ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Securing Digitally Signed Documents on Cloud Infrastructure

[1]Mr. C. Mani, M.C.A., M.Phil.,M.E., Associate Professor/MCA
[2]Mr. P. DhineshRaaj, Final MCA,
Department of MCA, Nandha Engineering College (Autonomous), Erode-52.
Email ID: cmanimca@gmail.com, dhineshraajp@gmail.com

Abstract-Cloud computing is the most demanded advanced technology throughout the digital world. One of the prominent services offered in cloud computing is the cloud storage.Cloud computing services need to address thesecurity during the transmission of sensitive data and critical documents between shared and public cloud environments. It essentially shifts the user data and application software to large data centres i.e. cloud, which is remotely located, at which user does not have any control and the management of data may not be completely secure. However, this sole feature of the cloud computing introduces many security challenges which need to be resolved and understood clearly.There is a concept for securing data with Digital Signatures in the cloud computing. In the serviceprovider's data centre, protecting data privacy and managingcompliance are critical by using encrypting and managingencryption keys of data in transfer to the cloud. In this study, an attempt is made to review the research in this field. The results of review are categorized based on type of approach and the type of validation used to validate the approach.

Keywords-Data security, cloud data concealment, cloud security, digital signature

I. INTRODUCTION

Cloud computing is an emerging technology which recently has drawn significant attention from both industry and academia. It provides services over the internet, by using cloud computing user can utilize the online services of different software instead of purchasing or installing them on their own computers. According to the National Institute of Standard and Technology (NIST) definition, cloud computing can be defined as a paradigm for enabling useful, on-demand network access to a shared pool of configurable computing resources [1]. According to Gartner [2] cloud computing can be defined as a style of computing that delivered IT capabilities 'as a service' to end users through internet.

According to recent survey by International Data Group (IDG) enterprise, the top three challenges to implementing a successful cloud strategy in enterprise vary significantly between IT and line-of-business (LOB). For IT, concerns regarding security is (66%) and 42% of cloud-based projects are eventually brought back in-house, with security concerns (65%) [3]. A survey conducted by International Data Corporation (IDC) in 2011 declares that 47% IT executives were concerned about a security threats in cloud computing[4]. In survey conducted by Cisco's CloudWatch 2011 report for the U.K. (research conducted byLoud house) 76% of respondents cited security and privacy a top obstacle to cloud adoption [5].

Different countries, IT companies, and the relevant departments have carried out the research on cloud computing security technology to expand the security standards of cloud computing. Existing security technology reflected in six aspects which include: data privacy protection, trusted access control, cloud resource access control, retrieve and process of cipher text, proof of existence and usability of data and trusted cloud computing. To enhance the data security the data can be converted into cipher text, but this may cause to lose many features when data is converted into cipher text.There are two widely used methods to retrieve the cipher text. First, there is a safety index-based approach which establishes a secure cipher text key words indexed by checking the existence of key words. Second, there is a cipher text scanning-based approach which confirms the existence of key words by matching each word in cipher text Lists the top ten obstacles in the popularity of cloud computing.

II. RELATED WORKS

The data security and storage issues are discussed in this article and it also analyses the main reasons of data security issue, possible solutions of this issues and some future development of cloud computing are also discussed. Explains the seven phase of data life cycle in cloud computing that also need security to get user trust these phases include; generation, transfer, use, share, storage, archival and destruction. The aim of cloud computing is to provide better consumption of resources and reduce the work load from user end, but it suffers with security threats. The complexity of security in complete cloud computing environment is shown in fig 1.

In figure 1the lower layer indicates the deployment models of cloud computing namely private cloud,
development of cloud computing are also discussed. Explains the seven phase of data life
cycle in cloud computing that also need security to get user trust these phases include; generation, transfer, use, share, storage, archival and destruction. The aim of cloud computing is to provide better consumption of resources and reduce the work load from user end, but it suffers with security threats. The complexity of security in complete cloud computing environment.

