security, and more precisely, information security [5].

Security issues involved in Cloud computing and the storage involved provides the users with the capabilities to save and process their data stored in the third party data canters. There are many security concerns that are associated with cloud computing which can be categorised into: security issues that are faced by the cloud providers (institutions that provide data storage on third party data centres) and security issues that are being faced by the customers associated with those third party data centres (people who avail the storage by these organizations) [6]. The storage or the third party data service provider must see to that the infrastructure of their cloud is secure and that the clients data and the sensitive information that are being stored are protected. The user must also take all measures to fortify their data and use passwords that are strong and all the other necessary authentication measures.

When an organization helps to provide a platform to store data or the host applications on the public cloud, it loses its own ability to have the physical access to their own servers hosting information [7]. Thus, the sensitive data of the user is at risk from the insiders attack. Therefore these organizations, ie, the Cloud Service providers must potentially ensure that indefinite background checks were conducted for their employees who have the physical access to these servers in their data centres. In addition to these the data centres must always be frequently monitored for any kind of suspicious activity.

2.1.1 Cloud security controls

Cloud storage architecture is trusted and used only if the correct defensive implementations are made in the storage environment. A good and an efficient cloud storage providing architecture should recognize all these issues that can arise in the security management of the stored data on the cloud. The security management deals with the issues related to the security controls. These effective controls are taken in place to safeguard all the weaknesses involved in the system and to reduce the effects of an attack.

2.1.2 Dimensions of security

The dimensions of security involved in the information security controls are selected and are

implemented depending on the proportion to the impacts, risks, vulnerabilities and threats, and impacts. These factors are taken into account to determine the dimensions of security that is being involved in a cloud storage.

2.1.3 Data security in cloud computing

Data security in cloud environment working on confidentially, access controllability and Integrity. Data confidentiality determines that the contents of the data are not made available or are not disclosed to illegal users. The outsourced data is saved in a cloud and out of the owners control over it. Only the authorized and authenticated users can have an access to these sensitive data while the others, cannot gain any information of the data [8]. Meanwhile, the data owners expect to be fully utilizing these cloud services to store their data, e.g., the data search, the data computation, and the data sharing, without any leakage of data contents to the CSPs or any other adversaries. Access controllability indicates that the data owners can perform any selective restriction or authorization of access to their data that is outsourced to the cloud. The authenticated users will be granted an access by the owner to access their data, while the others cannot access it without the permissions [9].

2.2 Cloud trust management

Cloud computing provides a convenient space for the enterprises by offering a variety of scalable, dynamic and shared services. Generally, the cloud platform providers provide the assurance of their service by specifying their functional and technical descriptions in Service Level Agreements (SLAs) regarding to the services they offer. The descriptions they provide in the SLAs are not persistent among the existing cloud providers, even though they provide services with related and similar functionality [10]. As there is no previous experience in between the consumers and the cloud service providers, consumers often hold a high degree of uncertainty about the quality, performance and reliability of the services being offered by their service provider [11]. Different cloud service consumers could have different preferences and priorities based on the applications they are running. Trust plays a major factor for the success of any interaction within the cloud environment. Hence, trust could be considered as an estimating factor in identifying the future behaviour of another entity in the cloud. Establishing a basic trust level between the cloud service consumers and the service providers is always a major challenge since there is no previous experience between them [12]. Trust is essentially important when data is being processed in a decentralized manner, specifically across different geographical locations. Trust level helps the customers of the cloud service to make their decisions about which cloud service provider to choose for performing their operation. One of the most challenging issues in cloud computing is the trust management [13]. Security and Trust management are considered among the first 10 barriers for the growth of the cloud computing. A trust management system should be able to manage the trust relationships between the customers of the cloud service and the service providers, which will then greatly affect the success of the interaction between them [14]. On the other hand, the identification of the malicious feedbacks remain as a very important challenging issue in the area of trust management. An entity is said to be trusted if it always behaves in the expected manner of the customer for any intended purpose. Trust is considered as a combination of trust management, trust establishment and security aspects. Trust management is a unified approach for evaluating the service entities being provided by the service providers. There are several issues that affect the trust management services in cloud computing, most of which should be applied in order to guarantee the accuracy of the system evaluation. These issues include the Identification of a trustworthy service provider, Privacy of the customer data, security to the customer information, Dependability of the services, Scalability, Integration, non-transparent nature, poor identification of feedbacks, Weak service level agreement etc. [15]. Trust management techniques are classified into four categories namely: policy-based trust, reputation-based trust, recommendation-based trust and prediction-based trust. The Trust Management systems allow relying parties/entities to reliably produce their competence and capabilities of the underlying systems in terms of the relevant attributes. Multiple attributes and information about trust from multiple sources and roots has to be taken into account in cloud computing when selecting trustworthy cloud providers. Trust Management system for cloud computing should always be able to combine multi-attribute based trust derived from multiple roots and sources: soft trust such as user feedbacks or reviews and hard trust such as certificates or audits. In the Trust Management system multiple attributes have to be taken into account to ensure reliable decision making in any application scenario. This is notably true for the environment of cloud computing, where multiple attributes are essential for reliably

