Design & Implementation of Enhanced Security Architecture to Improve Performance of Cloud Computing

D.O.I - 10.51201/Jusst12655

http://doi.org/10.51201/Jusst12655

Anil Gupta
Research Scholar
CSE Department
Mewar University,
Chittorgarh, Raj, India.

Dr. Meghna Dubey
Professor
CSE Department
Mewar University,
Chittorgarh, Raj, India

Dr. Durgesh Kumar Mishra
Professor
CSE Department,
Sri Aurobindo Institute of Technology,
Indore, MP India,

***Abstract*— Cloud computing offers various features such as creates, configure and customize application online. User can access applications over the Internet and they can also access database via Internet. Open nature and public access make their application vulnerable for several security attacks. This paper attempt to integrated different previously defined security approaches to propose a new and novel model of security. Here, proposed solution approach to improve performance of confidentiality, authentication, integrity and access control with better and strong way. Proposed solution is implemented using java technology and evaluated based on computation time and memory consumption. A detailed comparison with graph is also demonstrated in experimental analysis section.**

Keywords—Cloud computing, cloud security, confidentiality, cryptographic technique

1. INTRODUCTION

Cloud security consists of a set of policies, controls, procedures and technologies. These all are work together to protect cloud-based system. These securities also protect customer's privacy. Data security is a major concern in the cloud because all data is transmitted via the Internet. The data must be stored in an encrypted form in the cloud. This constrains the client form directly accessing the shared data. For this reason, it is appropriate to employ proxy and brokerage services. Encryption helps protect the data transferred and the data stored in the cloud as well. Encryption also helps protect data from unauthorized access but does not prevent loss of data.

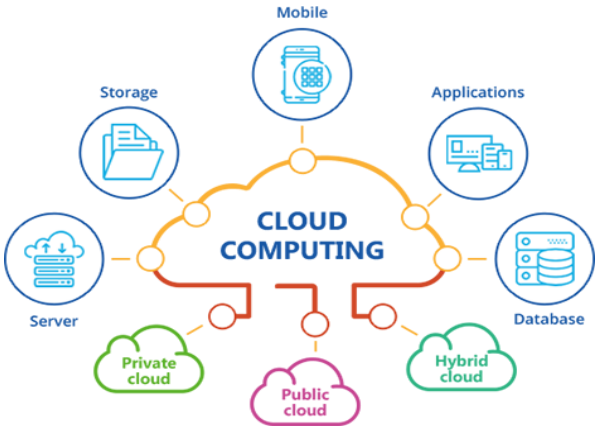

Figure 1: Cloud computing

In security planning, there is a need to evaluate different aspects of resources before deploying a specific resource to the cloud which are as follows:

- *Pick tool that needs moving into the cloud and investigate its chance of vulnerability.*
- *The cloud service models i.e. IaaS, PaaS, and SaaS need to be considered at different service levels for security.*
- *We also need to understand the types of cloud, i.e. public, private, community, hybrid.*
- *The risk generally depends on the types of software and service models in a cloud implementation.*

Cryptographic security mechanisms available for the cloud computing environment are as discussed below:

- **Encryption:** It is a technique of using cryptography and steganography to provide the security to the data. It is generally targeting the data integrity. The data is encrypted and hidden in some other data so that it seems to be noise to the unauthorized user.
- **Digital signature:** It is a technique where the data is kept secured through a specific digital key which is known as digital signature.
- **Authentication exchange:** This technique uses a specific identity to recognize the sender and receiver.
- **Traffic padding:** It includes the insertion of redundant bits into the gaps present in the data stream to mitigate the traffic analysis attempts.
- **Routing control:** This technique offers the security through the dynamically changing the routes through which the data is to be travelled between sender and receiver.
- **Notarization:** It presents a data security model through selecting a third party which is trusted one to control the information flow.
- **Access Control:** The access rights are controlled in this technique through various parameters.

Cryptography is an art of transforming the data in an unreadable form to protect the information from attackers.

The encrypted data seems to be in the form of noise for anyone who is not having the encryption key. It is classified as symmetric or asymmetric on the basis of the encryption key used in the process.

