A TECHNICAL SURVEY ON CRYPTOGRAPHY TECHNIQUES IN CLOUD COMPUTING ENVIRONMENT

V.Gunasundhari[1], Mrs.M.Parvathi[2]
[1]PG Scholar, Department of Computer Science and Engineering,
Nandha Engineering College, Tamil Nadu, India
[2]Associate Professor, Department of Computer Science and Engineering,
Nandha Engineering College, Tamil Nadu, India

ABSTRACT

Cloud computing could be a virtualization-based technology that permits to make configure and customise purposes by using an online affiliation. The cloud technology includes a development platform, hard disk, package application and info. Cryptography Technique is one in all the main aspects of Cloud Computing, improving the protection of the cloud storage system.Cryptographical techniques are used to guarantee secrecy and integrity of knowledge within the presence of an adversary. It's related to the method of changing normal plain text into unintelligible text and vice-versa. It's a way of storing and transmittal information in a very specific kind in order that only those for whom it's intended can read and process it. In this paper, we have present a survey of numerous cryptography Technique in Cloud Computing.

Keywords - *Cryptography, Authentication, Cloud Computing, Data encryption and Security.*

1. INTRODUCTION

Cryptography is the art of achieving security by providing completely different encryption algorithms to shield or secure the cloud inormation.Varied encryption techniques of cryptography are used in Cloud to secure knowledge which will be used or keep within the cloud. It permits clients to safely get to shared cloud administrations, as any data that's expedited by cloud suppliers is secured with encryption. Cryptography in the cloud secures sensitive knowledge while not delaying data exchange. Cryptography in the cloud permits for securing crucial knowledge on the far side our company IT surroundings, wherever that data isn't any longer beneath our management. In the cloud,we have a tendency to don't have any such mechanism that provides actual and physical management over the storage of knowledge, therefore the only method we are able to make sure that the data spreading through cloud is protected, encrypted and stored cryptographically by using numerous cryptographic techniques and algorithms.

1.1 CLOUD MODELS:

There are three types of models present in cloud computing which are given as follows:

Public Cloud Model: In Public Cloud, systems and services are simply accessible by everybody therefore, it's less secure due to its openness and needs a mechanism to create it secure .Public clouds provide an elastic, cost-effective suggest that to deploy solutions and beware of deploying, managing, and securing the infrastructure. Firms will use it on demand, and with pay-as-per use.

Private Cloud Model: Private cloud is used by an organization and so accessibility to systems and services is proscribed only to that explicit organization. Moreover, its safer than public cloud due to its private nature.

Hybrid Cloud Model: A hybrid cloud is a computing environment that combines a public cloud and a private cloud through permitting data and applictions to be shared between them.

1.2 CLOUD COMPUTING MODELS

Infrastructure as a service (IaaS) is additionally referred to as Hardware as a Service (HaaS). It's a computing infrastructure managed over the net.The important benefit of the use of IaaS is that it helps customers to keep away from the rate and complexness of shopping for and managing the physical servers.

Platform as a Service (PaaS) cloud computing platform is made for the computer programmer to develop, test, run, and manage the applications.

Software as a service (SaaS) is additionally called "**on-demand software**". It is a software during which the applications are hosted by a cloud service provider. Users will access these applications with the help of internet connection and application.

1.3. CLOUD COMPUTING TOOLS

Cloud services across a network are used as efficient, organizational-based business solutions. Various cloud computing tools, such as Eucalyptus, Open Nebula, Nimbus, Open stack, ete., are available where they all have different deployment strategies.

CRYPTOGRAPHY TECHNIQUE

Many security methods for cloud use numerous cryptographic techniques. Cryptographic techniques become essential for security in cloud. Cryptography refers to the technique widely used in computer networks to produce security to the information and messages communicated over the network. The plain text message being sent from sender is encrypted in to a special format known as a "Cipher Text" by applying some cryptographic rule and then communicated over the network. At the receiver's end, the Cipher text message is decrypted within the original plain text once more by applying some decryption rule. Therefore only the sender & receiver of the communication can read the encoded message and nobody else.