determining the nature and quality level of the cloud service provider. A various number of trust management systems were introduced in an effort to measure the reliability and trustfulness of cloud service providers. Making these computed trust values to be available for the customers of cloud service in order to assist them in making their results of decisions in prediction-based trust, which is performed by deriving the unanimity of feedbacks on the same cloud service either trusted or untrusted, thus increasing the quality and nature of the feedback. The approach is centralized. Due to the basic unknown relation in between the customers and the service providers several attacks could occur. This is mainly due to the trust values which should be computed based on the previous experience between both the parties. One of the major challenge that faces computation of trust management is identifying false or tendentious feedbacks. On the other hand, trust management varies due to the differences in calculation, perception, interpretation and criteria. Most of the time, trust is computed based on the overall transaction by neglecting the little components underneath that could affect positively or negatively on the other transactions [16]. In other cases, the computation of the trust is performed with different criteria such as priorities or attributes. The trust values of the cloud providers may be different values at different occasions and applications. Trust Management systems require specific properties to incorporate the attributes for the establishment of trust in a cloud marketplace such as Multi-faceted Trust Computation, Trust Evaluation, Trust Customization, Trust Representation and Attack Resistance.A trust management protocol should accurately compute the trust values of the entities of the cloud. It should also be able to predict the success of an interaction between the customer and service provider based on their past experiences [17]. Trust Management should be dynamic and be updated regularly based on interactions. A trust management system should be capable enough to handle or encounter attacks targeting the system itself. It should also provide services of security, such as validating the identity of the interacting parties and other services such as privacy support, secure storage etc. It should also ensure to be an effective and efficient trust decision tool that ensure the accuracy of trust computation. Therefore, due to this highly dynamic and distributed nature of the environment of the cloud, a trust management system should be highly scalable to conveniently process the collected feedbacks and update the trust results accordingly [18].

The related work is to collect the information and technical issues of cloud service providers, cloud user and data owner. For this concern security and trust is the major problem in public cloud environment [19], so we define the Multilevel security frame with re-encryption technique that is bilinear mapping for cloud ecosystem. The section 3 explains about the proposed multilevel security framework and bilinear pairing technique.

3. Multilevel security framework

Multilevel security framework is specially designed for improving the security of public cloud environment. This framework concentrates on five modules namely: user module, service module, transaction processing module, security functional module and cloud infrastructure. Each module in the security frame worked independently and other cloud functionalities worked as a group. Figure 1 describes about the elements of security framework for all modules. This proposed paper totally focuses on resource and data security, and hence we majorly concentrate on user module and security functional module. User module is a working module for cloud consumers or CR and resource owner otherwise data owner in the cloud environment. In this user module we use a bilinear mapping techniques this is also called as re-encryption technique which is used to protect the sharing resource in a cloud.

3.1 Bilinear pairing techniques

Normally in a crypto system, key pairing is a three member mathematical model. In this proposed framework, the pairing technique involves Cloud Consumers(CC) Who wants the respective secure service from the cloud, Data owner (DO) who is ready to offer the encrypted service outsourcing to cloud server and delegates the re-encryption process to CSP and the Cloud service providers(CSP) access control of the data and re-encrypt the information to new users. The role of CSP is to store the DO services and check the role of the third party authenticator (TPA) that verifies the status of the service and security gateway approval.

