PSDS: Privacy Preserving System for Data Security Implementation and Countermeasures

Arpit Sohani
Computer Science Department
Jagadguru Dattatry College of Technology,
Indore (India)
Rajiv Gandhi Proudyogiki Vishwavidyalaya
(State Technological Univercity of State Madhya Pradesh, India)

Khushboo Sawant
(Asst. Prof.)
Computer Science Department
Jagadguru Dattatry College of Technology, Indore (India)
Rajiv Gandhi Proudyogiki Vishwavidyalaya
(State Technological Univercity of State Madhya Pradesh, India)

ABSTRACT
The Cloud computing is a latest technology which provides various services through internet. The Cloud allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data.Search over encrypted data is a technique of great interest in the cloud computing era, because many believe that sensitive data has to be encrypted before outsourcing to the cloud servers in order to ensure user data privacy. In this paper, we proposed cryptography based Privacy Preserving System of Data Security i.e. PSDS. We implement AES algorithm to perform encryption and decryption. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when assessing shared data integrity.

Keywords
Data Security, Encryption, Decryption, AES, Cloud Computing, Cryptography, Privacy Preserving.

1. INTRODUCTION
Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements [1].. Need for self-services, universal network processing of a network location autonomous resources availability, spontaneous resources flexibility, pricing is determined on the level of usage also on the risk of the transfer [2].As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud, such as e-mails, personal health records, company finance data, and government documents, etc. The fact that data owners and cloud server are no longer in the same trusted domain may put the outsourced unencrypted data at risk [3] the cloud server may leak data information to unauthorized entities [4] or even be hacked [5].

1.1 Cloud Data Storage
In the last decade, the demand of outsourcing data is greatly increased. Data storage and high performance computation are the main needs which have to be fulfilled. These services are provided by many cloud computing service providers like Drop box, Amazon Simple Storage Service (AmazonS3), etc. The advantage of storing data in cloud servers is that the data owners can reduce the overhead of buying extra strong servers and also avoid hiring of server management engineers. Data encryption is a basic solution to maintain security of data and the encrypted data is uploaded into the cloud. Depending on the possibility to identify privacy and security users cannot join the cloud computing systems [6].

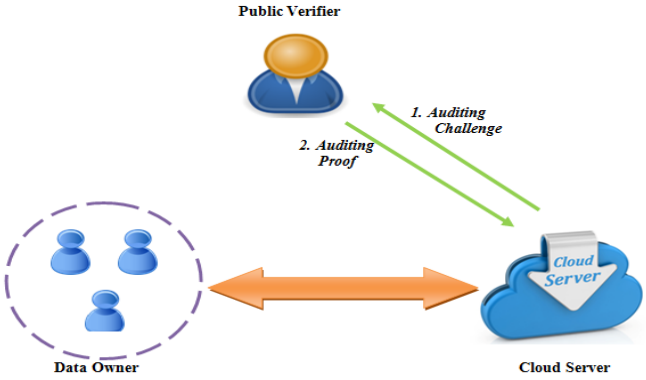

Figure1: Cloud Data Storage [7]

While considering data privacy, we cannot rely on traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with user's own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime to anyone. For example, organization may grant permission to access part of sensitive data to their employees. But challenging task is that how to share encrypted data. Traditional way is user can download the encrypted data from storage, decrypt that data and send it to share with others, but it loses the importance of cloud storage [7].

1.2 Cryptography
Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is

used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography [8].

1.3 Classification of Cryptography

Cryptography can be divided into three major category based on the use of key [9] [10].

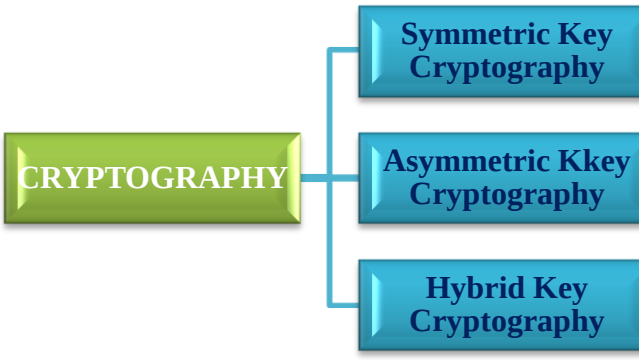

Figure 2: Cryptography Classification

a) **Symmetric Encryption (Private Key Encryption):** In this type of encryption same key is used at the time of encryption and decryption. The key distribution has to be made before the transmission of the information starts. The key plays a very important role in this type of encryption. Symmetric encryption is known as secret key or single key.

b) **Asymmetric Encryption (Public Key Encryption):** In this type of encryption different key is being used for encryption and decryption process. Two different key is generated at once and one key is distributed to other side before the transmission starts; Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver.

c) **Hybrid Encryption (Combination of private and public):** Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security.

