ISSN:2231-0711
Rakesh Kumar | IJCSET(www.ijcset.net) | 2020 | Volume 10, 17-20

Results Analysis for PAVD Cloud Computing Security System

Rakesh Kumar
Department of Computer Science & Engineering
Guru Nanak Dev University, Amritsar, India
1rakeshbhagat54@gmail.com

Abstract: This paper has based upon result analysis for PAVD security system. For the experiments, we had developed a set of 5 sample data files of 100 KB, 200 KB, 300 KB, 400 KB and 500 KB size. The task is to evaluate the existing PAVD and proposed group based digital signature PAVD system by these data and in this paper and also evaluate the upload and download time of Box, Drop box, Google Drive and Sky Drive. To draw comparison between PAVD security system and proposed group based digital signature PAVD system based on the following parameters: Down- load time, Upload Time, Overheads, Response Time and Execution time.

Keywords: PAVD, Cloud Computing, uploading, Downloading, Security problems, Data Secrecy, Group Signature.

Performance Metrics

The experiments are carried out using MATLAB, JAVA and common storage as a service cloud providers and the performance of the proposed system is analyzed using some evaluation metrics. This section deals with the detailed description of various performance metrics to effectively compare the existing PAVD technique and proposed group based digital signature PAVD system. The parameters are:

- Upload Time
- Download Time
- Overheads
- Response Time
- Execution time

In our proposed group based digital signature PAVD system, there is a basic task of data file encryption, uploading, downloading, and decryption. This process executes as:

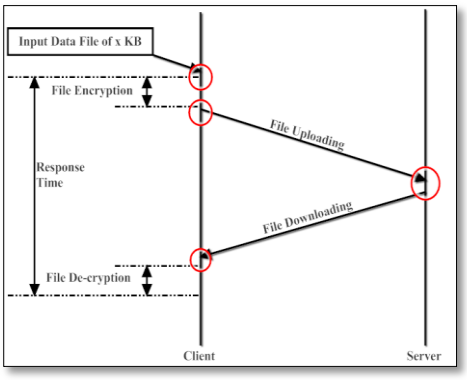

Figure 1: Data file encryption, Upload, Download, de-cryption, response time and overheads in RED ovals.

Figure 1, demonstrates the time taken by the proposed group based digital signature PAVD system and the various overheads that are marked RED in the Figure. These all time measures are detailed in this section as:

1. **File Encryption Time (T1):** It is time taken to encrypt the data file of size X and produce an encrypted file of size Y. We had used AES encryption algorithm and this algorithm is basically a block cipher. It requires adding some padding to develop the blocks. This extra padding is an encryption overhead and is calculated as:

   (1)

   This overhead is calculated in milli-seconds.
2. **Upload Time (T2):** It is the time taken to upload an encrypted data file of size Y to the cloud. It is measured in seconds.

   (2)

   For this metrics, we had taken 2 time instances, 1.The system time before initiating the upload and 2. The system time after successful uploading of the data file on cloud. The difference of these 2 time instance is the file upload time.
3. **Download Time (T3):** It is the time taken to download a file of size Y from the cloud. It is calculate similar to that of upload time by considering the time Instances. This time is calculated in seconds.

   (3)
4. **File De-cryption Time (T4):** It is time taken to decrypt the data file of size Y and produce a decrypted file of size X. This time is calculated in milli-seconds.
5. **Total Execution Time:** This is the sum of the time taken to encrypt, upload, download and decrypt the data file. It is calculated as:

   —— —— (4)

   Where, T1 is the time taken to encrypt the data file, T2 is the time taken to upload the data file, T3 is the time taken to download the data file and T4 is the time taken to decrypt the data file.

6. **Response Time:** The response time is basically the sum of the Total Execution time and the other time overheads. This is calculated by differencing two time stampings. One is taken before starting the process and one is taken after successful execution of the task. It is represented as:

(5)

By this above equation, we had calculated the time overhead, as:

(6)

RESULT ANALYSIS

For the experiments, we had developed a set of 5 sample data files of 100 KB, 200 KB, 300 KB, 400 KB and 500 KB size. The task is to evaluate the existing PAVD and proposed group based digital signature PAVD system by these data files.

Objective – 1: To evaluate the upload and download time of Box, Drop box, Google Drive and Sky Drive.

Here, we are going to upload a sample data file of size X to the cloud and then download that data file in order to test the performances of various storage as a service providing cloud services. Table 1 and Figure 2, demonstrates the time taken by various common storage as a service providers for uploading of various data files through their provided portals.

Table 1: Upload time of various common cloud storage providers.

