ISSN:0975-9646

Cloud Data Outsourcing and off sourcing using trust computation

Priyanka Motwani[#1], Priya Saxena[*2]

[#]*M.Tech scholar, Sanghvi Innovative Academy, Indore, India*

[*]*Asst.Professor,Sanghvi Innovative Academy, Indore, India*

Abstract—**The cloud computing is becomes popular for providing the efficient and scalable experience of computing and storage. Therefore the traditional data hosting and management frequently adopts this approach. But some of industries are not adopting the cloud services due to the data security and privacy issues. The data owners are worried about the sensitivity of data and the privacy of the data owners who faith on them. Therefore the cloud storage services are need to be enhance for improving their trust on end clients and other service providers. In this presented work a detailed study on the cloud data storage services and their distribution is investigated and demonstrated. Thus a detailed review on existing techniques of security and privacy concern is provided and those key issues are addressed. Additionally for resolving the obtained problems a solution is proposed for secure data storage and access on cloud servers.In this context a storage service provider is demonstrated who offers storage services to their clients additionally the intermediate service distributors are also demonstrated that re-distribute the service of primary service providers. Due to this for securing the data on the cloud storage and unsecured network transmission the cryptographic solution is proposed. The proposed cryptographic technique provided by the combination of SHA1 for key generation process and for encryption the AES algorithm is used. On the other hand for securing the communication among two servers a trust computing methodology is prepared. This technique of trust computation includes the server rating by user, dynamicity of IP address, and the number of connection refused. Using these parameters a weighted value is approximated which is used for evaluation of the trust of the requester.The implementation of the proposed concept is provides using the JAVA technology and for deployment a public cloud is used (i.e. OpenShift). After the implementation the performance of the system is evaluated and compared with the traditional RSA algorithm. According to the experimental results the proposed method provides better security as compared to the traditional algorithms.**

Keywords— **data outsourcing, cloud storage services, security, trust management, security**

I. INTRODUCTION

In this age of internet the information and a number of service becomes online. Additionally the rapid development on digital technology the new techniques of internet and their service access is designed. All these efforts are made for improving the utilization of internet based services. Due to access growth of traffic over the internet a scalable source of computation and storage is required. The cloud computing is a solution for such requirements. But the cloud service consumers are worried about the security and privacy concerns of the data. Therefore the security is needed to be improved. Thus a secure and trusted technique is required to motivate the data owners for utilizing the services of the cloud storage[1].

The proposed work is a study of the cloud storage service, which includes the demonstration of distribution of storage services, the intermediate service providers and the user data access and trust management[4]. Therefore a cryptographic cloud hosting service development is proposed in this work. In addition of that how the data securely accessed by the third party intermediate service providers are also provided. The cryptographic technique of storage encourages the data owners to host their data, even when the data is outsourced from the third party data storage. Additionally the system also demonstrates the data access control and management when the request made from the third party host. Therefore a trust based security and access mechanism is also developing to unsecure data access prevention.

The main of the proposed study work is finding the way of secure hosting of the cloud storage servers[7]. Therefore the cryptographic nature of cloud can prevent the data from the privacy and security issues. But when the cloud data storage service provider need to distribute their data through the different intermediate agencies then the intermediate service providers are utilizes the storage and access control service of the basic storage providers. This leads to demonstrate the two way of data management, first primary storage service provider to intermediate providers thus storage needs to be secure the data in cryptographic manner. On the other hand when the secondary server users accessing the data from primary data centers, then during this access control technique is required. The access control of the data can be developed by evaluating the behaviour of user and also depends on the server rate by which the data is going to be access. Therefore that is required to

demonstrate the data storage security and data access management by the clients in secure manner[11].

II. LITERATURE SURVEY

The background technology of cloud computing and the key issues involved in designing the secure and trustworthy system for finding the appropriate and efficient method for performing the trust computation on the cloud environment.

A Data servers

The term "cloud" and "data center" may sound like interchangeable technical jargon or trendy buzz words referring to the same infrastructure, but the two computing systems have less in common than the fact that they both store data [7].

B Data outsourcing

Cloud computing relies on sharing computing resources rather than having local servers to handle applications for a particular organization or individuals. Since there is no infrastructure investment needs, expand or shrink resources based on demand, payment based on usage makes it popular a mong various technologies. Many enterprises look for these benefits to be utilized to maximum extend. Cloud service makes it possible to access information from anywhere at any time [10].