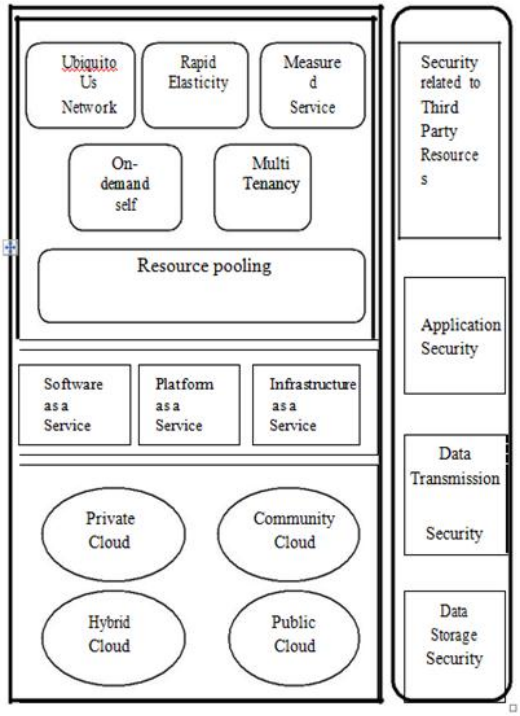

Fig.1 Complexity of security in cloud environment

In figure 1the lower layer indicates the deployment models of cloud computing namely private cloud, community cloud, public cloud and hybrid cloud. The layer just above the deployment model represents the services delivery model of cloud computing. These service delivery models exhibit the certain characteristics that are shown in the top layer. These fundamental elements need security with respect to the characteristics of selected deployment model. Some of fundamental security challenges are shown in the vertical layer given in figure 1.(1) public cloud, that owned by service provider and its resources are rented or sold to the public (2) private cloud,that is owned or rented by an organization (3) community cloud, that is similar to private cloud but cloud resources is shared among number of closed community (4) hybrid cloud, exhibits the property of two or more deployment models .Figure 2 shows the NIST definition framework for cloud computing

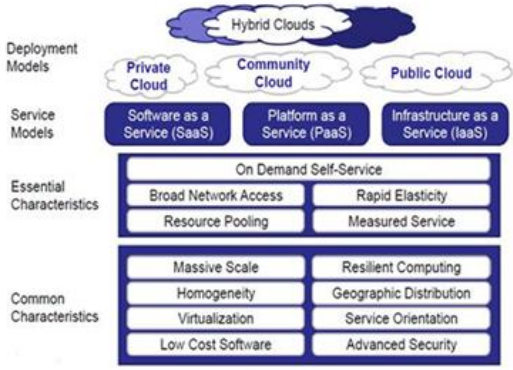

Fig2: NIST cloud definition Frame work

III. SYSTEM METHODOLOGY

Empirical studies are now being undertaken more frequently, as a means of examining a broad range of phenomenon in computer field. A systematic literature review presented in is followed in this research work to conduct the review. The review process is shown in figure 3. A systematic literature review endeavour to provide a comprehensive review of current literature relevant to a specified research questions.

Many researchers contribute their efforts in the field of software engineering/computer science by adopting systematic literature review process such as in systematic literature review process is adopted for the review of aspect-oriented implementation of software product lines components and software component reusability assessment approaches.

The review process has three phases that consist of ten sub activities.This approaches are formulated during the first sub activity of phase 1, a review protocol was developed. The review protocol includes the sources, time period under review and key words used. This protocol is reviewed and validated after making some changes by researchers.

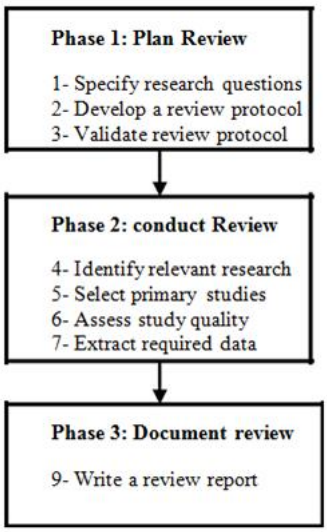

Fig 3: Adapted review process from

The sources used for this review include science direct, IEEE explorer, Google scholar, Scopus, ACM portal digital library. Additionally, we have looked at JCMS, IJSI journals. The research focuses on the year's 2007 to 2014.