2. LITERATURE SURVEY

Mbarek Marwan[1], present a method based on the visual cryptography to secure medical image storage over cloud. This technique ensures privacy without complicated mathematical computations. The experimental results show that this technique ensures data confidentiality by splitting medical image into many shares. And also, we propose a multicloud environment to reduce security risks and to enhance performance

Sun lei, Zhao kun, Sun Ruichen, Li Shuai[2], conferred the study that aims at designed the framework of the cryptography cloud framework that has cryptography services with the cloud computing mode. The design plan of the framework is expounded from 2 aspects embrace the operate of modules and repair flow of cryptography cloud, that resulted at intervals the development of the flexibility of the applying of cryptography technology at intervals the cloud atmosphere. Through the analysis of system perform and management mode, it illustrated the supply and security of cryptography cloud framework. It had been proved that cryptography cloud has the characteristics of high-availability at intervals the implementation and experiment, and it'll satisfy cryptography service demand at intervals the cloud atmosphere.

Xiaoying Shen, Licheng Wang, Huijun Zhu, Yuan Liu[3],presents a technique based on A Multivariate Public Key Encryption Scheme with Equality Test. This paper combines multivariate public key encryption and equality test, and proposes the primary multivariate public key encryption theme with equality test (MPKEET), that inherits the benefits of each primitives. Moreover, the equality test algorithm proposed during this paper relies on a straight line. Compared with the schemes based on bilinear pairing, it's and easier to implement. And our MPKEET theme achieves fascinating security, which might resist linearization equation attacks, differential attacks, XL attacks, Gröbner basis attacks and therefore the attack of quantum computer, when appropriate parameters are selected.

Baodong Qin, Dong Zheng[4], propose a generic approach for constructing ABE with outsourced decryption from normal ABE, as long because it satisfies some further properties. Its security are often reduced to the underlying normal ABE within the selective security model by a black-box method. To avoid the disadvantage of selective security in observe, we've tendency to more propose a modified decryption outsourcing mode so our generic construction are often adapted to satisfying adaptive security. This partially solves the open drawback of constructing an ODABE theme, and its adaptive security are often reduced to the underlying ABE theme during a black-box method. Then, we present some concrete constructions that not only encompass existing ABE outsourcing schemes of Green et al., but also lead to new selectively/adaptively-secure OD-ABE schemes with more efficient transformation key generation algorithm. Finally, we use the PBC library to check the efficiency of our schemes and compare the results with some previous ones, that shows that our schemes are have lot of efficient in terms of decryption outsourcing and transformation key generation. Experimental results showed the benefits of these two key splitting methods.

Baris Celiktas, Ibrahin Alikbilek, Enver Ozedemix[5], construct a key access management theme that seamlessly transitions any hierarchical-like access policy to the digital medium.We offer a secure technique for each user of this entity to access the general public cloud from each within and outdoors the company's network. The thought of our key access management theme, that's predicated on Shamir's secret sharing formula and polynomial interpolation technique, is acceptable particularly for class-conscious structure structures. It offers a secure, flexible, and class-conscious key access mechanism for organizations utilizing mission-critical information. It additionally minimizes considerations concerning moving mission-critical information to the overall public cloud and ensures that solely users with decent approvals from identical or higher privileged users will access the key by creating use of the topological ordering of a directed graph, together with self-loop. Main overheads like public and personal storage wants area unit reduced to a tolerable level, and therefore the key derivation is computationally economical. From a security perspective, our theme is each immune to collaboration attacks and provides key identicalness security.

Biwen Chen, Libing Wu, Li Li, Kim-Kwang Ranmand Choo, Debioo He[6], propose a variant searchable encryption with parallelism and forward privacy, namely the parallel and forward private searchable public-key encryption (PFP-SPE). PFP-SPE theme achieves each the parallelism and forward privacy at the expense of slightly higher storage prices. PFP-SPE has similar search efficiency with that of some searchable symmetric encryption schemes however no key distribution drawback.