Comparison between Asymmetric and Symmetric algorithm:

Symmetric Algorithm	Asymmetric Algorithm
It uses session (single) key for both encryption and decryption.	It uses (public & private) different keys for encryption and decryption.
It is fast in execution.	It is slow in execution due to high computational burden.
It is used for bulk data transmission.	It is often used for securely exchanging secret key.
It is also called secret key or private key cryptography.	It is also called public or modern cryptography.
It utilizes fewer resources as compared to asymmetric key cryptography.	It utilizes more resources as compared to symmetric key cryptography.
It is safe and faster.	It allows letting other people read the encrypted message and no issue of key distribution.
Examples: DES, 2DES, 3DES, AES, RC4	Examples: RSA, Diffie-Hellman

2. Literature Review

Siddharth Choubey Dutt and Namdeo Mohit Kumar (2015) recommended that cloud computing is a rapidly growing computational mold. It has many users who use cloud services such as social media, electronics, etc. Mails, file sharing, and others that increase cloud data weight recurring storerooms.The danger of data-freeness also rises. The data security measures, therefore, need to be provided in cloud computing models. There are some expected answers to assess these questions, based on techniques on encryption. The authors presented some data security and privacy enhancing models using the different encryption techniques. Their main contribution is the execution of a study of various Data Security and Privacy solutions in existing cloud Scenarios on computing. However the computation complexity associated with adding more tedious encryption algorithms presents a trade off with other network parameters like throughput, end to end delay and latency.

Jingwei Huang and David M Nicol (2010) emerged with an analysis of the manual trust mechanisms and comment on their limits. Then there they tackled those constraints by suggesting more precise mechanisms on proof, certification attribute, and validation, and finish by suggesting a system for uniting different trust strategies to uncover confidence chains web. A detailed survey has been presented in this paper to understand the depth of various trust-based security models are proposed by researcher over the last two decades. The limitations and potentials of these techniques were studied through various attributes, evidences, certificates and validation to derive a conclusion about the research gap. The researchers have addressed this research gap by providing the chain of trust mechanism for the cloud environment. The authors have also verified the effectiveness of their proposed system using some simulation analysis. But the proposed chain of trust algorithm has introduced the delay in the network due to the extended security model. Also, it addressed the authentication aspect of cloud only, other aspects like integrity and authorization has remained as a challenge to the researchers and been compromised.

One of the key issues is the protection and confidentiality of data information stored and managed on systems provided by cloud service providers. In this work, (Farrukh Shahzad 2017) surveyed quite a few cloud computing research works related to security confrontations and privacy issues. The author has specifically addressed the nature of the attacks which are encountered generally in a cloud environment. It has been done to identify the characteristics of the malicious intentions of the attackers and has been analyzed further to understand the trend. Depending on the analysis about the nature of attacks, various security and privacy models have been discussed in this paper to present a complete insight about the utility of a typical algorithm in a specific case of attack. This work although has helped in relating the utility of various security models under different malicious environment, but could not be able to reflect the effect of implementing these models to the other network parameters. As cloud computing is a technology which heavily relies upon the users' expectations fulfillment, the security model should be selected in such a way that the service to the users does not get affected severely. A balanced approach has to be selected to attain this objective.

Yong Yu et al. (2014) put forward a possession of Remote Data Possession Checking (RDPC) algebraic sign mechanism for the security of data in cloud computing environment. It was a combination of two data checking algorithms which has some remarkable statistical value. RDPC is implemented in this work to check the data remotely first before sharing it on cloud so as to avoid the unauthorized access. The authenticity is further enhanced using the statistical security framework known as algebraic sign mechanism which presents a mathematical model to evaluate the authenticity of the user. Negative sign represents the unauthorized access and positive sign of the evaluation parameters reflects the authorized access. It is very simple and computationally easy algorithm for the security of data. It helped in establishing a fine tradeoff between the security metrics with the network parameters. This technique has achieved many desirable features, such as maximum reliability, small confrontational length, and reactions. It has shown as an improved scheme to fix original security flaws through the suggested protocol. A simulation analysis was also performed by the authors to verify the effectiveness of the proposed algorithm and both the conceptual and productivity exams findings suggest the improvement is safe and practical.

