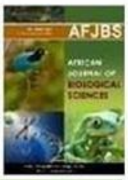
https://doi.org/10.48047/AFJBS.6.Si3.2024.1204-1211

AFJBS

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com



Research Paper Open Access

Enhancing Public Cloud Security: A Novel Model for Strong Confidentiality and Authentication

Kuber Datt Gautam[1], Chhaya Moghe[2], Shimna Mohan.K[3]

1. Assistant Professor, Department of Computer Application Medi-Caps University Indore.

2. Assistant Professor, Department of Computer Application Medi-Caps University Indore.

3. Assistant Professor, Department of Computer Application Medi-Caps University Indore.

Volume:6,IssueSi3,2024
Received:20May2024
Accepted:11june2024
Doi:10.48047/AFJBS.6Si3.2024.1204-1211

ABSTRACT

The invention of cloud computing is relatively recent, providing significant potential without the need for costly hardware or software upgrades. It enhances resource sharing across hardware, software, and platforms, reducing overall system costs. Due to its widespread adoption and practical benefits, cloud computing has become indispensable in the modern business environment. However, its popularity and reliance on third parties make it an attractive target for cybercriminals. Security is crucial for service providers to build customer trust and maintain a positive brand image. The affordability and efficient infrastructure sharing of cloud computing are driving more large enterprises to migrate their services to the cloud. Prioritizing safety is essential due to the vast amount of remotely stored data and third-party involvement. This study examines various security algorithms' ability to protect sensitive data with minimal resource consumption, focusing on data integrity. ECC and RC6 are evaluated as alternatives to ECC + RC6 and MD5. The research proposes an enhanced security system based on the ECC and RC6 algorithms and the Rolebased Access Control Model. A public cloud application developed with Java technology validates the proposed approach, and its computation time for different file sizes and formats is analyzed.

Keywords: ECC, RC6, Hybrid Model, Cloud Computing, MD5

I. INTRODUCTION

Virtualization, web services, and SLA are just a few of the many technologies that are combined in a way that epitomises cloud computing. Server virtualization, web services, and SLAs are just a few examples of the numerous technologies that are all included in the concept of cloud computing. Several cloud services are required for network connectivity by enterprises, the military, and the government in order to provide high-quality services. On-demand, scalable, and affordable software, platform, and underlying infrastructure service delivery is an example of cloud computing. All people have access to cloud services.Using a network of distant servers to store and process data is referred to as "cloud computing," and it is a type of computing. It serves as a central store for data that is accessible online at any time and from any location. Cloud-based apps can get the resources they need through the cloud. Parallel, virtual, distributed, and cloud computing all work together. Instant access to a multitude of resources is made simple and effective via the cloud. With a browser that offers access to them, you can access these resources and services. Several cloud models necessitate specialized services because of the nature of the cloud architecture. The most practical way to communicate with any hardware component or developer in the ecosystem is through the cloud. Service delivery that is quick and easy is made possible by the cloud. The businesses in charge of data transportation are cloud providers. Virtualized OSes may have instant access to cloud information. A data center, which each cloud has, is where all the information kept in a cloud is kept. A data center is full of information that is dispersed everywhere. The most well-known cloud service providers include Amazon Web Services, Apache Hadoop, and Google Drive.

II. PROBLEM DOMAIN

Any project that involves sensitive information must include setting up a security parameter. When that shouldn't be broadly disseminated. Trust problems may arise when a supplier divulges information to a user. The user has little faith in the possibly dishonest third-party vendor.

Authentication and authorization problems must be resolved in order to guarantee that only people with permission can access information. Users who participate in unlawful conduct are treated as prospective hostile attackers or intruders who need to be tracked down, stored, and analyzed for future security needs.

