A Matrix Based Encryption with Advance Hashing Scheme Over Cloud

Rashi Mehra[*1] Ravindra Patel[*2], Varsha Sharma[#3]

Rajeev Gandhi Prodyogiki Vishwvidhyalaya, RGPV, Bhopal, India

Abstract: **Cloud environment is an important platform today in IT industry. It deals with several industry aspect and data storage for the information access. Security is always an concern along with the data usage and proper storage using hashing technique in cloud data center. Integrity verification helps in detecting authenticity of data. Various techniques for the security protocol is proposed such as RSA, AES, Blow fish, ECC and many other approach for security encryption. Hashing technique such as MD4, MD5 and other SHA signature were also proposed to verify the data integrity. Existing paper used ECC for the security along with key generation, verification approach with group key management. In this paper our discussion is performed the work derived in existing approach as well as the limitation may associate with the existing paper work. Our proposed algorithm makes use of new encryption technique which is matrix based transmission. Our approach also use efficient group key management and file sharing for the multiple group level file sharing in industry. An advance hashing scheme SHA-2 is integrated in the system for data integrity verification. Our Experiment performed with Java Apache 2 with Data center storage which proves the efficiency of proposed work in terms of computation time, computation cost and overall performance using proposed technique.**

Keywords**: Matrix based Encryption, group sharing, cloud storage, Hashing technique, ECC algorithm.**

I. INTRODUCTION

Cloud computing is a platform where different kind of on-demand pay per use services are driven by the multiple organization. There are different cloud levels which provide different service as per their capacity. These are IaaS [5], PaaS , SaaS are the different model services type which provided by cloud provider. According to IaaS infrastructure by the major industry is provided while platform as a service provide the efficiency of individual or group of platform for user availability. SaaS which is Software as a service gives the advantage of application for the user interest and make it available in public use.

Cloud can be public, private, hybrid or community based and according to requirement of cloud it can be utilized.

Here is few required concern which need to deal with and further be proposed for the computation requirement.

Cryptography serves the following goals of security:-

- **Confidentiality:** Confidentiality means the information is known to the sender and the intended receiver only. It is unknown to the other persons. Only authorized person is able to access the information.
- **Authentication:** Authentication specifies identity of the sender of the information whether the sender is authorized or not.
- **Integrity [7]:** Integrity means the message has not been modified before reaching to the intended receiver. The contents of message cannot be altered by another person.
- **Non Repudiation:** When the message is sent by the sender it cannot refute that message has not been sent. In a similar way, the message cannot be denied by the receiver that has not been received.
- **Access Control [6]:** It specifies that what could be accessed by an authorized person.
- **Availability:** It specifies that the authorized parties will have availability of resources all the time.

II. RELATED WORK

Existing work make use of algorithm which is ECC elliptic curve cryptography along with SHA-1 hashing for the integrity verification. A combination is of recent encryption technique for data security storage and further hashing function technique SHA-1 is using for the dynamic integrity verification process. Our proposed system also used ECC [3] algorithm for the data security and data processing for the upload over the cloud server and simulation performance. Previous hashing technique and other integrity verification such as Panda [1] is also been derived in the past algorithm approach.

SHA-1 contains the key length of 128 bit [4] which is not breakable with the brute force attack system which is the key main point of the hashing scheme, also the MAC security provided in case of encryption where the highest number of security is being transformed. Recent work aims to provide a high security combination approach while dealing with the cloud security approach, as the general method either work with the security encryption or hashing data verification technique. Thus our proposed work implied which work on both the area as a algorithm where the data hash value is calculated at the time of implementing encryption and data storage performance into the cloud data center.

III. PROBLEM IDENTIFICATION

As per the literature survey is performed with different techniques and different results from the algorithms were monitored and other different technique for data processing, security approach over data store[8,9].

Upon verifying different scenario and the available technique different short comes with the Existing algorithm ECC-SHA1 with file key generation which is taken as base for our research work.

The following are the monitored points which identified as problem and further analyzed and performed further with enhancements.