C Data encryption

Classical cryptography provided secrecy for information sent over channels where eavesdropping and message interception was possible. The sender selected a cipher and encryption key, and either gave it directly to the receiver or else sent it indirectly over a slow but secure channel (typically a trusted courier). Messages and replies were transmitted over the insecure channel in cipher-text [11].

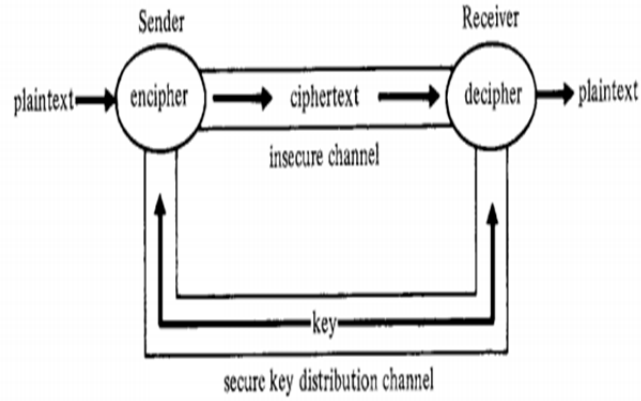

Figure 2.1 information channel

Modern cryptography protects data transmitted over high-speed electronic lines or stored in computer systems. There are two principal objectives: secrecy (or privacy), to prevent the unauthorized disclosure of data; and authenticity or integrity), to prevent the unauthorized modification of data.

D Trust and security

The security issues identified above are very common in any networking environment. All computer or telecommunications networks are expected to provide a certain level of confidence in terms of security although the exact requirements depend on the nature of the application and its intended use. We are slowly migrating from wired networks to wireless networks in which case the security requirements are strict due to the fact that the air interface is open to everyone. As mentioned in the example above, security goes hand in hand with trust[12]. If we do not trust anything or anyone then it will be very hard, or may be impossible to implement proper security in that environment

III. PROPOSED WORK

The section provides the detailed understanding about the proposed secure cloud environment. Therefore the detailed description of the benefits and the solution details are reported.

A. Domain overview

The internet is a huge source of data, knowledge, business and other opportunities. In recent years the awareness about the internet is also increases rapidly. Therefore a significant amount of new user is appeared. Therefore need of computational ability is also increasing in the similar ratio. In order to fulfil this needs the cloud computing offers solutions. That provides scalable computational ability and data storage. This cutting edge technology also offers the developers to add the innovative techniques to implement and also distribute among all. Therefore a huge amount of data is generated and to manage, such amount of data and requests handling need sharing and collaboration techniques. Continuously increasing data and information in a cloud data centers, also increases the data manage cost. Service providers collaborate with third party servers for outsource the data for proper management. But service providers are worried about trust and security, of sensitivity data and their reliability[17].

The proposed work is reports the investigation about the outsourced data and their sensitivity and security issues. Additionally for securing and managing the data with the client level a trust based data access control technique is proposed in this work. The proposed technique not only used for data hosting services that also computes the trust of third party host during distribution and access of data. Therefore a web application for cloud data storage service is intended to created and demonstrate. Additionally for providing the user end trust and security management the upload, download and sharing services are provided. Using these distributable services, other servers which are collaborated with the first party servers denoted as secondary server can also manage their data. The secondary server consumes authentication service and storage space for data outsourcing and access control.

In addition of that for improving data access security and trust, a trust computation technique is also involved in this system. The trust value is computed among two party which are utilizes the services of data outsourcing. For computing the trust the two different security feathers are combined using the weighted technique [5]. If computed trust label is not found secured the primary server not outsources the data nor provides access to data others.

B. Methodology

In order to develop the proposed technique of the data storage services for security and privacy concern the figure 1 provides the initial assumption about the proposed system. According to the given diagram the primary server is developed for providing the cloud storage services. Therefore to distribute the services to the end client primary server offers the service through the intermediate servers (secondary servers) or directly from the primary servers. Therefore the primary service provider needs to secure their storage data using the cryptographic manner[4].