In the second phase of review, the search is performed by using different queries related to data security in cloud computing environment. The initial collection of research papers was based on the key words in Table 1 in the papers keywords and abstract. The quality criteria set to assess the studies was to include papers in the review if it contains a model, an experiment, a framework, or a guideline. Therequired data was extracted from the papers to answer the questions posed above.

Another step in the search process was performed by searching the related work area of the selected papers to boost the review strength by confirming that no valuable reference is missed during the search process. The collected data was synthesized to exhibit complete results. Finally, in the third phase of the review process, the review report was written and validated.

APPROACHES HAVE BEEN INTRODUCED TO ENSURE DATA SECURITY IN CLOUD COMPUTING

The result of review (figure 5) show the proposed approaches for the data security in cloud computing. These results are categorized into: (1) Encryption, where the plain text isconverted into cipher text by using some encryption algorithms; (2) Homomorphic token. A technique ensures that we do not need to decrypt the key for data checking instead we can directly compare with encrypted token; (3) Guidelines. Some of the studies have outlined some guidelines to ensure the data security in cloud; (4) Harmonizing scheme. Building a data repository; (5) data concealment component; (6) token;(7) Framework; (8) stripping algorithm.

Question	category	No. of papers
What approaches have been introduced to ensure data security in cloud computing?	Encryption	14
	Homomorphic token	2
	Sobol sequence	1
	Guideline	6
	Harmonizing scheme	1
	Data concealment component	1
	Framework	5
	Stripping algorithm	1
	Total	31

Fig 4: Data security to ensure

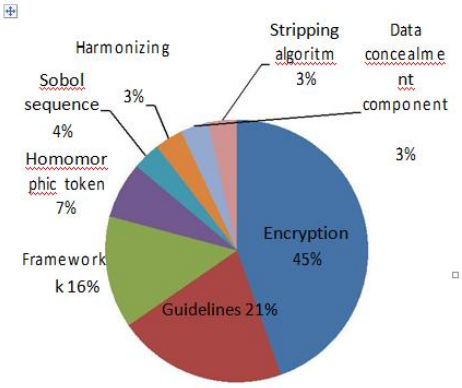

Fig 5: Proposed approaches to ensure data security

A. ENCRYPTION

The results show that most common approach was encryption (45%) to assure the data security in cloud. In a digital signature with RSA algorithm scheme is proposed to ensure the data security in cloud. In which software used to crunch down the data documents into few lines by using "hashing algorithm". These lines are called message digest then software encrypts the message digest with his private key toproduce the digital signature. Digital signature will be decrypted into message digest by the software with own private key and public key of sender.

In playfair and vigenere cipher techniques were merged with structural aspects of Simplified Data Encryption Standard (SDES) and Data Encryption Standard (DES). In which 64 bit block size of plain

text is taken which is fixed and this 64 bit plain text is divided into two halves by using the "black box" the right half have 2 bits whereas left half has 6 bits, then these 6 bits are feed into "superior function" block where these 6 bits are further separated in two halves where first two bits represent the rows and last four bits represent the column by identifying the rows and column the corresponding value can be selected. Then this function is applied to all 8 octets of the output of vigenere block the resultant of black box is again of 64 bits then these bits are further divided into 4 new octants similarly right 4 bits are unified to formulate right halves. Finally, left and right halves are XOR-ed to obtain left half of this arrangement. This process is repeated three times.

In RSA algorithm used to encrypt the data and Bilinear Diffie-Hellman to insure the security while exchanging the keys. In proposed method a message header is added in front of each data packet for direct and safe communication between client and cloud without any third-party server. When user sends the request to the cloud server for data storage then cloud server creates the user public key, private key and user identification in certain server. Two tasks performed at user end before sending the file to cloud, first add message header to the data and secondly encrypt data including message header by using secret key. When user request for data to the cloud server then it will check the message header of received data and pick up the Unique Identification for Server in cloud (SID) information. If SID information is found it will respond the user request otherwise request will be discarded.