1. Previous ECC Approach makes it less effective while implementing and applying in real scenario.
2. Implementation of equation computation, determining point requirement of ECC is difficult process which increases complexity of system.
3. SHA-1 introduce low avalanche effect , which may be problem while working with large number of data inputs.
4. Previous algorithm takes an advantage of asymmetric encryption technique which is used by base paper, but still when we talk about the multiple tenant, multiple ownership and multiple user over the data. Thus a security of key sharing is still a challenging issue which is faced by authors.

IV. PROPOSED METHODOLOGY

As per our observation about the previous technique and their disadvantage in different terms and scenario‘s. Our work present a new approach matrix based [10] which is highly secure and consumes low computational time and thus computational cost over the large number of structured available dataset.

Our work propose a new algorithm, Enhanced Dynamic matrix based encryption along with SHA-2 hashing scheme is proposed in the system which make it effective presentation of our proposed work. Our algorithm also checks for proper access control using more secure and reliable parameters.

The proposed algorithm is described below:

1. Loading of the complete data file inputs , file reading and storing into the binary format in temporary data store.
2. Creating an object of all required component.

   Cloud object creation:

   VM – virtual machine creation requirement
   DC- local Data server is configured with WAMP 2.35.
3. Perform communication in between UB-user base with data binary format and data store using a secure algorithm using dynamic matrix operation.
4. Perform encryption using effective matrix input and processing [11] over the symmetric key approach.
5. Perform encrypted data transmission over the DC and storage in the scenario.
6. Monitoring integrity verification over the data store and producing the output value of matching.
7. Finding the execution time as per formulae-

   Execution time = final completion time- initial time;
8. Observing the execution time and thus it effect computational cost for the complete transmission.
9. Exit .

Algorithm Psudo Code :

Dynamic Matrix SHA-2 Approach:
Input: File f, Data centre DS, Matrix init, Plain text, Key.
Output: Matrix process, Cipher text, Computation time.
Steps:

```
Load Matrix initials;
For Each file(i-n)
{
File Load inputs();
Binary conversion();
Data updating matrix();
Transpose creation for matrix();
Cipher Text Return();
}
Send VerReq(FileID);
Sha2= SHA2(CipherText);
ProofGen(sha2);
If(Match==true)
{
File verified return 1;
}
Else
{
Return 0;
}
Group key sharing();
File access();
Return Computation time;
}
End.
```

V. EXPERIMENTAL & RESULT ANALYSIS

In this section detail about the implementation and results is presented. Java language over NETBEANS IDE simulator is used to implement the proposed methods and a comparison of result with the existing technique is presented using RAM 8 GB, 2 TB HDD and standard apache server with MYSQL as database for storage and accessing purpose.

Performance Measures

Computation Time: A training time of a dataset in Java is computed with the help of start and end time class variables defined in the tool.

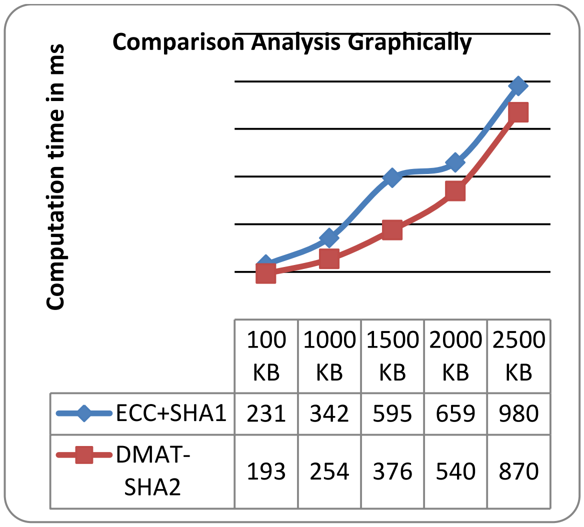
In result analysis computation several files and user were taken where the consideration of data sharing with different file size is performed. Computation time and cost is observed with tabular and graphically[12]. The Results presented shows the effectiveness of proposed algorithm over existing ECC and SHA-1 technique.