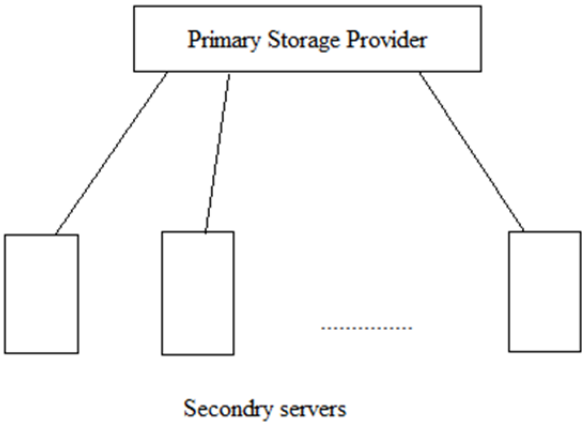

Figure 1 server organization

Additionally during the communication between the primary server and secondary server is also need to be secure for different kinds of security attacks therefore the hybrid cryptographic technique using the SHA1 and the AES algorithm is proposed. In addition of that when the data is accessed using the intermediate servers the primary server need to compute the trust level for providing the data to the user through the requested server. Therefore a weighted trust computation is performed. This weighted trust used to make the decisions for secure data access. Therefore the following organizations of the servers are prepared as given in figure 2.

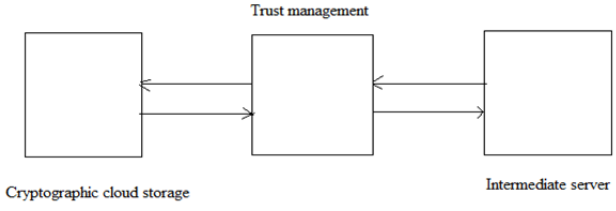

Figure 2 trust management

According to the above given diagram the trust computation is taken place among both the servers when the client makes request for data storage and access. Therefore the two key contribution of the work is demonstrated in two different modules namely cryptographic technique, and the trust computing technique.

Cryptographic process

The proposed cryptographic process for secure data storage is provided using the figure 3. In this diagram the cryptographic process is demonstrated using AES and SHA1 hash generation technique. In this diagram the input data for upload or downloaded by the user is provided to the SHA1 algorithm first. The SHA1 algorithm is kind of hash generation algorithm. That hash is fluctuated as the data is changed that can be due to the errors and other kind of attack process. The length of the SHA1 hash key is 160 bits. That is used with the AES algorithm. But the AES algorithm needs 128 bit key, therefore a key processing system is designed which discard the remaining bits and only generates 128 bit key for used with the AES algorithm. The AES algorithm accepts the input data and the 128 bit hash key for process the information to be store and generates the cipher text[9].

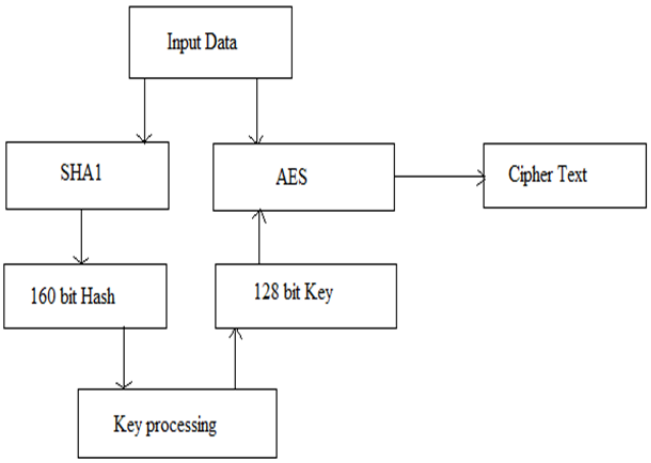

Figure 3 cryptographic process

For more understanding the cryptographic process of encryption algorithm is demonstrated using table 1.

Input: Data D Output: cipher text C
Process: 1. $O = ReadData(D)$ 2. $Key_{160} = SHA1\_Hash(O)$ 3. $Key_{128} = KeyProcess(Key_{160})$ 4. $C = AESEncrypt(Key_{128}, O)$ 5. return C

Table 1 encryption algorithm

Trust computation

The trusts among both the communicated parties are provided using the weight based technique. Therefore number of connection failure is considered as the initial parameter and denoted using N_c. If the intermediate server is not reliable to distribute the services then the N_c is frequently fluctuating and a number of connection failures are observed. In further server IP address are used as IP_{host}, if the server is not secure then this simulate the frequent changes in IP address. Finally the user rating of the server is considered as U_{rating}. All the considered parameters are measured in different scales therefore a factor is required to regulate the values of parameters. Therefore the weighting factors is associated with each the factors for regulating the values between 0-1. The weighting factors are given here as $w_1, w_2, and\ w_3$. The values of these weights always defined in between 0-1. To regulate the computed factors between 0-1 finally the combined weight is computed using the following formula.

$$W = N_c * w_1 + IP_{host} * w_2 + U_{rating} * w_3$$

The computed weights of the host decide the trust level of the requested host and also responsible for the data access and distribution decisions.