A technique is introduced to ensure the availability, integrity and confidentiality of data in cloud by using Secure Socket Layer (SSL) 128-bit encryption that can also be raised to 256-bit encryption. The user who wishes to access the data from cloud is strictly required to provide valid user identity and password before access is given to the encrypted data. In , user send the data to the cloud then cloud service provider generate a key and encrypts the user data by using RSA algorithm and stored the data into its data centre. When user request the data from cloud then cloud service provider verify the authenticity of the user and give the encrypted data to the user that can be decrypted by calculating the private key.In a three-layered data security model is presented in which each layer performs different task to make the data secure in cloud. First layer is responsible for authentication, second layer performs the duty of data encryption and third layer performs the functionality of data recovery. In RC5 algorithm is implemented to secure the data in cloud. An encrypted data is transmitted even if the data is stolen there will be no corresponding key to decrypt the data. In Role Base Encryption (RBE) technique is proposed to secure the data in cloud and role base access control (RBAC) cloud architecture was also proposed which allows organizations to store data securely in public cloud, while maintaining the secret information of organization's structure in private cloud.

In four authorities are defined i.e., data owner, data consumer, cloud server and N attribute authorities where attribute authority's sets were divided into N disjoint sets with respect to the category. The data owner gets the public key from any one of the authority and encrypt the data before sending it to the cloud server. When data is requested the authorities will create private key and send it to the data consumer and consumer will be able to download the file only if he get verified by cloud server. In two types of secure cloud computing are proposed one require trusted third party and other does not. These types use Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing to ensure the data security in cloud environment.

Inlocation-based encryption technique by using user location and geographical position was introduced. In which a geo encryption algorithm was implemented on the cloud and user computer and the data was labelled with the company name or person who work in the company. When the data is required then in the cloud similar label will be searched and retrieved and the information corresponding to the label will be retrieved. In a technique is proposed by using digital signature and Diffie Hellman key exchange in combination with Advanced Encryption Standard encryption algorithm to protect the confidentiality of data stored in cloud. This scheme is referred as three-way mechanism because it provides authentication, data security and verification at the same time.

B. GUIDELINES

The result of our review shows that 21% of studies use guidelines to ensure the security of data in cloud. In guidelines are provided for data security in cloud by introducing new cloud system architecture approach which has three features i.e., separation of software service providers and infrastructure service providers, hiding information about owner of data and data obfuscation. In , agents method is introduce to ensure the data security in cloud architecture. In which three agents namely file agent, authentication agent and key managing agent was used for data security.In guidelines about six key data technologies are provided which are: data privacy protection, proof of existence and usability of data, trusted access control, retrieve and process of cipher text, cloud resource access control and trusted cloud computing. In , guidelines are provided by giving

the meta analysis of four different encryption algorithms that are also helpful to selecting the best algorithms according to need.

C.FRAMEWORK

The framework approach represents 14% of the results. In , a framework is provided; known as Trust Cloud, in which data centric and detective approach is propose to increase the security of data with the objectives to encourage the adoption of file-centric and data- centric logging mechanism to increase the security and confidentiality of data in cloud computing. In , a framework is provided by building a multi-tenant system. In which developed solution is divided into three layers i.e. presentation layer, business logic layer and data access layer. These layers provide very high security to user data.

In a framework is provided that consists of protocol named SecCloud, which is a first protocol spanning secure storage and secure computation in cloud environment by designated verifier signature, batch authentication andprobabilistic sampling procedures. In, proposed framework is consist of three steps, in first step precaution is made against semi-honest cloud service provider by indexing data and its metadata to ensure complete data privacy.

In second step multi user private keyword searchable encryption is performed on encrypted data to keep searches and resulting files secrecy from cloud service provider. Final step makes the use of policy in order to support data sharing between users by using metadata and encryption scheme.