The proposed and existing technique is performed with the above different data size file, where the data is processed and following output results were monitored:

Table 1: Computation time and cost analysis with techniques.

Technique Approach File size / Computation time in ms	**Existing technique (Computation time in ms) ECC+SHA-1**	**Proposed Technique (Computation time in ms) DMAT-SHA2**
100 KB	231 ms	193 ms
1000 KB	342 ms	254 ms
1500 KB	545 ms	476 ms
2000 KB	659 ms	540 ms
2500 KB	980 ms	870 ms

In the table 1 above, it is demonstrated that the proposed technique is effective while comparing with ECC encryption process.



	100 KB	1000 KB	1500 KB	2000 KB	2500 KB
ECC+SHA1	231	342	595	659	980
DMAT-SHA2	193	254	376	540	870

Figure 2: Comparison Line graph for Technique analysis

In the figure 2 above a graphical analysis of proposed and existing approach is shown. Using the graph it clearly understands the effectiveness of proposed algorithm.

Working on Dynamic matrix encryption algorithm such as our proposed technique authentication will be efficient and easy to visualize and in order to make it easier for user to use, such security technique will be efficient to use.

VI. CONCLUSION & FUTURE WORK

Cloud computing playing a vital role in industry for file sharing, data storage and effective grouping of data for sharing and managing purpose. Different approaches were proposed in past for effective security and integrity verification. In this paper Dynamic matrix based encryption technique for the data security storage purpose is used. Further SHA-2 hashing scheme with dynamic group key sharing is implemented. Data storage security and verification make use of advance security terms. Experiment using Apache framework is performed with standard server configuration. Experiment parameter performances were taken as computation time, cost and overall efficiency which proves the effectiveness of our algorithm over the existing ECC and SHA-1 hashing scheme.

Future Work

As the proposed work computes the efficiency using proposed matrix approach with SHA-2, group key sharing concept make it affectivity. A further real time implementation with application is left for future work. A further cryptanalysis can be done with proposed security algorithm and architecture.

REFERENCES

[1]. "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, VOL. X, NO. X, XXXX 2014, accepted.

[2]. Shaohua Tang, Xiaoyu Li, Xinyi Huang, Yang Xiang, and Lingling Xu," Achieving Simple, Secure and Efficient Hierarchical Access Control in Cloud Computing", IEEE 2016.

[3]. Y.-L. Lin and C.-L. Hsu, "Secure key management scheme for dynamic hierarchical access control based on ECC," J. Syst. Softw., vol. 84, no. 4, pp. 679–685, 2011.

[4]. https://www.tbs-certificates.co.uk/FAQ/en/sha256.html

[5]. Tiantian LIU, Tongkai JI, Qiang YUE, Zhenchu TANG "G-Cloud: A Highly Reliable and Secure IaaS Platform" IEEE, 2015.

[6]. Kadam Prasad,Jadhav Poonam,Khupase Gauri, N. C. Thoutam "Data Sharing Security and Privacy Preservation in Cloud Computing" IEEE, 2015.

[7]. N. Shanmugakani, R. Chinna "An Explicit Integrity Verification Scheme for cloud Distributed systems" ICSO, IEEE, 2015.

Nivedita Simbre, Priya Deshpandey "Enhancing Distributed Data Storage security for cloud computing using TPA and AES algorithm" IEEE, 2015.

[8]. Naithik Shah, NisargDesai,ViralVashi," Efficient Cryptography for Data Security",2014 International Conference on Computing for Sustainable Global Development (INDIACom).

[9]. M. Yamuna, S. Ravi Rohith, Pramodh Mazumdar, Avani Gupta "Text Encryption Using Matrices ", International Journal of Application or Innovation in Engineering & Management (IJAIEM)Volume 2, Issue 3, March 2013.

[10]. Devendra Prasad,Govind Prasad Arya, Chirag Chaudhary, Vipin Kumar, "A Text Encryption and Decryption Technique Using Substitution-Transposition and Basic Arithmetic and Logic Operation ",International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014.

[11]. Udepal Singh, UpasnaGarg," An ASCII value based text data encryption System", International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013 1 ISSN 2250-3153.