Time Based Encryption & Decryption for Enhancing Security in File Sync & Share System over Business Cloud

Anulekha Goud[1*], Khushboo Agarwal[2], Jaimala Jha[3]
[1*]CSE/IT Dept., Madhav Institute of Technology and Science, RGPV, India
[2] CSE/IT Dept., Madhav Institute of Technology & Science, RGPV, Gwalior, India

ABSTRACT: "Cloud computing is the new standard of delivery of information technology resources and capabilities as a service with fewer efforts to end user over the cloud. Cloud computing enable users to store and access data and programs through the internet, rather than of your computer system. The cloud is just a mirror image of the internet. There are several security threats over cloud and some dedicated solution." In this paper We Proposed a multi-layer model for file sync and share system which assistance to enhance traditional file sync and share model of data security for cloud computing. Proposed security model based on cloud file sync and share system. This model provide 3 layers system structure in which these layers are used for ensuring cloud data security. All techniques and mechanism useful to implementing a highly protected environment for cloud user to secure their private data over the cloud. This model support high security login feature which will prevent end user from unauthorized users who tried to access secured file stored on cloud.

Keywords: Cloud Computing, Cloud Computing Adoption Framework, Enterprise File Sync And Share, Multilayer Security, RSA Algorithm, ECC Algorithm.

I. INTRODUCTION:

Cloud computing is a technology that enables online access to computing resources like platforms, hardware components, infrastructure, computing applications etc. without much effort. It is cost effective where service consumer will pay for what he used. Cloud computing is a technology that plays vital role in IT industry. Not only in IT field but also smaller enterprises are adopting this technology where cloud service provider provides services and consumers access those services through the internet. Cloud is a place where service provider keeps their resources which are available to the consumers/users and consumers are billed on pay per use basis [1]. This technology provides its services in three layers. They are Infrastructure as a service, Software as a service and Platform as a service. These services deployed in three ways i.e. as public cloud, private cloud and hybrid cloud. In public cloud services are made available to public over the net, in private cloud services are available only to etherize party and hybrid cloud used to mean two separate clouds join together (public, private, internal or external). [5]
Firstly according to Pay-as-you go, it allows consumers to utilize the services with no upfront payment. So that one can deploy and develop applications without initial investments. Consumer has to pay according to the usage. [2].

❖ CLOUDCOMPUTING ADOPTION FRAMEWORK:

Cloud computing (CC) and their services have currently become a vital issues in today's world. Cloud Computing can be consider as a technology which provide users to access computing facilities such as "data storage" and "software services" through the Internet. Cloud Computing Adoption Framework (CCAF), to contribute a way to successfully adopt and deliver any Cloud services and projects for any other organizations.[10] The CCAF is a complete model for adopting and implement cloud security principles systematically and also help to understand the security challenge. This frame-work can consolidate with Cloud Computing services to provide supplemental values for adopting organizations [12]. It is also an architecture framework focused on the delivery of a security service, in the form of developing a multi-layered security for Data centers. This help to design a complete multilayer model for implementation and service for Cloud security under the CCAF

recommendation.[22] Computer or network security has been classified into a number of general concepts and processes such as identification, which identifies objects, functions, action, authentication, authorization, privacy, integrity and durability.[15] There is a need to follows a well-established general security aspect with identification, authentication, authorization, and digital security encryption and decryption. [21]

❖**ENTERPRISE FILE SYNC AND SHARE (EFSS):**

Enterprise File Sync and Share (EFSS) is a software service which provide organization to securely share or synchronize cloud data such as photos, videos and file from multiple devices with employees and end user in a business cloud environment. To provide enterprises with the beneficial cloud file sync and share service while consider enterprise Concerns such as security, compliance, and regulation, the cloud file sync and share service was been deployed by either on-premise or hybrid cloud model to target high value. Existing EFSS systems based on system security and manageability. CCAF framework, important EFSS security issues should be well addressed, particularly for businesses with serious data services.