Leyou Zhang, Gongcheng Hu, Yi Mu, Fatemeh Rezaeibagha[7],proposed the traditional ciphertext-policy attribute-based encryption (CP-ABE), It provides the fine-grained access management policy for encrypted PHR data, but the access policy is additionally sent along with ciphertext expressly. However, the access policy can reveal the users' privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by concealing access policies. The experimental results show that the proposed theme achieves full security within the standard model under static assumptions by using the dual system encryption method.

Shradha Bhatia, Sunil Kumar Khatri, Ajay Vikram Singh[8],explores an improved color image security algorithm. The algorithm encrypt and decrypt the color image using the decomposition of RGB components (sieving), Pixel shuffling, RC4 cipher algorithm, image division and combining using visual cryptography to result in shares of image. The generated encrypted shares are further shared over the network.

Karthik, Chinnasamy, Deepa Lakshmi[9], discovers a hybrid technique of using both Symmetric-key and Asymmetric-key algorithm is implemented to give strong security. Our proposed technique manifest that the time of encryption is more appropriate than the existing technique.

Feddy Ronaldo, Dadet Pramadihanto, Amang Sudhasona[10], propose a hybrid cryptography that a combination of AES256, ECC, and SHA256. The projected rule is focuses on a reliable digital communication security system between drone services and server. The projected theme is economical in terms of interval therefore it'll not considerably have an effect on the realtime sensing element information from the drone. The experimental results show that the projected system reaches eighty eight.61 milliseconds to cipher and decipher messages victimization the Raspberry Fi device.

Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, J.M Eghan, Nii Narkur Quaynor[11],propose an encryption technique of securing the biometric image data collected from devices with an approach of feature based on encryption technique for securing forensic biometric image data using AES and visual cryptography method. The encryption is done by engaging visual cryptographic encryption techniques based on image shares and transposition of the share. A key is extracted from the image and then encrypted using AES before using its engagement in the encryption process. At the end of the process, it has been observed that there was no pixel expansion hence there was no loss in image quality.

Ravi Raushan Kumar Chaudhary, Kakali Chatterjee[12], proposed a new block cipher technique for the secure transmission of data from these IoT devices. This technique requires low computation load and less energy consumption. The implementation result shows that it is computationaly efficient and the memory occupation is small while the speed is considerable for generating efficient cipher.

Taranpreet Singh Ruprah, Vishal S kore, Yogesh K Mali[13], proposed a Elliptical curve cryptography technique for sending the encrypted message from one android smart phone to another android smart phone also we compare the elliptical curve cryptography with the RSA algorithm. The experimental result show that the proposed system will help us to transfer the text messages in very secure manner.

Himanshu Gupta, Nupur Sharma[14], projected a model that is consisting combination of Visual Cryptography and Steganography with the association of QR codes.A purpose of Visual Cryptography for making 2 shares within which one of the share will be turned in a clock wise direction concerning one hundred eighty degree & alternative concerning 270 degree and so we have a tendency to ar implementing Steganography by victimisation two’s complement on each the share image. once the transformation of shares into steganoimages, we have a tendency to ar changing one in every of the steganoimage into a QR code which can be unbroken secret with the user.During the verification time, the QR code are needed for the authentication of user.

M. Thangapandian, P.M. Rubesh Anand, K. Sakthidasan @ Sankaran[15], proposed a techique which aims to develop a novel key distribution and encryption mechanism namely, Quantum Key Distribution andNon-Abelian Encryption (QKD-NAE) for secure storage and access of PHR. The experimental results evaluated the performance of the QAD-NAE by using various measures and also its superiority is proved by comparing it with the existing techniques.