The algorithms of the original system were mainly concerned with confidentiality, integrity, or authentication. Along with the others, this level of security has never been accomplished before. [1] Proposes creating a hybrid cryptography system by fusing the RSA and AES algorithms. Even though the AES technique requires more work than other symmetric key algorithms, it is frequently employed by researchers for primary encryption. Nonetheless, RSA is less secure than ECC. Another problem with [1] is that honesty and integrity are lacking. To solve these issues, the proposed study employs the best data security measures for web applications. The suggested approach will be the most effective and efficient way to safeguard sensitive data in web applications. The user is guaranteed to receive content that is secure and unique, as well as authorized access and privacy during the uploading and downloading processes, by adopting the suggested effort into the current paradigm. The goal of the whole project is to accomplish the subsequent way:First, the ECC and RC6 algorithms are used for encryption. Second, figuring out and resolving problems that emerged during the course of the previous task. To speed up the encryption process, third, divide the data into more manageable portions. Fourth, the MD5 algorithm safeguards data integrity.An altered version of Kerberos should be used for authentication,

3. METHODOLOGY

The integrity of the system is now at risk due to a hacker attack that just started. Online apps have long recognized the value of both internal and external security when it comes to safeguarding sensitive data because they can operate on any platform with any software, web applications are the only ones that can provide cross-platform capability... Encryption is an excellent approach to protect sensitive information, but when dealing with large datasets, it can considerably raise the processing and storage requirements of web services. Successful online applications require quick computation, which can only be accomplished with little processing overhead. The RC6 security technique, which outperforms AES and ECC in terms of speed and security, has replaced the AES method. The ECC technique can offer the same level of security as RSA with a big enough modulus and key. The Kerberos protocol was changed to integrate MD5 for input verification in order to do this.

Theory of Research

If you need a secure way to encrypt and decrypt sensitive data, this method is excellent. The web application's resources cannot be accessed without first requiring client authentication via a customized Kerberos protocol. As soon as the authentication server has verified the client's credentials, the resource server will give access. Customers' information is encrypted with ECC and decrypted with RC6. The data's validity is further ensured by the use of the MD5 algorithm.

The overall logic of the architecture is shown in the following figure:

We opt for the fundamental text because:

For the reader's convenience, the information has been divided into sections.

The substances C3 and C4.

The pieces are arranged in alternating-size pairs and sets.

Even sections are encrypted using ECC, and odd parts are encrypted using RC6.

The plain text was then encrypted to create cypher text as the last stage.

The complete project process is shown in the block diagram that follows.

A customized version of Kerberos is used to validate the user's credentials as soon as they are entered by the user. The user will be correctly forwarded to the desired homepage if their login credentials are legitimate. Information in the ongoing investigation is verified using this process. Instead of the two servers needed by the Kerberos 5 protocol, we use the Authentication Server to perform authentication and create tokens.

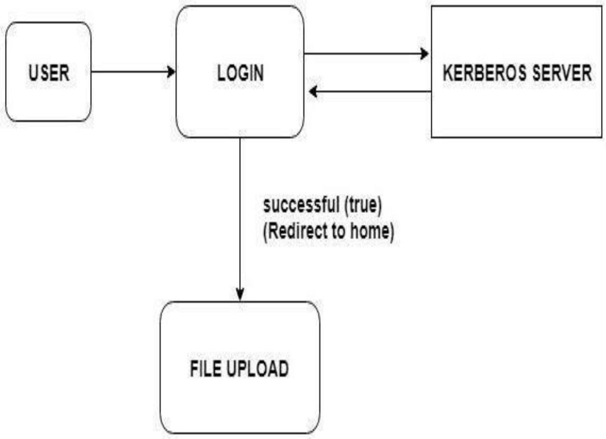


Figure 1: Block diagram of Authentication Model.