IV. Results Analysis

After the successful implementation of the proposed cloud security technique a performance analysis is performed. Additionally for demonstration of effective performance the system is compared with the existing cryptographic security technique. Therefore some essential performance parameters are calculated for comparative analysis. The detailed discussion of the experimentation and results are given.

A. Encryption memory

The amount of main memory required to execute the encryption algorithm, where the input amount of data depends on the user input is known as the encryption memory. The encryption memory is also termed as the time complexity of algorithm. The figure 4 and the table 2 show the encryption memory. In this diagram, the amount of main memory consumption is reported in Y axis. Similarly, the file size used for experiments, are given using X axis. According to the obtained results in both the systems the amount of memory is increases with the amount of file size. The computed file size is given here in terms of milliseconds (MS). According to the made observation in the experimental results the proposed algorithm consumes fewer resources as compared to the traditional encryption technique. Furthermore to estimate the computational cost difference, the mean performances of both the cryptographic techniques are computed. Using the observation table made given in table 2.

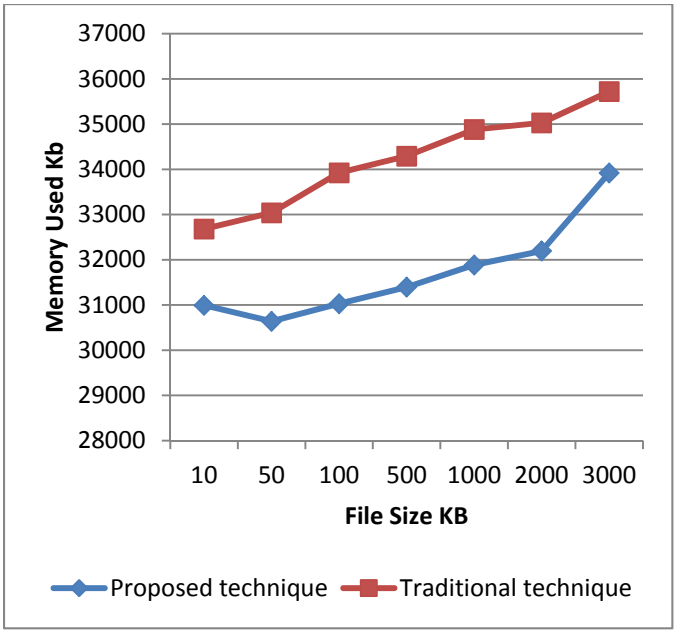

Figure 4 encryption memory

File size (KB)	Proposed technique	Traditional technique
10	30992	32681
50	30638	33039
100	31028	33924
500	31394	34292
1000	31884	34881
2000	32194	35028
3000	33920	35719

Table 2 memory consumption

The mean performance of the techniques is calculated using the following formula.

$$Mean\ Encryption\ time = \frac{1}{N}\sum_{i=1}^{N} O_i \dots\dots\dots\dots\dots\dots (Eq1)$$

Where the O_i is the observation made and N is the number of observation is taken. The figure 5 contains the mean performance of the algorithms. The given figure contains the methods implemented, in X axis and the Y axis, is reported mean encryption time in milliseconds. According to the evaluated results the memory consumption of the RSA algorithm is higher enough as compared to proposed light weight algorithm.