Jolanda Modic et al. (2017) build up new security for the cloud method of evaluation known as Moving Intervals Process (MIP) which has all of this quality. They have presented that integrity and confidentiality play a very important role for the trust of Cloud Service Customers (CSCs) on Cloud Service Providers (CSPs). The authors have emphasized on the need of continuous assessment of security at the end of CSPs. These assessment schemes should also be efficient enough in real time applications such that they are able to support multiple requests in parallel incorporating the ever increasing number of CSCs. The

authors have proposed a new cloud security assessment named as MIP. In comparison to the conventional methods of security assessment, the proposed model is found to have a lesser computation complexity and better implement ability for real-time internet use evaluation. Although MIP offered both correctness and high computational skills but lacks in the depth of security for the highly sensitive applications.

3. Problem Statement

"Privacy is a state in which one is not observed or disturbed by other people" Privacy protection policy is an approach to isolate the sensitive information from unauthorized access. Cryptographic techniques are used to convert human readable text into non readable format. Security keys are used to make every transaction unique and generate different cipher text. Security algorithms always introduce extra computation and second level of effort to make things unreadable.

The study of existing solutions address that security algorithms always increase overhead of encryption and decryption. The security of data has been debated in detail. Comprehensive literature was clarified here Cloud Security review, RSA-related research article, elliptic review Curve cryptography and search algorithms for cuckoos. Many have been analyzed good cloud encryption and decryption methodologies safety. Following observations are made during the literature survey:

1. Security, privacy, confidentiality and integrity are very important parameters in the cloud computing environment.
2. Various researchers have addressed these issues and presented their techniques to improve these parameters.
3. The researchers have addressed the problem of cloud security and presented various techniques like RDPC, MIP, etc., but the other parameters like computational complexity, amount of overhead, throughput have been traded off.
4. Some researchers have presented the RSA, ECC and CSA based encryption techniques to enhance the security for cloud environment but the security level has not been achieved to a desired level for sensitive applications. The performance was also a function of initial conditions of evolutionary methods.
5. A security model which could present a perfect combination of security depth along with mathematical simplicity has been the research gap identified.
6. The combination of hybrid security framework can provide an optimal solution considering the security parameters and the network parameters.

4. Methodology

Proposed methodology evaluates on five major objective: confidentiality, authentication, integrity, access control and non-repudiation. We are concentrating on all aspects of security to improve the performance of cloud computing in all stages. Proposed solution is majorly divided into three major objectives which are cited below;

1. Data Privacy & Confidentiality

The proposed solution observes that hybrid encryption algorithms could help to raise the level of security and also provide better privacy level. This paper proposed use of RC6 and Blowfish as symmetric cryptography and ECC & RSA for asymmetric cryptography.

2. Authentication, Authorization & Access Control

Proposed authentication solution would help user to identify the user in better and strong authentication way. This field will help to improvise the level of user authentication and authorization using different approached. The objective of proposed model is to improve the performance of authentication by proposing certain techniques which are followed as;

1. Username & Password technique
2. Security Question verification approach
3. Security token based verification
4. Mobile Verification using One time password
5. IP & MAC Verification
6. Kerberos Authentication systems

This work examine that there are multiple cases when user will try to get login into system. Here, few most popular cases are considered to proposed authentication layer in particular situation.

3. Access Control

In this paper, a Hybrid approach is used for healthcare cloud using RBAC and ABAC access control with using encrypted technique like ECC and Blowfish.

The information related to health care can be threaded by the following ways:

- Intruders that are the human threats can be hacker.
- Threats through natural disasters like earthquakes, fire etc.
- Technical issues and failures like damage of system and crashing.

By analyzing the complete work, its main objective is illustrated using some mitigating approached diagnosing the existing work.

1. To simulate the mapping of role and attribute based access control.
2. To diagnose the issue of information mislead because of the insecure and sensitive information.
3. It determines which roles can be accessed by which attributes.
4. For privacy maintenance, the complete work is contributed.
5. ABAC and RBAC are combined to form RABAC.