2. LITERATURE SURVEY

Cloud computing faces many problems on integrity and privacy of user's data stored in the cloud. Hence it requires some secure and efficient methods which can ensure the integrity and privacy of data stored in the cloud.

Wang et al. [11] has proposed a privacy preserving public auditing protocol which makes use of an independent TPAto audit the data. It utilizes the public key based homomorphic linear authenticator (HLA) with random masking techniques. But this protocol is vulnerable to existential forgeries known as message attack from a malicious cloudserver and an outside attacker.

To overcome this problem, Wang et al. [12] proposed a new improved scheme which is more secure. It is a public auditing scheme with TPA, which performs data auditing on behalf of users. It uses HLA which is constructed from Boneh-Lynn Shacham short signature referred as BLS signatures. It also uses random masking for data hiding.

For the sake of data binding, this new scheme involves computationally intensive pairing operation thus making it inefficient to use. This proposed scheme has been implemented practically on Amazon EC2 instance which demonstrates the fast performance of the design on both the cloud and the auditor side. But the full-fledged implementation of this mechanism on commercial public cloud is not been tested. So it is difficult to expect it to robustly cope with very large scale data [13].

Arasu et al. [14] has proposed a method that uses the keyed Hash Message Authentication Code (HMAC) with homomorphic tokens to enhance the security of TPA. It is a technique for verifying the integrity of a data transmitted between two parties that agree on a shared secret key. HMAC's are based on a key that is shared between the two parties, if either party's key is compromised, it will be possible for an attacker to create fraud messages.

Adhav et al. [15] have introduced an attacking module which continuously keeps track on data alteration in the cloud. The attacking module is a small code which resides on cloud server. Confidentiality of stored data is achieved by encrypting the data using AES algorithm.

3. PROPOSED SYSTEM

3.1 Problem Domain

The cloud environment provides support for efficient computing and enables to provide the efficient computing and storage solutions at the remote end. In this presented work the main aim to address the following issues in the existing cloud storage:

Data security: The data is placed on the cloud which is not much secured due to third party access and treads therefore the data security in cloud storage is required

Data owner and client privacy management: The data owner and client in not distinguishable using the data additionally the privacy on such data is access is required.

3.2 Solution Domain

In order to provide end to end solution for the cloud storage the following solution steps are included.

Authentication Management: In authentication management the system and user attributes are recovered additionally the one time password is included to manage the secure authentication.

Cryptographic Data Security: In this phase the MD5 and AES based hybrid cryptographic algorithm is consumed for providing the security.

Providing The Search Solution Over The Encrypted Data: The keyword based search system is provided for identifying the user and their data during different data retrieval operations

3.3 Methodology

For the advancement of the current security scenario here we present a proposed PSDS scheme for ensure security and privacy enhancement of the system using figure 3.

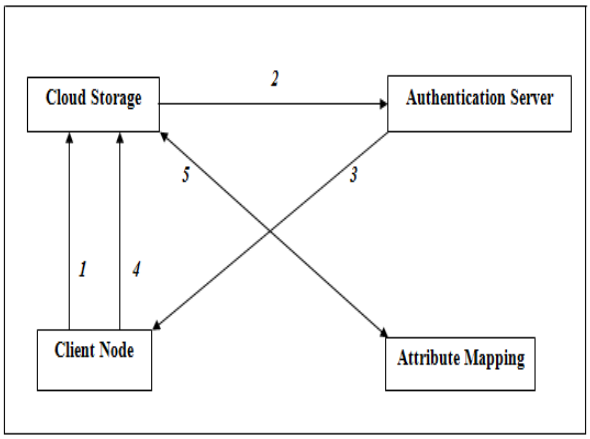

Figure 3: Security Management

According to the given figure the proposed security technique involve the following steps of authentication and data preserving technique.

a) Client node is an end client system who wants to store or retrieve the data from the secure server. In this step the end client initiate the authentication by making the request from the server.

b) In this phase the server system trigger the authentication server for finding the user credentials and data attributes and ask for the security questions, in this phase the OTP is applied to make secure the communication between client and server.

c) After authenticating the user access the system ask for user id, password and OTP again here the OTP works as the salt for the encryption and validation.

d) In this step user initiate the communication and data request from the server, during this the MD5 and AES algorithm is organized for encrypting the data additionally the following information is preserved into the attribute MAP. MAP data for finding the user targeted information from search space.

i. User ID
ii. Password
iii. Session key
iv. Text file features as frequent token
v. Original file name
vi. Mapped file name

4. PROPOSED ALGORITHM

This section introduces the summarized steps of the proposed encryption technique proposed for securing the data during network file exchange in untrusted environment.