D. HOMOMORPHIC TOKEN

The homomorphic token scheme represents the 7% of the results. Inhomomorphic token scheme is introduced to ensure the data security. The proposed scheme utilizes homomorphic token with distributed verification of erasure-coded data. It supports secure and efficient dynamic operation on data block including data delete, update and append. A model proposed in by utilizing homomorphic token scheme with token pre- computation algorithm to achieves the integration of storage correctness insurance and identification of misbehaving server(s).

E.STRIPPING ALGORITHM, DATA CONCEALMENT COMPONENT, HARMONIZING AND TOKEN SCHEME

Stripping algorithm, data concealment component, and harmonizing and token scheme each represent 3% of the results. In , stripping algorithm is used to secure the picture data in cloud, the approach is consist of three modules which are image analysis, data separation and data distribution. Proposed a design of data concealment component that composed of three sub components: the prediction component, data generator and data marking to secure the data in cloud. The Evaluation of this component shows the successful conceal data of legitimate users and protect them against potential attacks.

A privacy preserving repository presented in , this repository was basically concentrated on the harmonizing operations to achieve data confidentiality while still keeping the harmonizing relations intact in the cloud. This proposed scheme make data owner enables to assign most of computation intensive tasks to cloud servers without disclosing data contents. Proposed an effective and flexible distribution verification protocol to address data security in cloud computing. This protocol utilizes token pre-computation using spool sequence to verify the integrity of erasure coded data instead of pseudorandom data. The proposed model consist of three phases that are: file distribution, token pre-computation and challenge response protocol.

APPROACHES VALIDATION

The results related to the second question are presented here. Figure 6 shows the result of review regarding the procedures adopted for validation.The categories are: (1) Experiment, where an experiment is carried out to validate the results; (2) Comparative analysis, where the results of proposed scheme is compared to other schemes to validate the results; (3) Test bed is used to validate the proposed approach; (4) Statistical analysis, where the results are analyzed by using some statistical technique; (5) Meta analysis is used to validate theresults; (6) Performance analysis, where the performance of proposed approach is analysed by different methods; (7) Some of the proposed approaches have not performed any validation.

The category wise detail is presented in table IV and fig 6 shows the type of validation in percentage. Let us explain the term validation. It refers to any kind of empirical method used as a proof, apart from the demonstration/ application of the proposed approach.The results of the question regarding validation of proposed approaches show that 47% of the selected papers proposed approach to secure data in the cloud environment but provide no validation of the proposed approach.

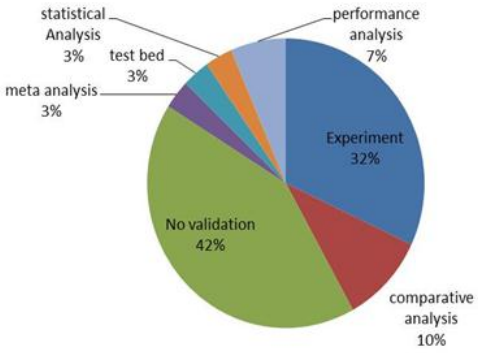

Fig 6: Type of validation

.

A.EXPERIMENTAL APPROACH

Experiments are used to validate the proposed approach in 32% of the selected papers. In, experiment was performed to test the validity of proposed model by using cloud simulator named Hadoop. It shows the status of security after implementing three security parameters which are; Message Authentication Code, classification of data, index and encryption technique. In Aneka 2.0 software is usedin cloud environment to validate the results obtaining by the implementation of RC5 algorithm and then compare these results with Amazon S3 service. Aneka allows building and managing an interconnected network by using Microsoft.NET frameworks on these networks.

In proposed architecture is implemented in Java and results show that cipher text size is linearly proportional to the size of the plaintext and the efficiency of encryption and decryption is very good. Results also show that the size of the decryption key is 48 bytes which is convenient for the users. In cloud service is implemented using C# Microsoft.NET framework for collaborative online documentation. The experimental results show that service response time increases linearly as the size of the input text increases and data obfuscation and de-obfuscation do not cause much overhead, hence proposed approach showed realistic performance. In PHP language was used for the experiment in which performance test is conducted for three phases that are data generation, data marking and data extraction. During the performance test impact of component on data generation was also observed.