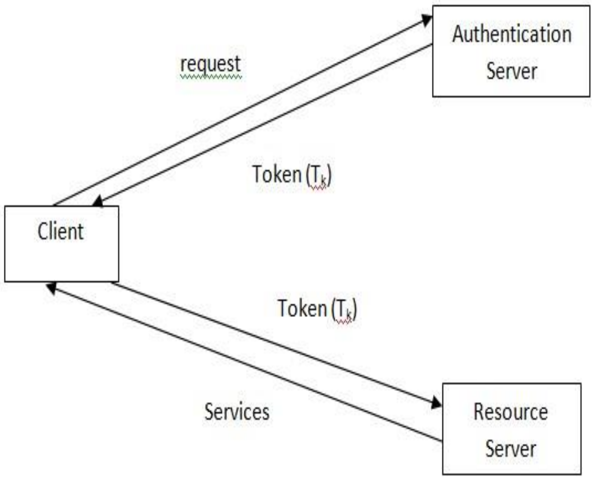


Figure 2: Upgraded version of Kerberos

The suggested authentication measures are as follows:

Here are some tips for checking the details of your account:

Before using the server's resources, the client must first log in to the authentication server using their email address and password.

An RC6-encrypted token (ETK) is created and given to the user after the client has been authenticated by the authentication server.

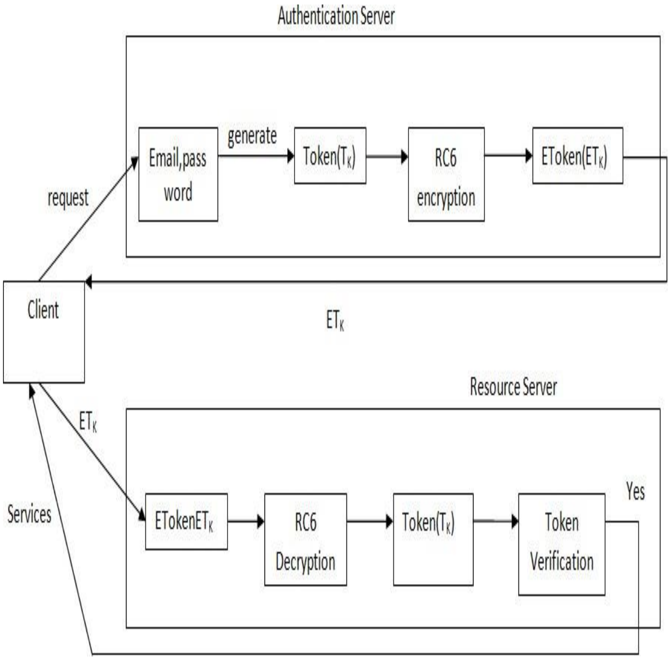
The Client then utilises the ETK to submit a service request to the resource server.

Before the token (TK) is checked for validity, the resource server decrypts the token (ETK) that the client has submitted.

If the token (TK) has not yet expired, forget about using it for that service; if the resource server doesn't start providing those services, the token (TK) will be thrown away. Terminated.

Figure 3: Detailed Authentication Protocol Architecture.

Integrity calculation Model:



The file is being uploaded while MD5 generation 256 bit encryption is applied to it. During this procedure, the file's integrity is examined. It will examine the file's uniqueness.