The proposed security strategy has been implemented for the Electronic Medical Records (EMR) data and its effectiveness has been evaluated on cloud environment. The development in the field of healthcare sector has seen revolutionary over the last decade because of digitization of complete medical data referred as electronic medical records

(EMR). It also has strengthened the research in terms of prognostic and diagnostic capabilities. EMR comprises of elementary information and medical history of the patients, clinical and doctor data, insurance information, etc. It also the readings and records generated through the internal and external sources like biometric data, genetics, blood pressure, electronic medical records, remote sensors data and social media data [1,2,3]. The application of cloud computing technology in healthcare sector can be proved useful in preventing epidemics, improving the quality of life, effectiveness of Clinical Trials, Detecting Side Effects of Drugs, etc. It can also avoid the preventable deaths through wise clinical decisions [4,5].

Considering the importance of the attributes of the patient's information in EMR, the security and privacy of the data has emerged as serious challenge. Any unauthorized access and unethical manipulation of the data may lead to large scale disaster medically and economically. Healthcare sector is also been changed a lot over the last two decades in terms of participation of technologies in the medical research and diagnosis. The available data of the medical records of millions of patients all over the world and their treatment history has changed the complete dynamics of the sector. This data has been used for the innovative treatment, focused care quality and value and evidence based medical practice instead of subjective treatment.

Cloud computing in healthcare sector has presented a great potential for completely changing the way of medical treatment and research. But it also has offered manifold challenges and constraints for the same. The biggest challenge associated with the implementation of cloud over healthcare is the privacy and security of the EMR. The available security frameworks for the healthcare sector are not very efficient and secured for the ever increasing threat of cyber crime. Any compromise with the medical record may be severely used by the malicious stakeholders and may results into a medical blunder all over the world. Therefore, security of the huge amount of medical data is a big concern for the researchers.

Hybrid technique will be implemented and then permission will grant to user on the basis of some set limit of threshold value. These threshold values are set which will decide whether the user is attacker or genuine on the basis of Hybrid Technique which is the combination of Role Based Access Control (RBAC) and Attribute based Access Control (ABAC).

At last for decryption process, authenticate user will be given information that even chunks will be decrypted using ECC algorithm and odd chunks will be decrypted using Blowfish algorithm. The process of implementation of the hybrid security framework for EMR is as follows:

- Uploading of the original data (text and image) by the user and verification of relative fake data cloud over insecure internet connection.
- Bifurcation of data into chunks in binary form.
- Then encryption technique will be followed on original and fake data using ECC and Blowfish technique.
- And, these cryptographic techniques will be applied randomly on any random data.
- With it, data will be shuffle for further process.

Finally, the complete study address a security model for particular security later with recommended algorithms. All recommended algorithms and layers are shown below:

Security Layer	**Recommended Algorithms**
Confidentiality	Combination of RSA, ECC, RC6, Blowfish
Authentication	1. Username & password verification 2. Security question approval 3. Security token verification 4. One Time Password verification 5. IP Address and MAC Address verification 6. Server Verification using Kerberos
Access Control	ABAC, RBAC, Combination of ABAC & RBAC

5. Experimental Analysis

The results analysis for the complete work describes the performance of the hybrid algorithm proposed in terms of cipher text size, encryption and decryption time taken by the hybrid algorithm proposed. We calculate the time of computation using different size of the paper. The hybrid algorithm proposed is also compared with the algorithms already in place. Experimental analysis enhance working on different size of data like 1KB, 10KB, 100KB, 1000 Kb and 10,000 KB, and on it different cryptography technique like RC6, AES, BLOWFISH, ECC and RSA is applied for the comparison of performance and evaluate the performance of encryption time and decryption time in terms of milliseconds.

Table 1: Encryption Time [ms]

Data [KB]	AES	RC6	Blowfish	RSA	ECC
1 KB	3	2.5	26	112	85
10 KB	19	16	40	212	115
100 KB	95	62	56	513	390
1000 KB	215	165	66	2356	856
10000KB	1856	1325	104	4569	1669

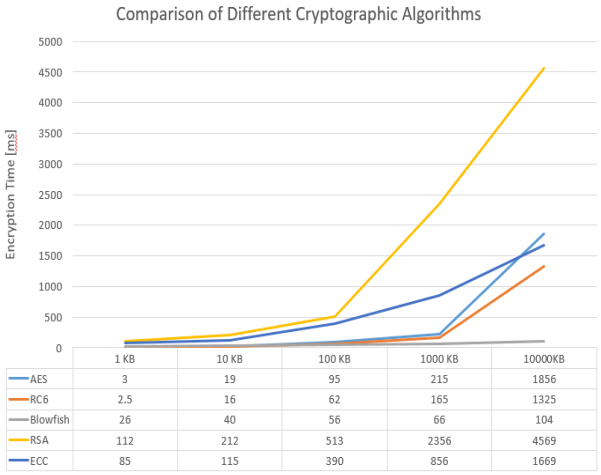

Fig5: Comparison of Encyption Time

Table 2: Decryption Time [ms]