II. RELATED WORK

Preeti Sirohi_and Amit Agarwal [2015] et. al presented that, Cloud Computing is next generation computing technology with the dynamic capabilities of adding new resources and services as per user demand and requirement. Cloud computing is fast growing technology which facilitates more and more users and organizations shifting towards opting their services to cloud. Data security is considered as the constant issue leading towards a hitch in the adoption of cloud computing. Data privacy, Integrity and trust issues are few severe security concerns leading to wide adoption of cloud computing. The advent of the proposed model has sufficient functionalities and capabilities which ensures the data security and integrity. The proposed framework focuses on the encryption and decryption approach facilitating the cloud user with data security assurance. The proposed solution only talks about the increased security but does not talk about the performance. The solution also includes the functioning of forensic virtual machine, malware detection and real time monitoring of the system. A data security framework also provides the transparency to both the cloud service provider and the cloud user thereby reducing data security threats in cloud environment.[7] Yu et al [13] and Wang et al [14] describe the fine-grained security model for Cloud storage. Both are similar, except that scheme from Yu et al [14] are added in specifics and they describe concepts and users associated with their proof-of-concept. Victor Chang (2015) et. al presented, some tests were planned to establish the robustness of the CCAF multi-layered security. However, they do not have any experiments, simulation and empirical data to prove the effectiveness and robustness of their fine-grained security model. Thus, both proposals do not address in-depth data security issues, when the rapid depth data security issues, when the rapid growth of data is a challenge for the Data Center.[9] Eman M. Mohamed [2012] et.al propose a new data security model based on studying of cloud computing architecture. A software is implemented to select the appropriate and the extreme security encryption algorithm. The proposed model resolves cloud user security glitches, which is assistance cloud provider to hand-picked the most appropriate encryption algorithm to its cloud.[24]

III. PROBLEM STATEMENT:

In the open stack EFSS There are some key security issues in multilayer environment which may be effect Employee privacy and their cloud data security. Following matters designate the opened EFSS security issues.[13]

(1) Employee Privacy: Existing EFSS systems generally encrypt data to prevent from leak of information. EFSS systems uses one Master key for the encryption of existing entire data space, which can examine enterprise data and prevent data leaks from outside but unable to prevent data leaks from inside. [9]

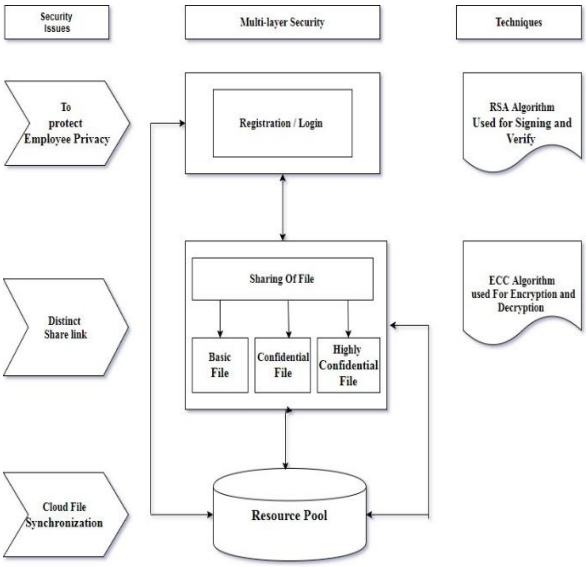
(2) Share Link: The share link is broadly used to share data to business associates who do not have an valid EFSS system account. Due to this it introduced a new security ambiguity which might be used for data to unauthorized domain without leaving enough audit trail [9].

(3)Cloud File Synchronization: Cloud File synchronization introduce a new security issue. It synchronizes mutual and collective enterprise data from a succeeded EFSS service to employee's endpoint devices, and enterprises then have no or may be less control to the synchronized enterprise data.[9]

IV. METHODOLOGY

MULTILAYER SECURITY FOR CLOUD:
This model having different encryption a different level which help to protect cloud file and also ensure confidentiality, integrity of the file (data) ,this model also provide faster retriever of data and file from resourceful . [6][7]
This proposed model mainly consist three layer which is interdependent.

Layer 1 - This layer is responsible for authentication of cloud user. It provide secure registration of end cloud user by using RSA algorithm for secure login. This algorithm used for authentication of user by using complicated password which generated at the time of registration because of using RSA algorithm it generated one time complicated (long) password due to single sign on service which can't altered by user the main task of this layer is to prevent unauthorized user entering in the cloud environment. In this phase if cloud user will enter password more than three time then user will be blocked by system. [20]



Multi-Layer Approach for File Sync & Share

Layer 2- This layer communicate with layer-1 to make sure that only authorized user can send and received files. This layer uses different encryption algorithm then previous one that is use for enhancing confidentiality and integrity of the file in cloud computing environment. This layer uses elliptic curve cryptography (ECC) algorithm for sharing a file with authorized user. This algorithm provide sync and share the file on the bases of their confidentiality. It provide multiple phase to sync and share a file.[13]

- If it is a Basic file (no needs to secure) then algorithm provide to sync a file with authorized user (either one or many)
- If it is confidential file then the file will be share only with the authorized user that has been selected by the sender.
- If it is a highly confidential file then system will ask user a personal question which will answered by only authorized user (who have authority to access a highly confidential file).