Security based researches introduced a special type of data and resource encryption techniques, called proxy re-encryption on the basic working model of the proxy re-encryption defined by the bilinear mapping technique. In this bilinear map a group generator G1, G2 were introduced and it was an additive cycle groups with prime order p: $g_1, g_2 \in G_1$ which were the generators of the group G1. The

finite set denoted as Z and $a, b \in Z_p$ indicates that a,b are randomly selected from the finite set Z.

The encryption function is $e: G1 \times G1 \rightarrow G2$ and this equation denotes the bilinear map. Bilinear is a mathematical model that deals with the combination of two vector space to yield another vector element space. In this cloud security model, the users private key and DO private key b are going to the map in the third vector space that is CSP. This expression is for all $a, b \in Z_p$ and it could be seen that $e(g1^a, g1^b = e(g1, g1)^{ab}$. Figures 1 and 2 show the abstraction of resource requesting and resource allocation process.

Service module is fully based on the cloud resource provisioning to the CC. After that, in this module those who want to share their resource to CC are called DO. The third layer is transaction processing layer in the cloud environment. Once the CC request is received, the TPA verifies the security key and forwards the request to CSP. The CSP checks the resource availability in the cloud and then they allocate the resource to the concerned CC. CSP always allocates the resources based on the request, Monitor the resource availability and status and forwards the lease amount to CC.

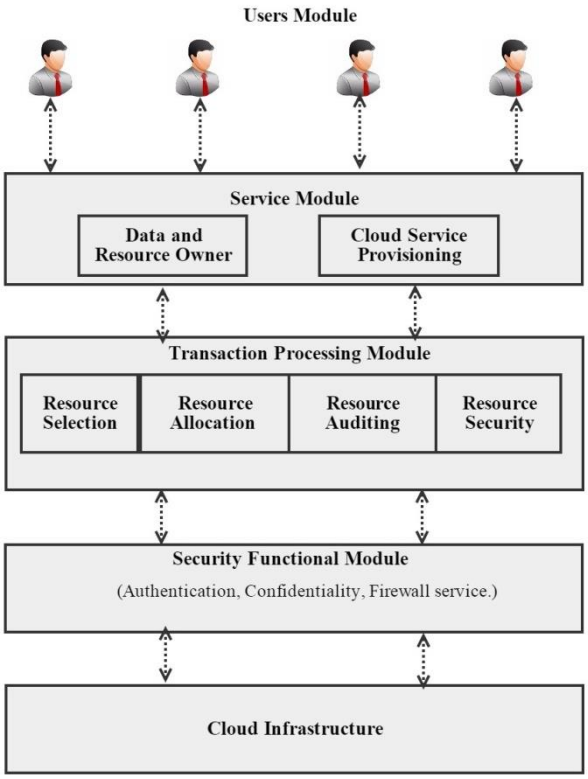

Figure.1 Multilevel security framework architecture

3.2 System operations

The proposed secure data sharing model works on four steps and the table 1 shows the symbols and description of proposed Bilinear Mapping technique.

Step 1: The proposed method operates over two cloud groups G1 , G2 of order p with the bilinear mapping property:$e = G1 \times G1 \rightarrow G2$ and G2 is the random key generation parameter and they distribute the key among the user and the DO. Each cloud users need to select the secret key and generate the random public keys. For example,$(Pk_u = ga^u, Sk_u = a_u)$ for each DO.