File Size	Box	Sky Drive	Drop box	Google Drive
100KB	7	6	5	8
200KB	9	8	7	15
300KB	10	12	7	20
400KB	11	16	5	20
500KB	12	18	13	22

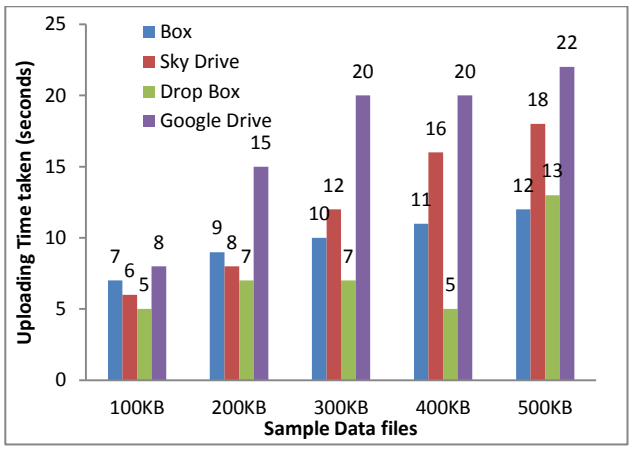

Figure 2: Data file uploading time of various common cloud storage service providers

From the Graph in Figure 2, it is depicted that the time taken by the Drop box is minimal in all the cases while for the Google Drive it is maximum. The Sky drive is showing an averaged performance from all the evaluated cloud storage service providers.

Table 2 and Figure 3, demonstrates the time taken by the cloud service providers for the file downloading through their portals as:

Table 2: Download time of various common cloud storage providers.

File Size	Box	Sky Drive	Drop box	Google Drive
100KB	3	5	5	6
200KB	4	6	5	6
300KB	6	10	5	7
400KB	6	14	6	8
500KB	10	16	7	10

From the Graph in Figure 3, it is depicted that the Drop box had taken minimal file download time for high sized data files that other evaluated storage services. The Sky drive had taken maximal download time for all types of files. Whereas the Box had shown best performance for the downloading of the data files of smaller size.

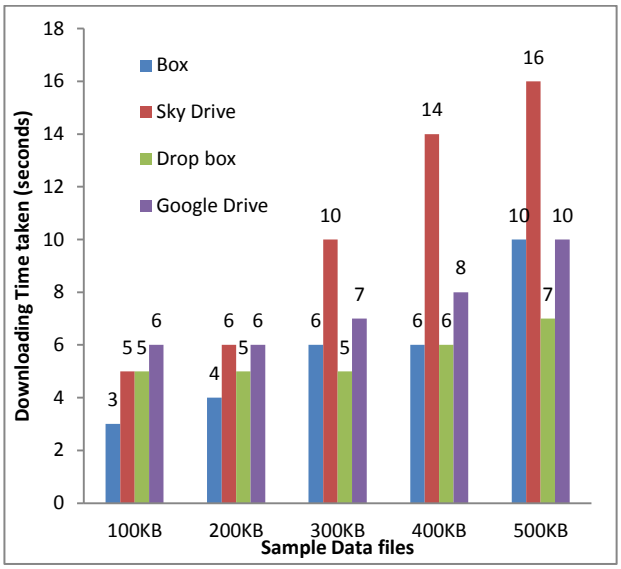

Figure 3: Data file downloading time of various common cloud storage service providers

Objective – 2: To improve the PAVD security system by using the group based digital signature in cloud environment.

For the improvement of the existing PAVD system, we had added the AES encryption for the data file which are to be uploaded and the key exchange is carried out using Diffie-Hellman key exchange algorithm, which leads to enhanced security in proposed group based digital signature PAVD.

Table 3: Various Time measure of proposed group signature based PAVD System

Data File	Encryption Time (Milli-Sec)	Uploading Time (Sec)	Download Time (Sec)	De-cryption Time (Milli-Sec)	Execution Time (Sec)	Response Time (Sec)	Overheads (Sec)	Overheads (KB)
100 KB	44	3.54	3.138	144	6.866	12.773	5.907	1
200 KB	52	3.72	3.426	210	7.408	13.25	5.842	16
300 KB	144	4.82	5.534	222	10.72	15.99	5.27	16
400 KB	186	6.27	6.088	268	12.812	19.23	6.418	15
500 KB	216	7.02	6.52	312	14.068	20.368	6.3	15

Objective – 3: The group based signature also provides freedom to group members to send and receive data directly to manager which will reduce the authentication overhead.

For the group based signature it will reduce the authentication overheads because intermediated directly send the data on cloud. There are many no. of member and they do not directly communicate to cloud. If they directly communicate to cloud the authentication overheads will increase and cloud is too many time busy that's why the member's send and receive data to manager and only manger communicate to cloud. So, this senior the authentication overheads will reduced and also enhanced the security.