It also provide a session to sync and share a file for encryption and decryption to ensure the true and authenticate file will share or received.

Layer-3 - This layer responsible for storing and managing data from layer 1 and layer 2 after encryption of data this layer interact with second layer and ensure that user requested data for accessing from resource pool is genuine at this layer uses strong security feature to protect data before storing the data into the resource pool.[17]
This layer provide all cloud user data whenever they requested for it and also provide appropriate information as they requested without any delay. This layer share confidential data only with authorized user and enhance security of confidential file and data stored in resource pool over the cloud. [23]

CRYPTOGRAPHY TECHNIQUE:
Mainly 2 cryptography techniques used in this multilayer model. RSA Algorithm ECC Algorithm.

1. RSA Algorithm:

RSA Algorithm is a asymmetric public key algorithm it uses two different keys one is public key and another is private key this algorithm includes multiplying two large prime numbers that establishes the public key and private key[18], once the keys have been developed ,the original prime numbers are no longer important and can be rejected. [29] The private key in RSA algorithm never needs to be sent across the internet. Private Key is used to decrypt text that has been encrypted with the public key. [30] RSA is a block cipher, in which every message is mapped to an integer. User data is encrypted first and then it is stored in the Cloud. When required, user places a request the data for the Cloud provider, Cloud provider authenticates the user and delivers data. .RSA is a block cipher, in which every message is mapped to an integer. Encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding private key.[31]

2. ECC Algorithm

Elliptic curve cryptography, an action takes over elliptic curves is called addition. Multiplication is distinct by repetitive addition. For instance, K×A = A + A + A + A + A + ……., K times, where the addition operation is performed over the elliptic curve. This forms the basis of the distinct logarithm problem for an elliptic curve and its property that is also referred to as a trapdoor [19]. It can be explained as follows: Cryptanalysis requires us to find the value of K, given A and K×A. This is computationally hard if we stick to repeated addition method and K is very large (which usually is, since we are talking about security).[16]Before exploring how this is a difficult problem let's see the equation which defines the elliptic curve,

$y^2 + axy + by = x^3 + cx^2 + dx + e.$

This curve has been defined over real numbers and may include infinitely many points.[21] For feasibility, we define the elliptic curves over prime field to include a finite set of points.[28] We define the curves over primes by simplifying the above relation:

The equation of an elliptic curve is given as,

$y^2 = (x^3 + ax + b) \bmod p$

Key Generation:

Step-1 Select a number'd' within the range of 'n'. This equation used to generate the public key.

Q=d*P

d = The random number that we have designated within the range of (1 to n-1).

P= the point on curve.

Encryption:

'Q' is the public key and'd' is the private key.

Let 'm' be the message that user wants to send. We have to represent this message on the curve. This have comprehensive implementation details.

Step-2 Let 'm' has the point 'M' on the curve 'E'. Randomly select k from [1 - (n-1)].

Step-3 Two cipher texts will be produced let it be C1 and C2.

C1=k*P

C2=M+k*Q

C1 and C2 will be send.

Decryption:

Step-5 We have to get back the message 'm' that was send,

M=C2-d*C1

M is the original message that send by user.

Proof: What is the use full step by which we get back the original message?

M = C2 - d * C1

'M' can be represented as 'C2 - d * C1'

C2 - d * C1 = (M + k * Q) - d * (k * P)

(C2 = M + k * Q and C1 = k * P)

= M + k * d * P - d * k *P (canceling out k * d * P)

= M (Original Message)