Table 1: Proposed PSDS Algorithm

Input: Input Data (D)
Output: Security using AES; Original File (O)
Process:

1:D = readData

2:F = fileReadData (R)

3:K_{128}(32 charatcter) = MD5. crypt(userid, name, F)

4:stringKey = K_{128}AESenc (srcPath, destPath, K_{128})

5:*if* (key == randomeKey)

D = AESdec (srcPath, destPath, randomKey)

6:*retune O*

5. RESULT ANALYSIS

5.1 Encryption Execution Time

The amount of time required to perform encryption using the selected algorithm is termed as the encryption of the cryptosystem. The encryption time of the proposed system is demonstrated using figure 4.

$$Time\ consumption = Algo.End\ Time - Algo.Start\ Time$$

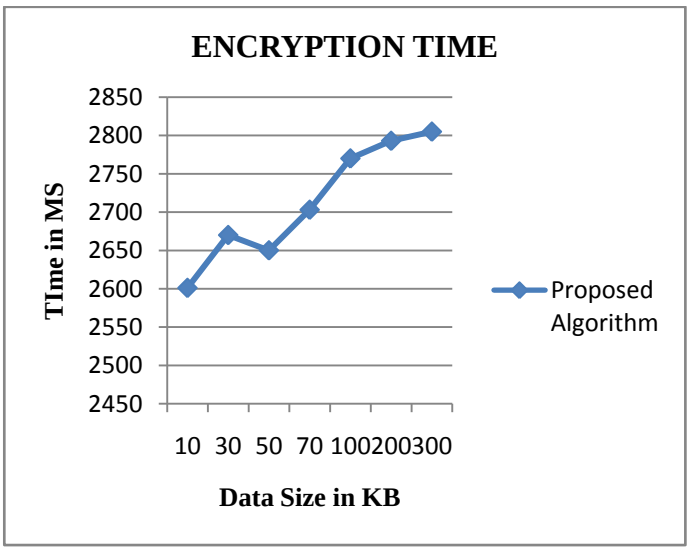

Figure 4: Encryption Time

In order to show the performance of implemented systems the encryption execution time is reported in figure 4. In this diagram the X axis shows the different file size on which different experiment values performed and the Y axis shows the amount of time consumed for processing the input file. Additionally the performance of proposed system is given using blue line. According to the given results the proposed system consumes less time. Additionally the results shows the amount of time consumed is depends on the amount of data provided for execution. Moreover, while using proposed PSDS, enhance the security for cloud storage publicly

5.2 Decryption Execution Time

The amount of time required to recover the original data from the cipher text is known as the decryption time of the algorithms. The figure 5 shows the obtained performance of the system in terms of millisecond. To show the performance of security system the blue line shows the performance of proposed algorithm. In given figure 5, x-axis shows the different file size on which different experiments values are

performed and the Y-axis shows the amount of time consumed. According to the observations the encryption time is higher than the decryption time in the system, but the decryption time of the proposed algorithm is much adoptable.

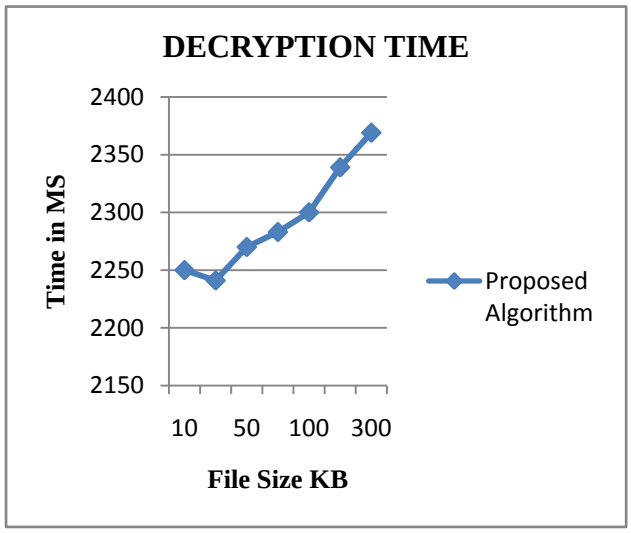

Figure 5: Decryption Execution Rime

5.3 Encryption Memory

The amount of main memory required to execute the algorithm with the input amount of data is known as the encryption memory. The total memory consumption of the algorithm is computed using the following formula.

$$Consumed\ Memory = Total\ Memory - Free\ Memory$$

The figure 6 shows the encryption memory consumption of the system. In this diagram the amount of main memory consumed is given in Y axis and the file size which are used for experiments are reported in X axis. According to the obtained results the proposed algorithm consumes fewer resources as we seen during the execution of algorithm.