Objective – 4: To draw comparison between PAVD security system and proposed group based digital signature PAVD system based on the following parameters: Download time, Upload Time, Overheads, Response Time and Execution time.

Table 3, demonstrates various time measure taken to test the performance of the proposed group signature based PAVD system. This measure defines about the performance of various sub processes that are carried out as sub-parts to accomplish the final goal of group signature based PAVD. The encryption time, uploading time, downloading time, de-cryption time, total execution time, response time, overheads in file size after encryption and overheads in time had been shown as:

Table 4, represents the uploading and downloading time of the existing PAVD system proposed by[ReferenceToPAVD] in seconds for the data files of various sizes of 100 KB, 200 KB, 300 KB, 400 KB and 500 KB. These results are directly taken from [ReferenceToPAVD], and added up to get the response time of the existing system.

Table 4: Upload and Download times of Existing PAVD approach

Data Size	Uploading Time (Sec)	Download Time (Sec)	Response Time (Sec)
100 KB	6	5	11
200 KB	12	7	18
300 KB	16	11	27
400 KB	21	15	36
500 KB	26	19	45

Table 3, shows the performance of the proposed group based PAVD system and the Table 4, shows the performance of the existing PAVD system in terms of Upload, download and Response Time. Figure 4, shows the performance enhancement in data file uploading time as:

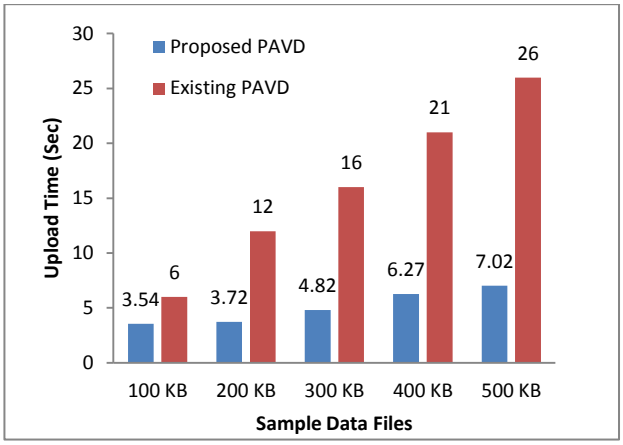

Figure 4: Comparison of Data File upload time of existing PAVD and proposed PAVD

From the Graph in Figure 4, it is depicted that the uploading time of the proposed group based PAVD system is far less than the existing PAVD system. On more visualization is that the uploading time is increased with data file sample size in fewer propositions to its size. Figure 5, demonstrates the comparison of the download time of the existing PAVD and the proposed group signature based PAVD system as:

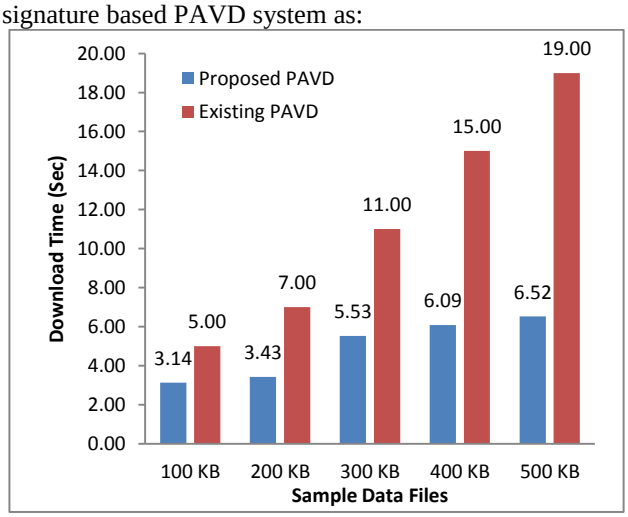

Figure 5: Comparison of Data File download time of existing PAVD and proposed PAVD

From the Graph in Figure 5, it clearly depicts that the download time of the sample data files in case of proposed group signature based PAVD system is far less than existing PAVD System. Figure 6, demonstrates the comparison of the response time of the proposed group signature based PAVD and the existing PAVD system as:

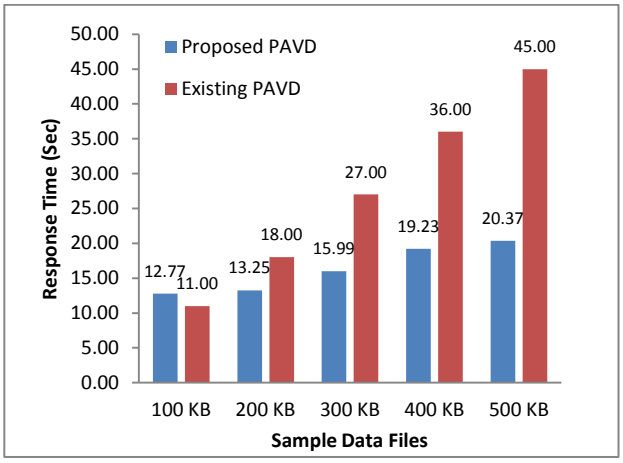

Figure 6: Comparison of the response time of existing PAVD and Proposed PAVD

From the Graph in Figure 6, it is depicting that the response time of the proposed group signature based PAVD system is less than that of existing PAVD system, which proves the better working and more reliable proposed system. PAVD is performing better for the smaller files, but for the medium sized files, the group based system is performing better.