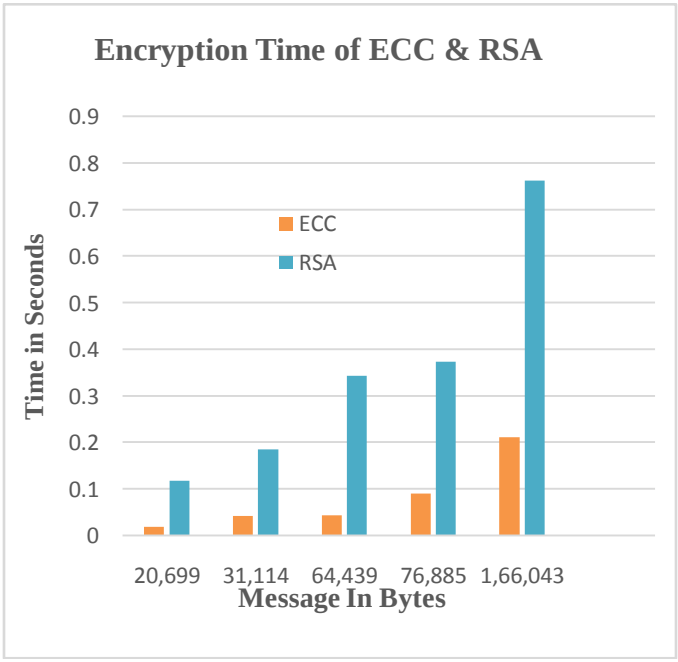
V. Results and Discussion

All the algorithms were implemented in Microsoft visual studio 2010 Framework with Intel(R) core(TM) i3-5010U processor 4.00 GB of RAM and 64-bit operating system. We give the encryption and decryption operating time taken in seconds. The result is the average of 4 test runs.

Layer-2 ECC & RSA Algorithm Encryption Time:

S. no	Message in Bytes	Key Size in Bit	Encryption Time in ECC (Second)	Key Size in Bit	Encryption Time in RSA (Second)
1.	20,699	ECC 224	0.0180	RSA 1024	0.1170
2.	31,114		0.0410		0.1840
3.	64,439		0.0430		0.3430
4.	76,885		0.0900		0.3730
5.	166,043		0.0210		0.7630

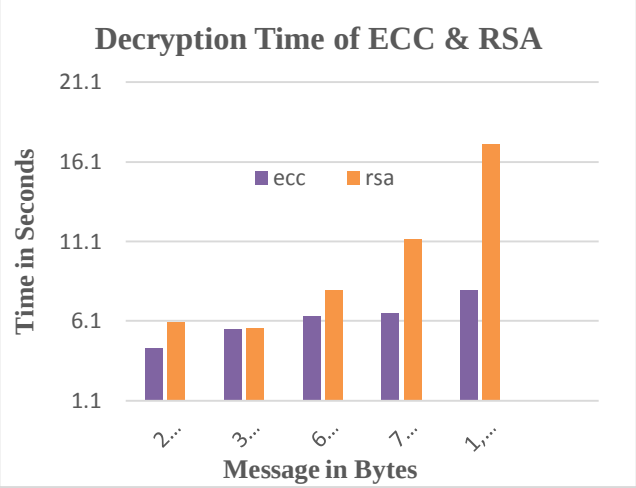
Table-1



Layer-2 ECC & RSA Algorithm Decryption Time:

S. no	Message in Bytes	Key Size in Bit	Decryption Time in ECC (Second)	Key Size in Bit	Decryp-tion Time in RSA (Second)
1.	20,699	ECC 224	4.4062	RSA 1024	6.000
2.	31,114		5.5523		5.6548
3.	64,439		6.4008		8.5529
4.	76,885		6.6058		11.2551
5.	166,043		8.0049		17.1979

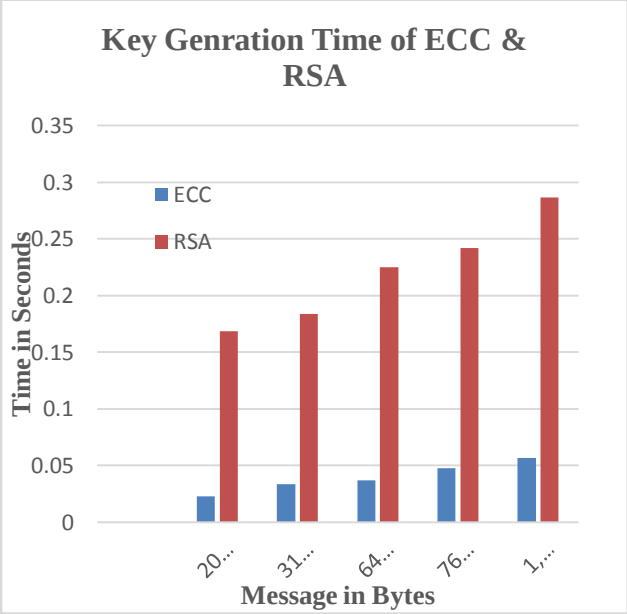
Table-3



Key Generation Speed in ECC & RSA:

S. no	Message in Bytes	Key Size in Bit	Key Generat i-on Time in ECC (Second)	Key Size in Bit	Key Generati-on Time in RSA (Second)
1.	20,699	ECC 224	0.023	RSA 1024	0.169
2.	31,114		0.048		0.184
3.	64,439		0.037		0.225
4.	76,885		0.048		0.242
5.	166,043		0.057		0.287

Table-4



Summary of Result:

Criteria	RSA Algorithm	ECC Algorithm
Key Generation Speed		√
Encryption Speed		√
Decryption Speed		√

Table-5

VI. CONCLUSION & FUTURE WORK

In cloud computing environment several security issues introduce day by day. This paper demonstrate multilayered security approach and its implementation, and consider some of security issues of EFSS (enterprise file sync and share) which help to enhance the security of CCAF (Cloud Adoption Framework).This proposed model consider CCAF multilayer security with three integrated layer those are interdependent and consist identity management, encryption & decryption of cloud data and secure database. This multilayer model help to resolve the security issues of EFSS System. Our Future work is to strengthen the multilayer model and also provide IDS (intrusion detection system) to block more of threats and protect the system.

REFERENCES

[1] Pawan Thakur and Roohi Ali "Cloud Computing" by Tech India publication series.
[2] Atul Kahate Cryptography & Network Security.

[3] Maneesha Sharma, Himani Bansal and Amit Kumar Sharma, "Cloud Computing: Different Approach & Security Challenge", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[4]http://www.barkatconsulting.com/wpcontent/uploads/2014/08/cloud1.png
[5] Harshitha. K. Raj."A Survey on Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering.
[6] RABAI, L. B. A., JOUINI, M., AISSA, A. B. & MILI, A. "A cyber security model in cloud computing environments". Journal of King Saud University -Computer and Information Sciences, 25, 63-75, 2013.
[7] Preeti Sirohi_and Amit Agarwaly "Cloud Computing Data Storage Security framework relating to Data Integrity, Privacy and Trust" Institute of Management Studies, Ghaziabad Department of Computer Science,UPES, Dehradun, India. 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015)
[8] Amin Saedi "Cloud Computing Adoption Framework: Innovation Translation Approach" Universiti Teknologi PETRONAS Perak, Malaysia 2016 3rd International Conference On Computer And Information Sciences (ICCOINS)
[9] Victor Chang, Yen-Hung Kuo, Muthu Ramachandran "Cloud Computing Adoption Framework – a security framework forbusiness clouds" School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds, UK. Data Analytics Technology & Applications, Institute for Information Industry, Taiwan, R.O.C
[10] Oayne Edward Skolmen "Protection of personal information in the South African Cloud Computing environment: A framework for Cloud Computing adoption"School of Information and Communication Technology Technology Nelson Mandela Metropolitan University Port Elizabeth, South Africa IEEE 2015.
[11] Ahmad Mohammad Zaher Asadullah and Ishaq Oyebisi Oyefolahan "Factors Influencing Information Privacy Concern in Cloud Computing Environment"Information System Department, International Islamic University Malaysia Kuala Lumpur, Malaysia 2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC).
[12] Ahmed Albugmi Robert Walters, "A framework for Cloud Computing Adoption by Saudi Government overseas agencies Gary Wills School of Electronics and Computer Science" IEEE 2016.
[13] Yen-Hung Kuo, Tzu-Wei Yeh, Guang-Yan Zheng, Jyun-Kai Wu, Chao-Chin Yang, Jia-Ming Lin"Cloud System Software Institute for Information Industry" Taipei City Taiwan "Open Stack Secure Enterprise File Sync and Share Turnkey Solution" 2014 IEEE 6th International Conference on Cloud Computing Technology and Science.
[14] Samsiah Ahmad Nor liza Saad 2, Zalikha Zulkifli and Siti Hajar Nasaruddin "Proposed Network Forensic Framework for Analyzing IaaS Cloud Computing Environment" Department of Computer Sciences, Faculty of Computer and Mathematical Sciences, UiTM Perak, 35500 Tapah Road, Perak, Malysia 2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC).
[15] Ryan K L Ko , Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg , Qianhui Liang, Bu Sung Lee "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" Cloud & Security Lab Hewlett-Packard Laboratories,Singapore 2011 IEEE World Congress on Services
[16] Soram Ranbir Singh, Ajoy Kumar Khan, Takhellambam Sonamani Singh "A Critical Review on Elliptic Curve Cryptography" Manipur Institute of Technology Takyelpat, Imphal, India 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (I²IT), Pune
[17] Asma Chaouch, Belgacem Bouallegue, Ouni Bouraoui "Software Application for Simulation-Based AES,RSA and Elliptic-Curve Algorithms" Laboratory of Electronic and Micro-electronics (EμE) Monastir, Tunisie 5000 2nd International Conference on Advanced Technologies for Signal and Image Processing - ATSIP'2016 March 21-24, 2016, Monastir, Tunisia
[18] Vishwanath S Mahalle , Aniket K Shahade "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm" Department of Computer Science & Engineering Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra, India IEEE 2014
[19] Madhumita Panda Lecturer, "Performance Analysis of Encryption Algorithms for Security" Computer Science SUIIT, Sambalpur University Odisha, India International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016
[20] Hwang, Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu, "A Business Model For Cloud Computing Based On A Separate Encryption And Decryption Service", 2011 IEEE.