Step 2 : Data encryption is done in this step and also key delegation is achieved. Let us assume the DO wants to share the resource or data to user based on request, The DO generates the unique large prime

Table 1. The symbols and description of proposed Bilinear Mapping technique

Symbol	Description
a_d	Secret key for DO.
a_u	Secret Key for User.
ga^d	DO Public Key
ga^u	User Public Key
r	Random Numbers
p	Prime Number
g	A generator for G1
Z	e(g)
pKu	Public Key
Sku	Secret Keu of User
C	Encrypted File
DO	Data owner
CSP	Cloud Service Provider
TPA	Third Party Authenticator

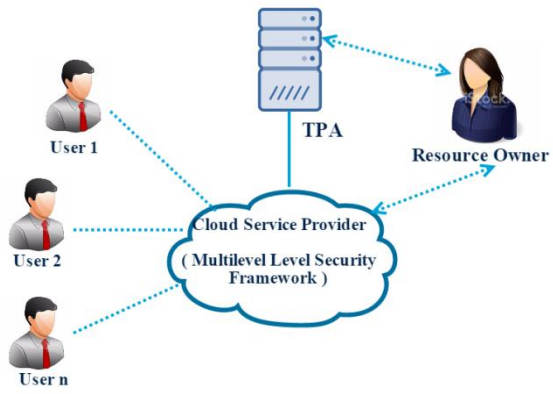

Figure.2 Secure data sharing in cloud environment

number p and also generates random number r for each file F. Then DO outsources the encrypted data as well as a list of authorized CC to the cloud and delegates the service level agreement (SLA) of the resource to the CSP. Then DO makes the TPA responsible for new users and sends re-encrypted key to new users. The encrypted file denoted as Eq. (1).

$$C = (Z^{rq} \ .F, g^{\left(r,\frac{ad}{q}\right)}) \quad (1)$$

Step 3:Data re-encryption is the third step in this multilevel security model. If new cloud user gives a request to CSP to access the encrypted file, then first the CSP is going to check whether the user is authorized user and the user is eligible to access the resource. After the verification the CSP instruct the TPA to generate the re-encrypted key depending on the users public key. Re-encrypted key is defined in the following Eq.(2).

$$re-enkey = pK_u{}^{\left(\frac{gau}{ad}\right)} = g^{\frac{au-gx}{ad}} \quad (2)$$

Step 4:Data Decryption: After getting re-encrypted file, the user can decrypt the file using the user private key. Finally the decryption formula is defined in Eq.(3).

$$F = \frac{Z^{rq}.F}{(Zr^{qau})^{1/au}} \quad (3)$$

After decryption cloud user will use the data and resources securely in the cloud environment. This multilevel framework based bilinear mapping method is proved using mathematical model. In the next section we will discuss the another view of multilevel frame work implementation and result.

Table 2. Working environment setup details

Machine	Host Machine	Guest OS / Cloud
1	Ubuntu 14.0	Windows 2003 Server
		Windows 2003 Server
2	Ubuntu 14.0	Windows 2003 Server
		Windows 2003 Server
3	Ubuntu 14.0	Openstack
4	Ubuntu 14.0	Windows 7
		Windows 7
5	Ubuntu 14.0	Windows 7
		Windows 7

4. Implementation and result

The proposed framework implementation is deployed in Openstack private environment with 5 Intel i7 machines running on ubuntu 14.04. XEN Virtual machine monitor is used for OS virtualization. Windows server was hosted in 2 machines and windows 7 is hosted in 2 machines and the remaining one machine act as the master. The machines are used for testing the multilevel security framework. The system details are given in table 2.

The machine 1 and 2 are working as a server and this server provides the security based on level by level in the security framework. First level is giving security to data owners to upload the resources in the cloud and the second level deals with the service registry protection and tracing the security attacks. Guest Server 2 is in the second level which provides the security to the service provisioning in the cloud environment.

Machine 2 having 2 guest windows servers provide security for sessions and service validation security and also on server working as a TPA. Machine 3 is a controller of overall framework. Machine 4 is having 2 windows 7 guest OS in a host Ubuntu. This guest provide the firewall, functional and Bilinear mapping based security. Machine 5 also has two guest OS where the client and applications are interacting to the servers. The first step is data owner upload the data in the Openstack cloud with encrypted file through server 1 in the machine 1. Once the data is hosted in cloud, server 2 is ready to provision the data resources to the cloud consumers. In this machine 1 we have first level of security that is tracing the user whether the user and data owner is authorized or unauthorized. the tracing process is achieved using cloud studio trace viewer. Machine 2 one server is used to share the data with another user and another server is act as TPA. TPA connected the openstack and it is trusted server for cloud, data owner and cloud consumers. In this server check whether the key and user is authorized or not. Machine 2 and 3 act as a user.