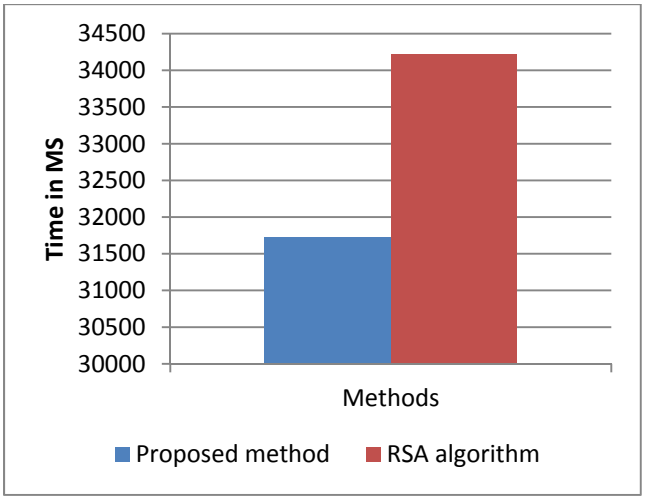

Figure 5 mean memory consumption

B. Decryption memory

For a cryptographic algorithm the amount of main memory required, to recover the original text from cipher is defined as decryption memory. That can also be termed as space complexity of decryption. The figure 6 and table 3 shows amount of memory consumed during data recovery. In the diagram X axis shows the different file size used for experimentation and Y axis reports amount of main memory consumed. The described main memory is measured here in terms milliseconds. According to the obtained results, main memory utilization is increases as experimental data size is increases. According to the computed results RSA algorithm consumes higher memory as compared to the proposed algorithm. Additionally the table 3 provide the quantities of the memory consumption. For differentiating the performance the mean performance of the system is also computed as defined in equation (1). The mean performance of both the algorithms is represented in the figure 7. In this diagram the Y axis contains the files size in KB used for experimentation and the X axis shows the implemented methods. The diagram clearly shows the difference of the memory utilization in both the techniques. Thus according to the demonstrated results the proposed algorithm consumes less memory for data recovery.

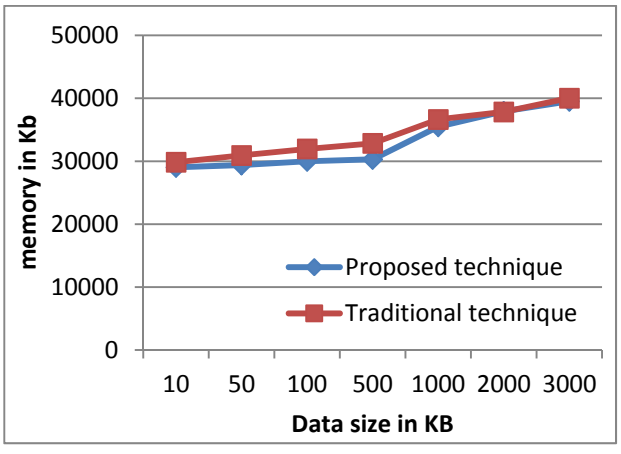

Figure 6 decryption memory

File size	Proposed technique	Traditional technique
10	29019	29847
50	29383	30924
100	29981	31947
500	30284	32844
1000	35472	36649
2000	37918	37845
3000	39519	40029

Table 3 decryption memory used

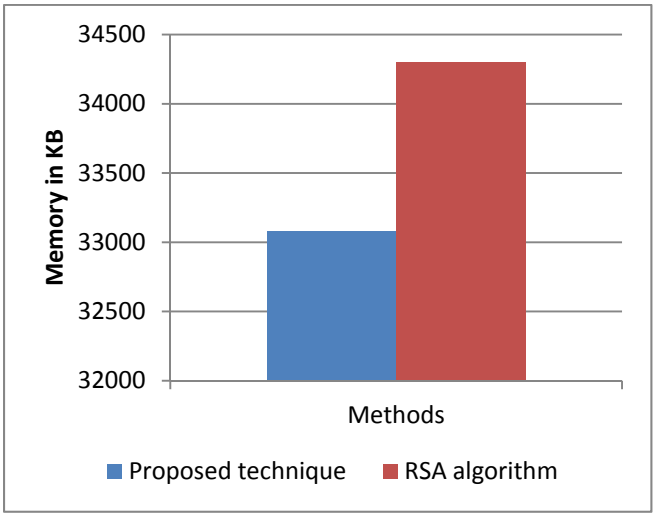

Figure 7 mean performance

C. Decryption time

The time difference between initialization of data recovery and finishing the recovery work is termed here as decryption time. This can also be termed as the decryption time complexity.