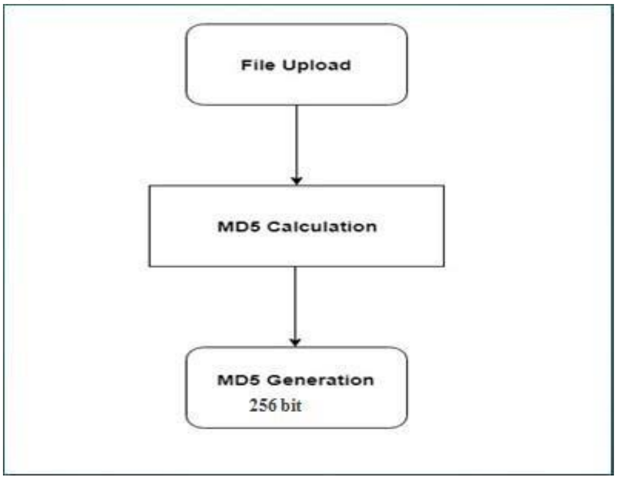
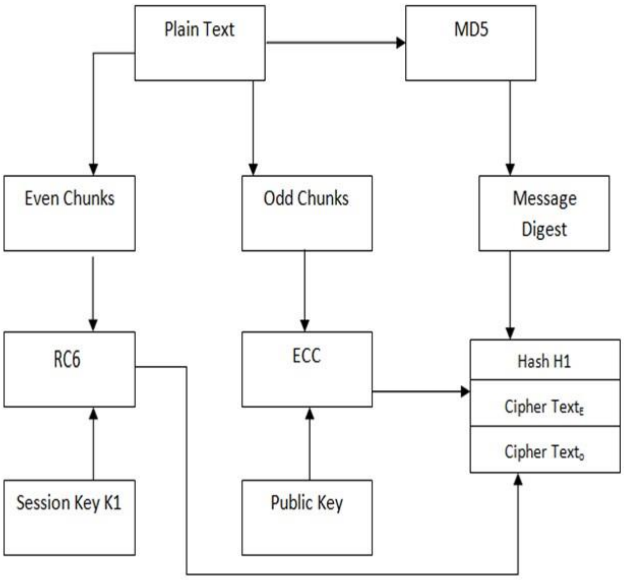


Figure 4: Block diagram of Integrity Calculation.

A file's secrecy status can be determined by encrypting and decrypting it. 3.4.2 The Algorithm for Exchanging Keys: The first step in any encryption procedure is to read in an input file, which is then divided into several blocks (C1, C2,... Cn). Even and odd pieces are sorted separately. Next, we encrypt everything, including bits of even and odd sizes. using theECC algorithm and RC6 algorithm, respectively, and the cipher chunks aregenerated.



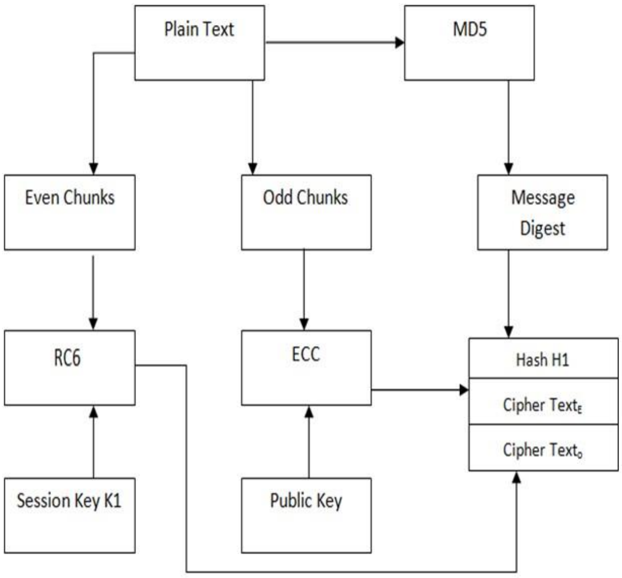


Figure 5: Block diagram of Encryption Architecture.

Decryption Model:

An algorithm to identify even and odd pieces of ciphered data after it has been decrypted. All even chunks are encrypted with ECC and all odd chunks using RC6 are encrypted with ECC. To finish the file, each of these sections is rebuilt.