B. COMPARATIVE ANALYSIS

Comparative analysis as the form of validation is employed in 10% of the selected studies in which results of proposed scheme is compared to other schemes to validate the results. In comparative analysis is conducted to validate the results by considering following variables granularity, key management, meta data management, level of concealment, degree of distribution and level of implementation. In comparative analysis is made between data Privacy by Authentication and Secret Sharing (PASS) and proposed technique that used trusted third party and non-trusted third party. In the proposed encryption technique is compared with DES, SDES, Playfair and Vigenere encryption technique to validate the proposed approach results.

C. PERFORMANCE ANALYSIS

Performance analysis is used to validate the proposed approach in 7% of selected papers. In, performance analysis is performed in terms of security and efficiency to show that the results are validated and proposed scheme is highly efficient and flexible against Byzantine failure and malicious data modification attacks.

D. STATISTICAL ANALYSIS

Statistical analysis, meta analysis and test bed as the form of validation are employed in 3% of the selected studies. In] NIST statistical test are used to validate the results by selecting eight modern encryption algorithms. In meta analysis of four different security algorithms which are; AES, RSA, Blow fish and DES are presented in term of platform, key size, key used, scalability, initial vector size, security, data encryption capacity, authentication type, memory usage and execution time to validate the results. In test bed is developed and tested for the validation of results.

IV. CONCLUSION

There are many benefits of using cloud computing such as cost efficiency, quick deployment, improved accessibility etc. However, there are yet many practical problems which have to be solved. The data confidentiality is one of them. Manyresearchers contributed their efforts to minimize the data security issue in this domain with different solutions that described in this work. A literature review of the works in the area of cloud computing data security is conducted and the results of review are presented in this paper. The results show that the majority of approaches are based on encryption (45%) out of which 71% encryption techniques results are validated. 67% of encryption techniques used experimentation to validate the results. These results point towards the fact that most of researchers show their interest in encryption technique to enhance the security of data in cloud computing environment. The results also reveals the fact of lack of validation in proposed approaches as 42% of the studies provide no validation of the results out of which 67% are guidelines. Only few studies have used statistical analysis for validation. This area (validation) needs the attention of the research community to gain the

trust and confidence of cloud computing users.

Although our review has explored the field, further studies are needed to confirm the obtained results. Future work includes the extension of this review by including more sources (conferences, journals and workshops) and questions. A future plan is to explore the other security issues in the cloud computing environment and we are also aiming to design a security model using some encryption techniques for data concealment in cloud computing.

REFERENCES

[1] NIST SP 800-145, "A NIST definition of cloud computing", [online] 2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP- 800-145_cloud-definition.pdf (Accessed: 23 December 2013).

[2] Gartner, "What you need to know about cloud computing security and compliance"(Heiser J), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud- computing- Security (Accessed 23 December 2013).

[3] IDG Cloud Computing Survey: "Security, Integration Challenge Growth", [online] http://www.forbes.com/sites/louiscolumbus/2013/08/13/idg- cloud-computing-survey- (Accessed: 28 December 2013).

[4] Ricadela, "Cloud security is looking overcast"[online] http://www.businessweek.com/magazine/cloud-security- is-looking-overcast-09012011.html. (Accessed: 29December 2013).

[5] Nguyen, "Only seven percent of UK it services in the cloud, says survey,Computerworld"[online] http://www.itworld.com/ cloud-computing/200657/only- seven-percent-uk-it-services-cloud-says- surveys. (Accessed: 29 December 2013).

[6] Elahi, T., & Pearson, S. (2007). Privacy Assurance: Bridging the Gap Between Preference and Practice. In C. Lambrinoudakis, G. Pernul& A. Tjoa (Eds.), *Trust, Privacy and Security in Digital Business* (Vol. 4657, pp. 65-74): Springer Berlin Heidelberg.

[7] Siani Pearson, "Taking Account of Privacy when DesigningCloud Computing Services," CLOUD'09, May 23, 2009, Vancouver, Canada,pp. 44-52.

[8] European Network and Information Security Agency (ENISA)"Benefits, risks and recommendations for information security"[online].