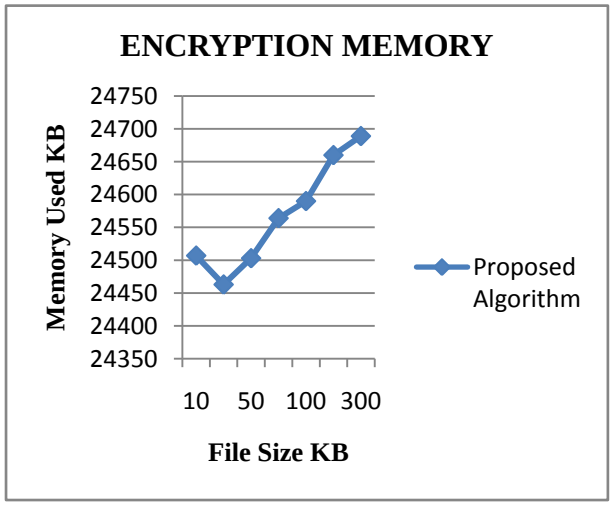

Figure 6: Encryption Memory

5.4 Decryption Memory

The amount of main memory required to recover the original file from the cipher text is known as the decryption memory consumption. The figure 7 shows the

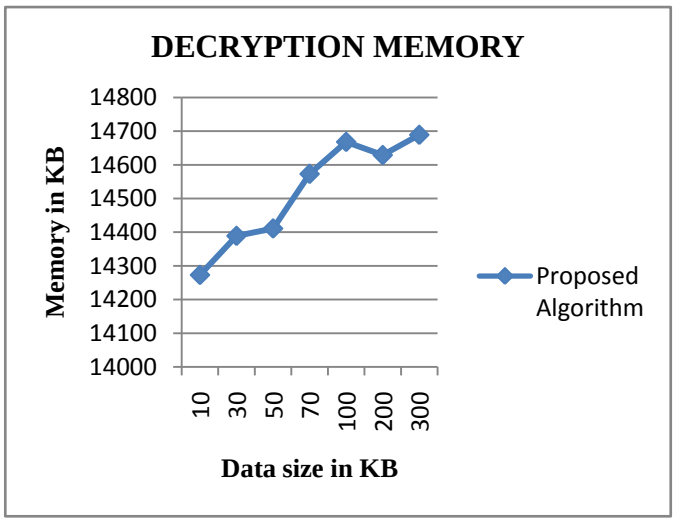

Figure 7: Decryption Memory

Amount of main memory consumed during the data recovery. In this diagram the X axis shows the different file size used for decryption and the Y axis shows the amount of main memory consumed during the decryption. According to the obtained results the amount of main memory used is less than of encryption memory and consume less space of proposed algorithm.

5.5 Encryption Response Time

The amount of time required to produce the outcome after making the request from the server is termed as the server response time. The computed response time of the proposed technique for cloud based secure communication is demonstrated using the figure 8. X-axis of this diagram contains the amount of experiments performed using the system and the Y axis shows the amount of time required for generating the response through the server. This can also term

as the communication overhead for the system. According to the computed results the response time is not depends on the amount of file size or other parameters. That is directly depends on the amount of work load on the target server where the data is stored or the application is hosted.

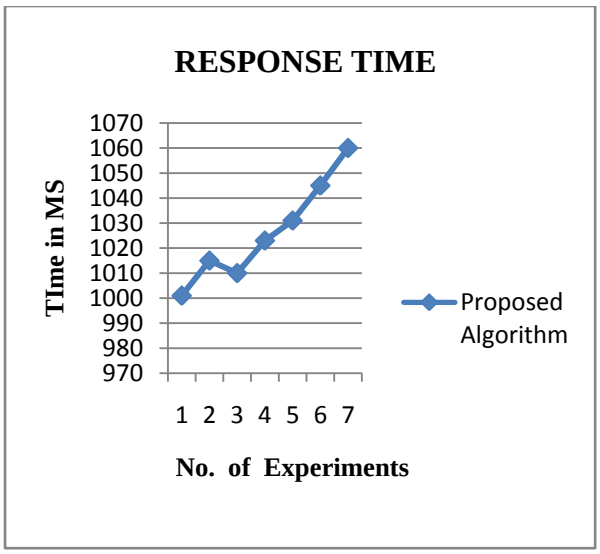

Figure 8: Response Time

5.6 Decryption Response Time

To get the original data via functioning of server and time to take all process in this system, so for downloading original file server responses some amount of time. This time is decryption response time. The calculated response time of the proposed algorithm for public cloud security is established using the figure 9. X-axis of this diagram contains the amount of runs performed using the system and the Y-axis shows the amount of time required for producing the response through the server. Giving to the calculated results the response time is not depends on the quantity of file size or other factors. That is directly depends on the total of work load on the target server where the data is stored or the application is hosted.