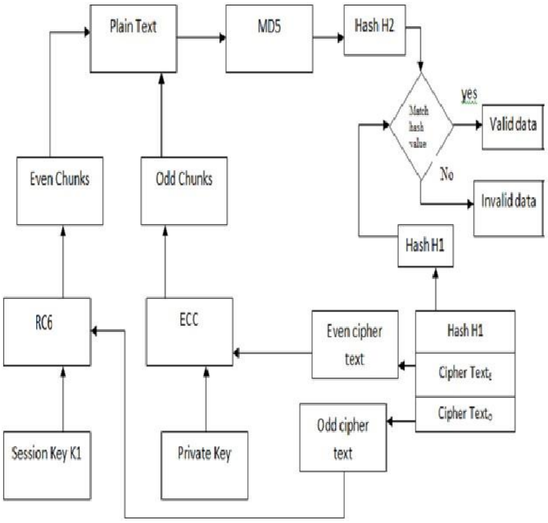


Figure 6: Block diagram of Decryption Architecture

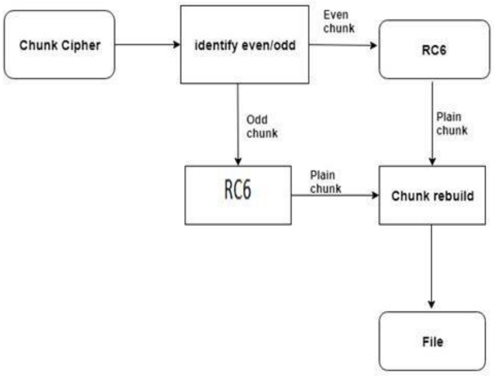


Figure 7: Decryption Model

Integrity Comparison Model:

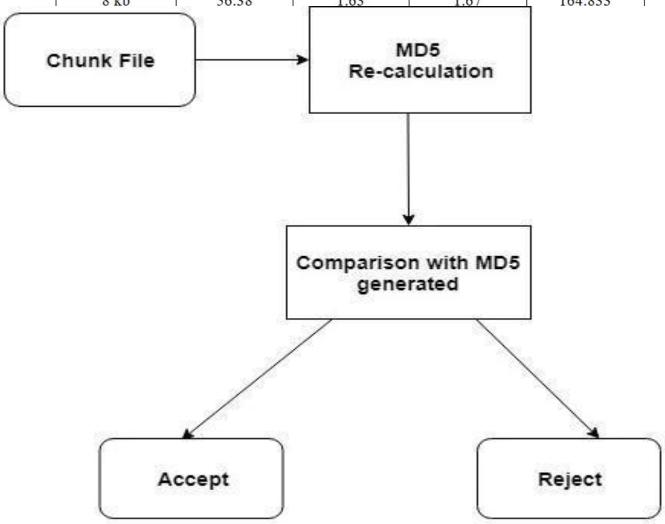
MD5 is used to recalculate the integrity of the chunk file. A comparison will be made between the recalculated file Hash 2 and the original calculation, and if the results match, the file is approved and not denied.

Figure 8: Block diagram of Integrity Check.

4. Experimental Analysis

For web-based programmer, the proposed hybrid model offers authentication and data integrity. It provides a quicker option than the present method for encrypting and decrypting data. We use the RC6 and ECC algorithms to achieve this. The suggested hybrid algorithm is evaluated in terms of the speed at which a text can be encrypted and decrypted, as well as the efficiency of the proposed hybrid method. The file size determines the processing time. The traditional techniques now in use are contrasted with the suggested hybrid algorithm.

Size of plain text(kilobytes)	ECC Time ms	RC6 Time ms	Message Digest Time ms	Total Time Ms
2 kb	19.25	0.37	2.216	30.23
4 kb	45	1.5	3.10	72.20
6 kb	52	1.65	2.35	125.56
8 kb	56.38	1.63	1.67	164.833



4.1 Encryption Time

The encryption time is the length of time it takes for the algorithm to convert plain text into cypher text. .Table1 Total Encryption Time taken by the proposed algorithm

Figure9: Encryption Time

4.2 Decryption Time:

The decryption time is the time taken by the algorithm to produce the plain text from the cipher text. Similar to the encryption time process, the decryption process follows. It is represented in tabular form in table 2 and its graphical form is shown in figure 10.

Table 2 Total Decryption Time taken by the proposed algorithm

Size of plain text(kilobytes)	ECC Time ms	RC6 Time ms	Message Digest Time ms	Total Time ms
2 kb	22.25	0.39	2.36	32.36
4 kb	34	1.69	2.45	89.65
6 kb	49	1.98	2.36	136.23
8 kb	64.25	1.85	2.35	175.25
10 kb	69.58	4.23	3.35	215.23

above table 1. In Figure 9 it is represented in graphical form to show a statistical view.