File size	Proposed algorithm	Traditional system
10	0.331	0.547
50	2.04	3.38
100	4.12	6.21
500	18.14	28.42
1000	34.93	46.52
2000	68.25	112.53
3000	105.39	158.45

Table 4 decryption time

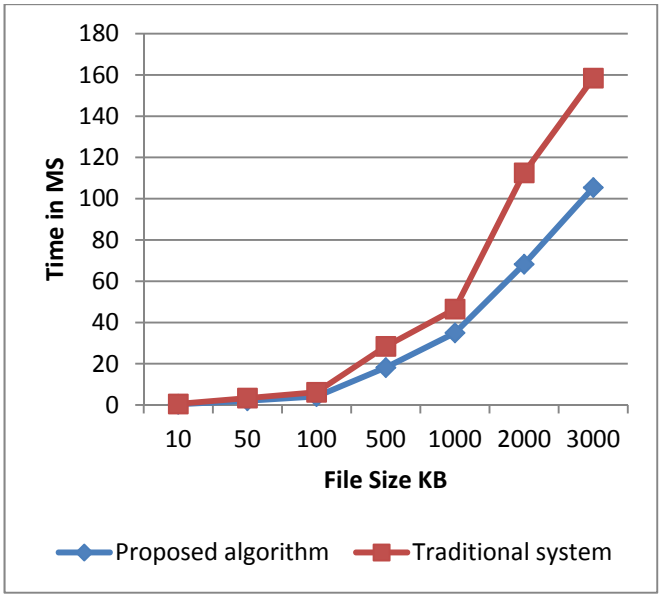

Figure 8 decryption time

The figure 8 and table 4 shows performance of the system, in terms of decryption time. To show performance of both techniques, blue line used for proposed algorithm and red line is used for traditional algorithms. In given figure, X axis includes the file size of experimental dataset, and Y axis shows required time for data recovery. According to the observations the encryption time is higher than the decryption time, but decryption time, of the proposed algorithm is efficient as compared to RSA algorithm.

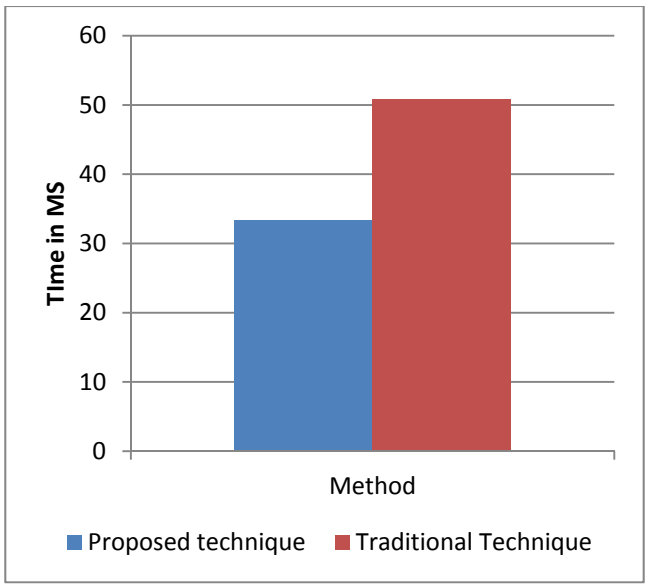

Figure 9 mean time complexity

To justify the results the mean time consumption is measured using the equation (1). The computed time is demonstrated using the figure 9. In this diagram the X axis shows the implemented techniques and the Y axis shows the corresponding mean time complexity of the algorithms, in terms of milliseconds.

D. Encryption time

The encryption time is measurement of time interval, computed between initialization of the encryption process and the end of process. That is also termed as the encryption time complexity. Figure 10 and table 5 shows the encryption time of both the techniques (i.e. proposed and traditional system (RSA algorithm)). In this diagram X axis shows file size used in experimentation and Y axis shows amount of time consumed, for processing input file size. The performance of proposed system is given using blue line, and traditional algorithm is represented using red line. According to given results proposed system consumes less time as compared to RSA algorithm. The result show amount of time consumed is depends on the amount of data to be process. The respective performance of system shows their effectiveness over the traditional RSA algorithm. In order to identify the computational time overhead more clearly the mean time consumption of the system is computed and demonstrated using the figure 11. The given diagram includes the encryption time in Y axis of diagram, in terms of KB, and the X axis shows the techniques implemented. According to the given observations the performance of the traditional RSA algorithm is cost effective as compared to the proposed cryptographic technique.