Data [KB]	AES	RC6	Blowfish	RSA	ECC
1 KB	4	3	29	186	109
10 KB	23	19	48	289	156
100 KB	101	78	65	796	456
1000 KB	245	195	79	2656	956
10000KB	1986	1675	125	4969	1869

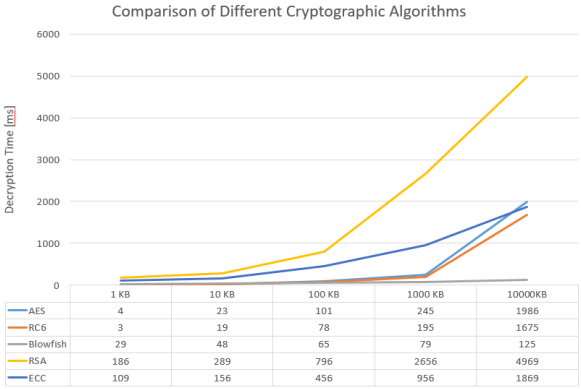

Fig 6: Comparison of Decryption Time

Experimental analysis enhance working on different size of data like 1KB, 10KB, 100KB, 1000 Kb and 10,000 KB, A comparison of different execution time is shown in below;

Table 1: Execution Time [Seconds]

Data [KB]	Traditional System	Proposed Model
1 KB	3	4.5
10 KB	19	22.56
100 KB	95	96.25
1000 KB	285	312
10000KB	2252	2312

6.Conclusion

The complete work concludes that security plays significant role to improve the confidentiality of system along with overhead for memory and computation also. The point of this review was to feature the confidentiality issues related with cloud computing by utilizing cryptographic technique.

We have developed a cloud based application where we implemented these 5 algorithms (RC6, AES, BLOWFISH, RSA and ECC) using restful API. Here, evaluation is performed by checking the behaviour of algorithm using the same type of data with same size on the same machine configuration. The complete implementation address that symmetric key cryptographic algorithms create less overhead in comparisons with asymmetric key cryptographic algorithms but they are less secure due to single key concept. ECC perform better than RSA and Blowfish perform better that RC6 and AES in symmetric key category. The complete work proposed that in future hybrid cryptographic solution could be develop to achieve high strength security with authentication and integrity. To improve the security structure, we have provide a security model defining different security mechanism to improve performance of cloud environment in different situation along with encryption algorithm, To improve the level of confidentiality, ECC & Blowfish algorithms are implemented.

The complete work also concludes that removing of mobile verification and Kerberos from private network help us to reduce lots of effort. Subsequently, integration of IP & MAC address verification help to keep the level of security at higher level and reduce the overhead of cost and time by removing mobile OTP verification.

We observe during Implementation that the encrypted data size is large than the plain text. The encrypted data size can be popular in the future without having to negotiate with encryption and decryption times.

With different types of files other than.txt files with example.mp4,.doc, etc., the suggested hybrid model can also be applied. It can be used in the future for specific applications such as military applications, hardware and software companies needing security in their products, large websites with large databases, mobile applications and cloud-based applications.

In this approach, we are working on 3A's (Authentication, Authorization and Access control) to implement multidimensional approach and overcome the issues of existing work regarding the data security and privacy protection in two dimensions in cloud computing.

Following conclusions were draws after the study of proposed work.

- Proposed solution not only increase level of security to insure proof of identity and access rights but also help to differentiate sensitive data and general purpose data.
- Proposed model increase little computation time but not very huge.
- Enhanced execution time is negligible against the level of security which has been increased due to AAA model.
- Proposed solution can be implementing for any public platform which is having sensitive data.

This paper observes that proposed model can also be integrated with e-commerce and other platform to increase the level of security.