[21] Cong Wang, Qian Wang, And KuiRen" Ensuring Data Storage Security In Cloud Computing"
[22] S. Sajithabanu and E. G. P. Raj, "Data Storage Security In Cloud, "International Journal Of Computer Science And Technology, Vol. 2, Issue 4,Pp.437-440,Oct. –December 2011.
[23] N. Antony And A. A. R. Melvin, "A Survey On Encryption Schemes In The Clouds For Access Control," International Journal Of Computer Science And Management Research, Issn 2278-733x, Vol. 1, Issue 5, Pp. 1135-1139, December 2012.
[24] Eman M. Mohamed, Hatem S. Abdelkader and SherifEl-Etriby, "Enhanced Data Security Model For Cloud Computing," IEEE 8th International Conference On Informatics And Systems (INFOS2012), Pp. CC12-CC17 , 2012.
[25] Madhumita Panda Lecturer ,Computer Science SUIIT, Sambalpur University Odisha, India "Performance Analysis of Encryption Algorithms for Security" International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.
[26] Hanane Bennasar Mohammad Essaaidi Ahmed Bendahmane Abdelmalek "State-of-The-Art of Cloud Computing Cyber-Security" IEEE 2015
[27] Siddharth Dutt Choubey and Mohit kumar Namdeo "Study of Data Security and Privacy Preserving Solutions in Cloud Computing" Shri Ram Institute of Technology Jabalpur, India IEEE 2015
[28] Sanchit Mehrotra and Prof. Arun Kumar Agrawal "Application of Elliptic Curve Cryptography in Pretty Good Privacy (PGP)."Integrated Dual Degree Student, Department of CSE IIT (BHU), Varanasi Varanasi, India International Conference on Computing, Communication and Automation (ICCCA2016)
[29] Assist.Prof Dr. Alaa Kadhim and Rand Mahmoud Mohamed "Visual Cryptography For Image Depend on RSA & AlGamal Algorithms" Computer science department University of technology 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and A pplications (AIC-MITCSA) – IRAQ (9-10) May
[30] Sangita A. Jaju and Santosh S. Chowhan "A Modified RSA Algorithm to Enhance Security for Digital Signature" Department of Computer Science Dayanand Science College School of Computational Science S. R. T. M. University Nanded, (M.S.), India Latur, (M.S.), India IEEE 2015
[31] Ni Made Satvika Iswari "Key Generation Algorithm Design Combination of RSA and ElGamal Algorithm"Faculty of Engineering and Informatics Universitas Multimedia Nusantara Tangerang, Indonesia 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia.

Authors Profile:

Anulekha Goud, pursuedBachelors of engineering From IPS College of technology & management Gwalior, India in 2014. She is currently pursuing Master of Engineering from Madhav Institute of Technology and Science, Gwalior (MP), India

Khushboo Agrawal, M.Tech, B.E.(IT) is an Assistant Professor in the Department of Computer Science Engineering and Information Technology at Madhav Institute of Technology & Science Gwalior (MP), India.

Jaimala Jha, M.Tech, B.E. is an Assistant Professor in the Department of Computer Science Engineering and Information Technology at Madhav Institute of Technology & Science Gwalior (MP), India