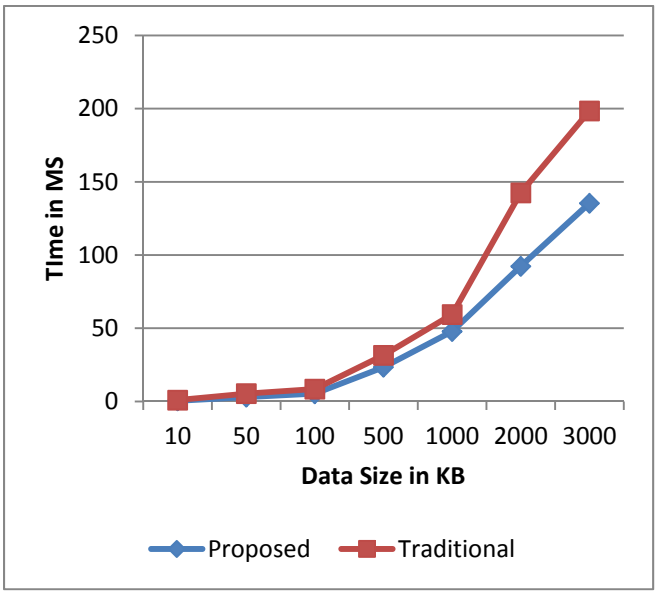

Figure 10 encryption time

File size	Proposed system	Traditional system
10	0.473	0.947
50	2.94	5.38
100	5.32	8.47
500	23.42	31.53
1000	47.82	59.41
2000	92.31	142.53
3000	135.33	198.44

Table 5 encryption time

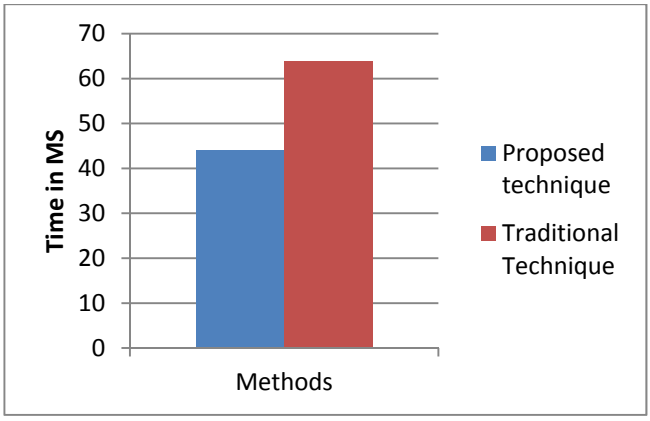

Figure 11 mean time consumptions

V. CONCLUSIONS

The main goal of the proposed study work to achieve the full proof security for data storage and access is prepared. This section provides the summary of entire work performed and the concluded facts are reported. In addition of that future extension of the proposed technique is also included.

A. Conclusion

As the new techniques for internet surfing is increases in the similar amount of work load on the servers are also increases. Therefore the need of computational and storage units is increases in recent years. But the collection, processing and re-distribution of the data are a complex task. Therefore recently a number of efforts are made to support the huge data request handling. The cloud computing offers the solutions for increasing load of data hosting and management. In addition of for demonstrating the scalable storage in cloud the service providers outsource the data on third party data storage service providers. Therefore the data owners are worried about the data sensitivity and privacy concerns. In this presented work the data management and hosting services are investigated, and a solution is formulated for enhancing the reliability, sensitivity and distribution of data with preserving the privacy techniques.

In this context a simulation model for data storage service provider and data re-distribution is demonstrated. During this the two different servers are prepared first primary server which is storage service provider and a secondary server who consumes the services of the primary server. Using the given infrastructure the entire data management, security and data access mechanism is developed. For providing the security on the primary server the cryptographic security is developed. The proposed cryptographic technique is developed with the help of SHA1 and AES algorithm. That approach provides security of data during network transmission and storage space also. In addition of that for managing the secure and controlled access of the data a trust based security is also implemented among the two different server communications, the trust computation usage the technique of weighted formulation. That is used to make decision for the secure communication and data exchange among two service providers also.

The implementation of the proposed technique is provided using the JAVA based technology and the performance of the system is noticed and compared with the traditional RSA algorithm. The performance summary of the proposed technique is provided using the table 6.