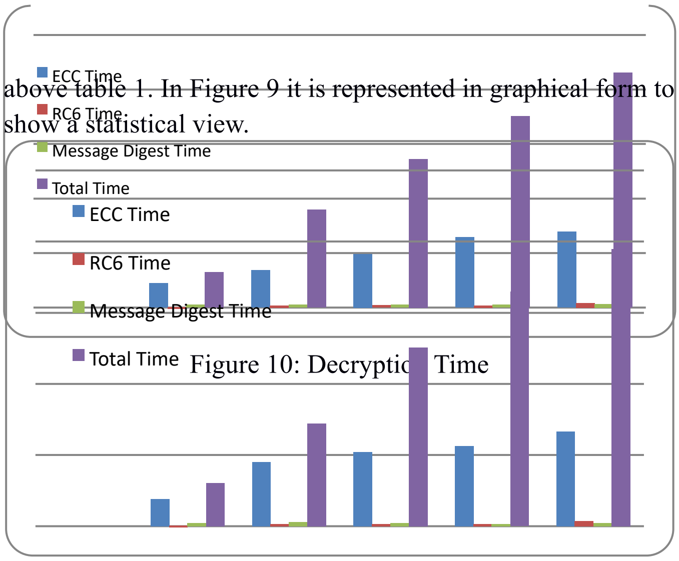
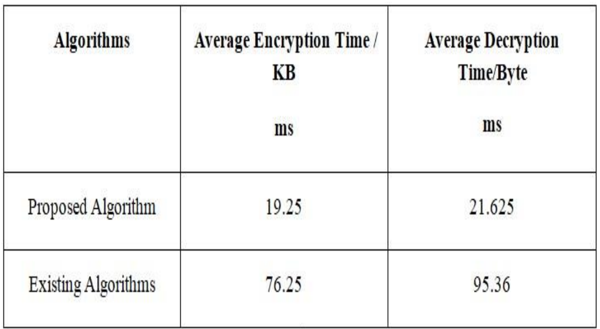


Figure 10: Decryptic Time

Comparison Work:

Comparison of time required in proposed work and existing work to encrypt and decrypt the file is shown here. Algorithms used in proposed work is compared with algorithms used in existing work (HCA + THCA) is shown in tabular form in Table 5.3 and represented in the form of a graph in Figure 5.3.Table5.3 Comparison Table of Encryption/Decryption Time of the proposed algorithm with existing algorithms



Algorithms	Average Encryption Time / KB ms	Average Decryption Time/Byte ms
Proposed Algorithm	19.25	21.625
Existing Algorithms	76.25	95.36

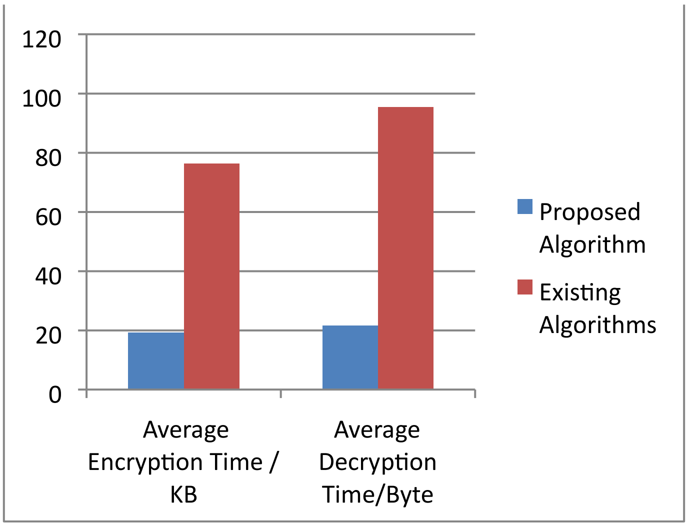


Figure5.3: Comparison Graph of Encryption/Decryption Time of the proposed algorithm with existing algorithms

Experimental Analysis of the complete work is described in this section where tables and graphs are plotted to represent the output in statistical form.