REFERENCES

[1] *M. Thangapandiyan, P. M. R. Anand and K. S. Sankaran, "Enhanced Cloud Security Implementation Using Modified ECC Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 1019-1022.*

[2] *Rohini and T. Sharma, "Proposed hybrid RSA algorithm for cloud computing," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 60-64.*

[3] *Salma, R. F. Olanrewaju, K. Abdullah, Rusmala and H. Darwis, "Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms," 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), Makassar, Indonesia, 2018, pp. 18-23.*

[4] *F. S. Wu, "Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm," 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Changsha, 2018, pp. 125-129.*

[5] *Akhil K.M, Praveen Kumar M, Pushpa B.R, "Enhanced Cloud Data Security Using AES Algorithm". 2017 International Conference on Intelligent Computing and Control (I2C2).*

[6] *B. Lee, E. K. Dewi and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," 2018 27th Wireless and Optical Communication Conference (WOCC), Hualien, 2018, pp. 1-5.*

[7] *K. Rani and R. K. Sagar, "Enhanced data storage security in cloud environment using encryption, compression and splitting technique," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-5.*

[8] *S. Ojha and V. Rajput, "AES and MD5 based secure authentication in cloud computing," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 856-860.*

[9] *P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1635-1638.*

[10] *I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 172-175.*

[11] *P. N. Hemanth, N. A. Raj and N. Yadav, "Secure message transfer using RSA algorithm and improved playfair cipher in cloud computing," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 931-936.*

[12] *A. Bansal and A. Agrawal, "Providing security, integrity and authentication using ECC algorithm in cloud storage," 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 2017, pp. 1-5.*

[13] *S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 267-271.*

[14] *S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 267-271.*

[15] *V. P. Bansal and S. Singh, "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs," 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), Chandigarh, 2015, pp. 1-5.*

[16] *Khalid M. Abdullah Essam H. HousseinHala H. Zayed, "New Security Protocol using Hybrid Cryptography Algorithm for WSN". 1st International Conference on Computer Applications and Information Security (ICCAIS), IEEE, 4-6 April. 2018*

[17] *Milind Mathur, AyushKesarwani, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH, and AES". Proceedings of National Conference on New Horizons in IT – NCNHIT 2013.*

[18] *V. Kapoor, Rahul Yadav, "A Hybrid Cryptography Technique for Improving Network Security", International Journal of Computer Applications, Volume 141, No.11, May 2016.*

[19] *M. Harini, K. Pushpa Gowri, C. Pavithra, M. PradhibaSelvarani, "A Novel Security Mechanism Using Hybrid Cryptography Algorithms". International Conference on Electrical, Instrumentation, and Communication Engineering (ICEICE), IEEE 2017.*

[20] *Kalyani Ganesh Kadam, Prof. Vaishali Khairnar, "HYBRID RSA-AES ENCRYPTION FOR WEB SERVICES". International Journal of Technical Research and Applications, Issue 31(September 2015), PP. 51-56.*

[21] *F. Fatemi Moghaddam, S. Gerayeli Moghaddam, S. Rouzbeh, S. KohpayehAraghi, N. MoradAlibeigi, and S. DabbaghiVarnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments," in IEEE Region 10 Symposium, Kuala Lumpur, Malaysia, 2014, pp. 508–513.*

[22] *JayrajGondaliya, JinishaSavani, Vivek Sheetal Dhaduvai, Gahangir Hossain, "Hybrid Security RSA*

Algorithm in Application of Web Service". 1st International Conference on Data Intelligence and Security IEEE 2018.

[23] *KirtirajBhatele, Prof Amit Sinhal, Prof Mayank Pathak, "A Novel Approach to the Design of a New Hybrid Security Protocol Architecture". International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) IEEE 2012.*

[24] *A. Arjuna Rao, K Sujatha, A Bhavana Deepthi, L V Rajesh, "Survey paper comparing ECC with RSA, AES and Blowfish Algorithms". International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 1, IJRITCC January 2017.*

[25] *Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk, "A New Security Protocol Using Hybrid Cryptography Algorithms". 9th International Computer Engineering Conference (ICENCO), IEEE 2013.*

[26] *Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).*

[27] *Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." INFOCOM, 2010 Proceedings IEEE, 2010*