In multilevel framework we have done a negative test because of finding the performance of the security framework. The result of security framework is tested negatively using metasploit attacking. After attack the intruders are identified using cloud studio track viewer. Finally the result of proposed multilevel framework for security provision is compared with current cloud security.

Second thing is the same test is applied in the normal openstack cloud. It will take some time to identify the intruders, finally the result of proposed method is compared with present day cloud.

Table 3 shows the comparison of multilevel security performance with present day cloud. The data processing time is a parameter for evaluate the result in a proposed system.

Table 3. Comparison of multilevel Security Framework with present day cloud

Number of security Levels	Datablock Size(KB)	Number of Data Blocks	Time Taken (ms)	
			Multilevel Security	Current Cloud Security
1	100	5	42	48
2	100	5	45	53
3	100	5	48	58
4	100	5	54	62

Figure 3 shows that the graph is clear and that the multilevel framework cannot affect the performance of normal security system because the security level gradually increases in the multilevel model but the time taken is same what we are using a current security model. In the current security level, data size and time are evaluated in the openstack cloud environment based on that we compare the proposed work. Finally the multilevel security framework achieves a better performance.

Figure 4 shows the comparison of multi-level security performance with current cloud security performance.

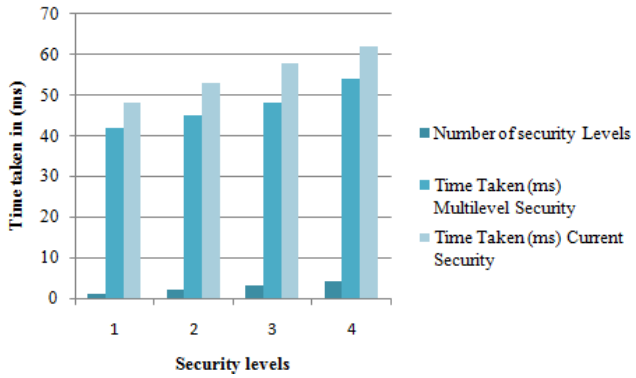

Figure.3 Performance evaluation of multilevel security framework compared with present cloud

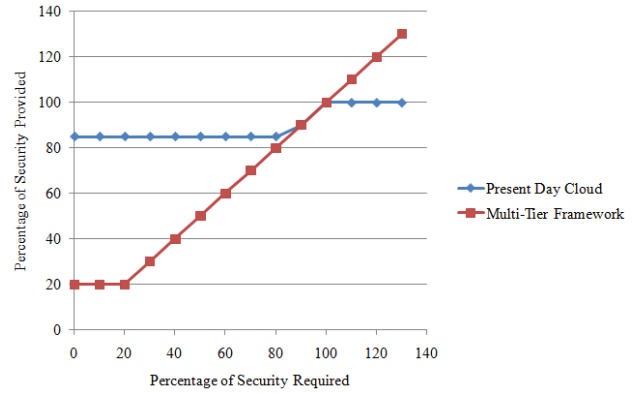

Figure.4 Cloud ssecurity requirement and security provision between present day cloud and multilevel framework

5. Conclusion

The multilevel security framework with bilinear mapping method provide the high level security to the current private as well as public cloud environment. This multilevel framework avoids the unauthorized users and intruders from accessing the cloud based data and resources. This method is used to predict the intruders before accessing the resource in the first security level. Another thing is data sharing between CSP, DO and users. This can be achieved using re-encryption techniques that is also defined as bilinear paring. This encryption techniques was proved in the mathematical model in section three. Finally the both multilevel security frame and bilinear mapping provides high-level security to the cloud environment. When multilevel framework is applied on data, the security is considerably increase when compared to present day cloud security. So in addition the bilinear mapping algorithm helps to reduce the time for data processing .When the data volume increases the security mechanism can be enhanced using data segregation techniques. Cloud users must adapt the security mechanisms provided with data and virtual machines in cloud to provide high level security.