CONCLUSION AND FUTURE SCOPE

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services and from huge number of applications, number of systems for secure data transmission have been proposed in recent years. In this work, we had ex- tended one of the existing technique called PAVD to group signature based PAVD. A protocol in which the group digital signature is generated using the strong RSA algorithm. In this method the freedom of the member is sacrificed by sending the message through the group manager. From experiments, the extended technique is working better than available PAVD technique. This research has offered a new framework which is based on group based signature to reduce communication overheads in PAVD security system. The group based signature will enhance the data storage and also provide the freedom to group member to send and receive data directly which will re- duce the authentication overheads. The overall objective of this paper is to offer a PAVD security system which is based upon Group based signature to reduce login overheads. In near future we will design and implements proposed technique in MATLAB Tool with the help of MATLAB Tool Box also to use some quality measure to evaluate the effectiveness of the proposed technique.

FUTURE SCOPE

In future this protocol will be re-modified with members freedom to send and receive the data directly in the cloud but at the same time, we have to keep in mind that traceability of user by the group manager must be maintained. Moreover, other Key exchange, Encryption algorithm can also be applied for enhanced security and better offloading of the data.

REFERENCE

[1] Mell P., Grance T., 2011 NIST Special Publication 800-145: The NIST Definition of Cloud Computing.

[2] Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia (2009). Above the Clouds: A Berkeley View of Cloud Computing. EECS Department, University of California, Berkeley.

[3] Buyya, R., C. S. Yeo and S. Venugopal (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. International Conference on High Performance Computing and Communications IEEE Computer Society.

[4] Vaquero, Luis M., Luis Rodero-Merino, Juan Caceres, and Maik Lindner. "A break in the clouds: towards a cloud definition." *ACM SIGCOMM Computer Communication Review* 39, no. 1 (2008): 50-55.

[5] Nurmi, Daniel, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff, and Dmitrii Zagorodnov. "The eucalyptus open-source cloud-computing system." In *Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on*, pp. 124-131. IEEE, 2009.

[6] Gens, Frank. "Defining "cloud services" and "cloud computing"." *IDC exchange*23 (2008).

[7] Shaikh, Farhan Bashir, and Sajjad Haider. "Security threats in cloud computing." In *Internet technology and secured transactions (ICITST), 2011 international conference for*, pp. 214-219. IEEE, 2011.

[8] Plummer, D. C., T. J. Bittman, T. Austin, D. W. Cearley and D. M. Smith (2008). Cloudcomputing: Defining and describing an emerging phenomenon, Research(Ed, Gartner), p.1-9.

[9] Rongxing et al, ―Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing‖, ASIACCS'10, Beijing, China..

[10] R. La'Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA.

[11] Mladen A. Vouch, ―Cloud Computing Issues, Research and Implementations‖, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[12] Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada

[13] Soren Bleikertz et al, ―Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds‖, CCSW 2010, Chicago, USA.

[14] Flavio Lombardi& Roberto Di Pietro, ―Transparent Security for Cloud‖, SAC'10 March 22-26, 2010, Sierre, Switzerland.

[15] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciesnces 2011.

[16] Jinpeng et al, ―Managing Security of Virtual Machine Images in a Cloud Environment‖, CCSW, 2009, Chicago, USA

[17] Miranda & Siani, ―A Client-Based Privacy Manager for Cloud Computing‖, COMSWARE'09, 2009, Dublin, Ireland

[18] Dan Lin & Anna Squicciarini, ―Data Protection Models for Service Provisioning in the Cloud‖, SACMAT'10, 2010, Pittsburgh, Pennsylvania, USA

[19] Selvi, S., S. Sree Vivek, C. Pandu Rangan, and Nikhil Jain. "Cryptanalysis of Li et al.'s identity-based threshold signcryption scheme." In *Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on*, vol. 2, pp. 127-132. IEEE, 2008.

[20] Neela, T. Jothi, and N. Saravanan. "Privacy preserving approaches in cloud: a survey." *Indian Journal of Science and Technology* 6, no. 5 (2013): 4531-4535.