5. Conclusion & Future Work

Businesses will be affected by increased Internet usage and automation in conventional sectors. When it comes to running a company these days, many people are shifting their focus to the internet rather of relying only on a brick-and-mortar location. Web applications may help businesses save money, boost productivity, and modernise their procedures. Personal information of customers who use internet applications is always at risk of being accessed by other parties. The existing security paradigm is expected to undergo a transformation that would improve security.

The proposed hybrid paradigm aims to provide authentication, confidentiality, and integrity to safeguard data from unauthorised access in online applications. According to the hybrid approach, both ECC (distribution of the key's value) and symmetric key encryption (simpler and faster computation) may be used to assure confidentiality. Hybrid models for securing data in web applications are the best and quickest technique for doing so.

Future Work

During implementation, we discover that encrypted data is larger than plain text. Encryption and decryption times may be reduced in the future without sacrificing the volume of encrypted data. To apply the hybrid technique to files other than.txt files, such as.mp4 or.doc, would be an option. Military applications, security-conscious hardware and software makers, major websites with enormous databases, mobile apps, and cloud-based applications may all make use of it in the future, as may many other niche markets.

6. REFERENCES

[1] C AkshitaBhandari, Ashutosh Gupta, Debasis D, “A framework for Data Security and Storage in Cloud Computing”, International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016, pp. 1-7.

[2] Arora, Rachna, AnshuParashar, “Secure user data in cloud computing using encryption algorithms”, International Journal of Engineering Research and Applications, Vol. 3, pp.19221926, 2013.

[3] Wang, Cong, “Privacy-preserving public auditing for secure cloud storage”, Computers, IEEE Transactions on Vol 62.2, pp 362-375, 2013.

[4] B. Shereek, “Improve Cloud Computing Security Using RSA Encryption WithFermats Little Theorem”, IOSR Journal of Engineering, vol. 4, no. 2, pp. 01-08, 2014.

[5] B. Samanthula,Y. Elmehdwi, G. Howser and S. Madria, “A secure data sharing and query processing framework via federation of cloud computing”, Information Systems, vol. 48, pp. 196-212, 2015.

[6] Jin-Mook Kim and Jeong-Kyung Moon,”Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments” published in International Journal of Distributed Sensor Networks by Hindwai Publication Corporation. Volume-1, 2014.

[7] MrudulaSarvabhatla, Chandra Mouli Reddy M, Chandra SekharVorugunti, “A Secure and Light Weight Authentication Service in Hadoop using One Time Pad”, “2nd International Symposium on Big Data and Cloud Computing (ISBCC’15)”, Procedia Computer Science 50 (2015) 81 – 86. [8]

TumpeMoyo, and JagdevBhogal, “Investigating Security Issues in Cloud Computing. IEEE Eighth International Conference on Complex”, Intelligent and Software Intensive Systems, 2014.

[9]. NasrinKhanezaei, ZurinaMohdHanapi, “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services”, System, Process and Control (ICSPC), 2014.

[10] Deyan Chen; Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647-651, 23-25 March 2012.

[11] C. Y. Chen and J. F. Tu2, “A Novel Cloud Computing Algorithm of Security and Privacy”, Hindawi Publishing Corporation: Mathematical Problems in Engineering, 2013.

[12] G. L. Prakash, M. Prateek and I. Singh, “Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System”, International Journal Of Engineering And Computer Science, vol. 3, issue 4, pp. 52155223, April 2014.

[13] ChorB,GilboaN,Naor M, “Private Information Retrieval by Keywords”, Report 98-03, Theory of Cryptography
Library, 1998.

[14] D. Zissis and D. Lekkas, “Addressing cloud computing security issues”, Elsevier Journal of Future Generation Computer Systems, vol. 28, pp. 583592, 2012.

[15] F. F. Moghaddam, M. T. Alrashdan and O. Karimi, “A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments”, Journal of Advances in Computer Network, vol. 1, No. 3, Sep. 2013.