References

[1] M.Ali, S.U Khan, A.V Vasilakos. "Security in cloud computing: Opportunities and chalienges", *Elsevier Journal of Information Security Technical Report Information Sciences*, Vol. 305, pp. 357-383, 2015.

[2] P. Rudlin, "Personal data in the cloud: A global survey of consumer attitudes", *A White Paper on survey on cloud computing, Fujitsu Research Institute*, 2013.

[3] L. Leong, D. Toombs and B. Gill, "Worldwide Survey of Cloud Infrastructure Service Providers*", in by Gartner*, 2015.

[4] J.Amlan, K.Pardeep , S.Mangal, L Hyotaek and L.Hoon, "A Strong User Authentication Framework for Cloud Computing", *In: Proc. of the IEEE Pacific services Computing Conference*, pp.110-115,2011.

[5] S. Balasubramaniam and V. Kavitha, "A survey on data encryption tecniques in cloud computing", *Asian*

Journal of Information Technology, Vol. 13, No. 9, pp. 494–505, 2014.

[6] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", In: *Proc. of the IEEE International Conference on Computer Science and Electronics Engineering,* pp.647-651, 2012.

[7] H. Chen, J. Chen, W. Mao and F. Yan, "Grid Security from Two Levels of Virtualization", *Elsevier Journal of Information Security Technical Report,* Vol. 12, No.3, pp. 123-138, 2007.

[8] T. Hassan and B.D James, "Security and Privacy Challenges in Cloud Computing Environments", *IEEE Computer And Reliability Societies*, Vol.8, No.6, pp.24-31, 2010.

[9] B.H. Krishna, S. Kiran, G. Murali, and R.P.K. Reddy, "Security Issues In Service Model Of Cloud Computing Environment*",* In: *Proc. of the International Conference on Computational Science Procedia Computer Science 87* , pp.246-251, 2016.

[10] S. K. Sood, "A combined approach to ensure data security in cloud computing", *Journal of Network and Computer Applications,* Vol. 35, No. 6, pp. 1831–1838, 2012.

[11] J. Li, J. Li, Z. Liu, and C. Jia, "Enabling efficient and secure data sharing in cloud computing", *Concurrency Computation Practice and Experience,* Vol. 26, No. 5, pp. 1052–1066, 2014.

[12] N. Chidambaram, P. Raj, K. Thenmozhi, and R. Amirtharajan, "Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique", *Hindawi Publishing Corporation International Journal of Digital Multimedia Broadcasting,* 2016.

[13] M. Tahira, Z. Maryam, and A. Gulnoor, "Adopting Information Security Techniques for Cloud Computing–A Survey", In: *Proc. of the 1st International Conference on Information Technology, Information Systems and Electrical Engineering,* pp.7-11, 2016.

[14] S. Udhayakumar, S. Chandrasekaran, T. Latha, and F. Ahamed, "An Adaptive Trust Model for Software Services in Hybrid Cloud Environment", In: *Proc. of the 15th WSEAS International Conference on Computers*, pp. 497-502, 2011.

[15] R.K. Sheu, S.M. Yuan, W.T. Lo, and C.-I. Ku, "Design and implementation of file deduplication framework on HDFS," *International Journal of Distributed Sensor Networks*, 2014.

[16] S. Tan, L. Tan, X. Li, and Y. Jia, "An efficient method for checking the integrity of data in the cloud", *China Communications*, Vol. 11, No. 9, pp. 68–81, 2014.

[17] S. Udhayakumar, T. Latha, "Trusted Computing Model with Attestation to Assure Security for Software Services in a Cloud Environment", *International Journal of Intelligent Engineering and Systems,* Vol.10, No.1, pp.144-153, 2017.

[18] C. Deyan and Z. Hong, "Data Security and Privacy Protection Issues in Cloud Computing", In: *Proc. of the IEEE-Conference on computer science and electronic engineering,* pp.647-651, 2012.

[19] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues", *Elsevier Journal of Future Generation Computer Systems,* Vol.28, No.3, pp.583-592, 2012.