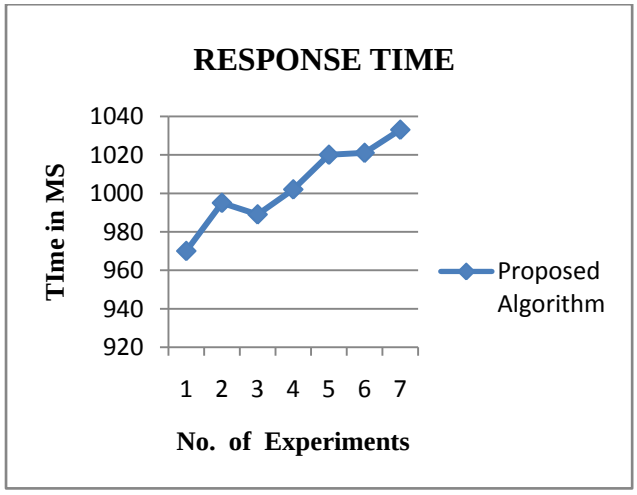

Figure 9: Response Time

6. CONCLUSION

Cloud data security is an important aspect for the client while using cloud services.The paper presents solution which offers user anonymity in authentication phase and confidentiality during file uploading and downloading for all users.We deal with user anonymous access to cloud services and shared storage servers. Our solution provides registered users with anonymous access to cloud services. In addition of that for preventing the unauthorized access to the system a strong user authentication technique using the normal credential and OTP is prepared. Furthermore for securing the data in storage and untrusted network an AES and MD5 based cryptographic technique is implemented. This technique also checks the communicated files integrity for finding the authenticity of the data transmission during the network file exchange.

7. REFERENCES

[1] Wang, Cong, et al. "Toward publicly auditable secure cloud data storage services." *IEEE network* 24.4 (2010): 19-24.

[2] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, PP. 1-6.

[3] C. Wang, K. Ren, S. Yu, K. Mahendra, and R. Urs, "Achieving Usable and Privacy-Assured Similarity Search over Outsourced Cloud Data," Proceeding IEEE INFOCOM, 2012.

[4] Cong Wang, Ning Cao and KuiRen, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 8, August 2012.

[5] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, "Towards Secure and Dependable Storage Services in CloudComputing," To appear, IEEE Transactions on Service Computing (TSC)

[6] Preeti Gulab Sonar and Pratibha Dattu Shinde, "A Novel Approach for Secure Group Sharing in Public Cloud Computing", International Journal of Computer Applications (IJCA), Volume 127 – No.11, October 2015.

[7] Omkar Patil, Ashish Tonde, Chinmay Sapkale and Smita Bansod, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing – A Survey", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2016.

[8] M. Kundalakesi, Sharmathi R and Akshaya.R, "Overview of Modern Cryptography", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6, PP. 350-353, 2015

[9] Mohammed AbuTaha, MousaFarajallah and Radwan Tahboub, "Survey Paper: Cryptography is the Science of Information Security", International Journal of Computer Science and Security (IJCSS), PP. 298- 309, Volume (5), 2011.

[10] PrakashKuppuswamy, and Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", MIS Review: An International Journal, Volume 19, No. 2, PP. 1-13, March 2014.

[11] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,"Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", in INFOCOM, 2010 Proceedings IEEE, PP. 1–9, 2010.

[12] Cong Wang, Sherman SM Chow, and Wenjing Lou, Privacy Preserving Public Auditing for Secure Cloud Storage,http://eprint.iacr.org/2009/579.pdf

[13] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou, Privacy Preserving Public Auditing for Secure Cloud Storage, Computers, IEEE Transactions on, 62(2), PP. 362–375, 2013.

[14] S Ezhil Arasu, B Gowri, and S Ananthi. Privacy-Preserving Public Auditing in cloud using HMAC Algorithm, International Journal of Recent Technology and Engineering (IJRTE), 2013.

[15] Jadhav Santosh and B.R nandwalkar, Privacy Preserving and Batch auditing in Secure Cloud Data Storage using AES, Proceedings of 13th IRF International Conference, 2014