S. no.	Parameters	Proposed	RSA algorithm
1	Encryption time	Low	High
2	Decryption time	Low	High
3	Encryption space	Low	High
4	Decryption space	Low	High

Table 6 performance summary

According to the given experimental results the proposed security technique is found optimum and also produces the less overhead during the cryptographic security. Therefore the proposed work is adoptable for secure data storage services.

B. Future work

The proposed system is an adoptable end to end security system for storage service providers and the intermediate service providers. In addition of that it can be used in various other domains of security and privacy. Therefore that can also be extended for the following domains.

1. Implementation of the ABE algorithm makes it more robust for utilizing the service securely.
2. The given concept can be utilizes in the banking and military applications for securing the information.

REFERENCES

[1] Deyan Chen, Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, 2012 International Conference on Computer Science and Electronics Engineering, 978-0-7695-4647-6/12 $26.00 © 2012 IEEE

[2] Guojun Wang, Qin Liu, Jie Wu, MinyiGuo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”, ª 2011 Elsevier Ltd. All rights reserved

[3] Dongyoung Koo, JunbeomHur, Hyunsoo Yoon, “Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage”, 2012 Elsevier Ltd. All rights reserved.

[4] torryharris, “CLOUD COMPUTING – An Overview”, http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

[5] Vaishali Jain, Akshita Sharma, “A Taxonomy on Cloud Computing”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014

[6] Balvinder Singh, Priya Nain, “Bottleneck Occurrence in Cloud Computing”, National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications

[7] MilenkoRadonic, “Cloud vs. Data Center: What's the difference”, http://www.glbrain.com/index.php?r=tool/view&id=2103&toolType=1

[8] ChittajalluSaiMeghana, “Security and Services Management Aspects of Cloud Architectures”, http://www.idrbt.ac.in/PDFs/PT%20Reports/2013/Chittajallu%20Sai%20 Meghana_Security%20and%20services%20management%20aspects%20of%20cloud%20architectures_2013.pdf

[9] V. Abricksen, "A Survey on Cloud Computing and Cloud Security Issues", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014)

[10] SwapnaLia Anil, RoshniThanka, "A Survey on Security of Data outsourcing in Cloud", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013

[11] KratiMehto, Rahul Moriwal, "A Secured and Searchable Encryption Algorithm for Cloud Storage", International Journal of Computer Applications (0975 – 8887) Volume 120 – No.5, June 2015

[12] PradipLamsal, "Understanding Trust and Security", Department of Computer Science University of Helsinki, Finland, 20th of October 2001

[13] Sheikh MahbubHabib, Sebastian Ries, Max Muhlhauser, "Towards a Trust Management System for Cloud Computing", 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)

[14] Khaled M. Khan and QutaibahMalluhi, "Establishing Trust in Cloud Computing", Published by the IEEE Computer Society 1520-9202/10/$26.00 © 2010 IEEE

[15] Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring", Published by the IEEE Computer Society, 1089-7801/10/$26.00 © 2010 IEEE, IEEE Internet Computing

[16] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10/$26.00 ©2010 IEEE

[17] JagpreetSidhu and Sarbjeet Singh, "Compliance based trustworthiness calculation mechanism in cloud environment", International Workshop on Intelligent Techniques in Distributed Systems (ITDS-2014), © 2014 The Authors Published by Elsevier B.V

[18] C. Bharathi, V. Vijayakumar, K. V. Pradeep, "An Extended Trust Management Scheme for Location Based RealTime Service Composition in secure cloud computing", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), © 2015 The Authors. Published by Elsevier B. V

[19] Atta urRehman Khan, Mazliza Othman, Sajjad Ahmad Madani, and SameeUllah Khan, "A Survey of Mobile Cloud Computing Application Models", IEEE Communications Surveys & Tutorials, Accepted For Publications

[20] Zheng Yan, Peng Zhang, Athanasios V. Vasilakos, "A survey on trust management for Internet of Things", & 2014 Elsevier Ltd. All rights reserved.

[21] SmitaSaini, Deep Mann, "Identity Management issues in Cloud Computing", International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 8 – Mar 2014

[22] Eric Kuada, "Towards Trust Engineering for Opportunistic Cloud Services: A Systematic Review of Trust Engineering in Cloud Computing", Aalborg Universitet, Publication date: 2014.