M. Sumathi, S. Sangeetha[16],present a Enhanced Elliptic Curve Cryptographic Technique for Protecting Sensitive Attributes. In the proposed method, the safety mechanisms are applied to sensitive attributes with the knowledge of information owner’s and inter-organization admin. Hence, security of sensitive attributes is to be enhanced with minimal storage value. High security is demanded by increased EECC algorithm. ECC yields better security through random keys, but true random key generation is a challenging task. EECC algorithm merged the pseudo random key with data owner private key and specific organization admin key. Compared to ECC algorithm EECC offers higher security with the knowledge of client and alternative organization admin.

Mukesh Kumar Sharma, Devendra Somwanshi[17], proposed a Improvement in Homomorphic Encryption Algorithm with Elliptic Curve Cryptography and OTP Technique. We have used elliptic curve cryptography algorithm for generation of keys which is having small size keys and as secure as RSA. From the results it is also demonstrated that performance is also better than the basic algorithm in terms of computation time, storage overhead and probability of attacks. In this approach we have also used OTP to secure the decryption process as well.

Wu Feng Sheng[18], explore a studying the basic thoughts of the elliptic curve encryption algorithm, an optimized method from the aspect of dynamic is designed based on elliptic curve encryption algorithm of cloud data protection technology to ensure the system running safely and efficiently, and the safety test is made in Matlab software. A implementation results show that the designed cloud data encryption technology based on ECC algorithm has high security and running speed, and it can effectively protect the security and stability of cloud platformdata.

Hangwei Li, Yi Yang, Yuanshun Dai, Shui Yu, Yong Xiang[19], propose a Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) schemes over medical cloud data. Firstly, we leverage the secure k-Nearest Neighbor (kNN) and Attribute-Based Encryption (ABE) techniques to propose a dynamic searchable symmetric encryption scheme, which can achieve two important security features, i.e., forward privacy and backward privacy which are very challenging in the area of dynamic searchable symmetric encryption. Then, it propose an enhanced scheme to solve the key sharing problem which widely exists in the kNN based searchable encryption scheme. Compared with existing proposals, this schemes are better in terms of storage, search and updating complexity. The experimental result shows that proposed scheme was very efficient in terms storage overhead, index building, trapdoor generating and query.

Shafali Ojha, Vikram rajput[20],proposed AES And MD5 Based Secure Authentication In Cloud Computing. cloud computing is one among the foremost growing field of analysis wherever many work done regarding in this field, as much as user increase over cloud security become a lot of concern there are many work done regarding in this field and all are using cryptographic technique existing technique have some disadvantages to beat these problems we have a tendency to use use authentication based AES and MD5 technique to secure data and login of user over cloud. In this paper we propose present technique of encryption and decryption for our data at the time of login however there’s no authentication provided at the given time of login. Due to only basis of trust value security isn’t provided.

3. COMPARITIVE ANALYSIS

S. No	Title	Techniques & Mechanisms	Parameter Analysis	Tools	Future Work
1	Protecting Medical Images in Cloud using Visual Cryptography Scheme	Visual Cryptography	Data Confidentiality	MATLAB R2014a	Use a lossless secret shared scheme to avoid image degradation
2	Research and Design of Cryptography Cloud Framework	Cryptography Cloud Framework	Availability analysis, Security analysis	MATLAB	Concentrate on key transfer problem in the scheduling process of cryptography resources and key storage problem in the sharing process of cryptography resource
3	A Multivariate Public Key Encryption Scheme with Equality Test	Public Key Encryption Scheme	Public key size, Private key size, Storage costs	MS SQL 6.0, windows 7	Proposed an efficient equality test encryption scheme based on bilinear pairings, which reduced the need for time-consuming hashto-point functions.

4	Generic Approach to Outsource the Decryption of Attribute-Based Encryption in Cloud Computing	Attribute-Based Encryption	Security, Key Update Time,	PBC library on a Windows 10 platform with 2.2GHz Intel Core i5-5200U CPU and 8GB Memory	Further impove to data accuracy
5	A Higher-Level Security Scheme for Key Access on Cloud Computing	Shamir's secret sharing algorithm and polynomial interpolation method	Secure, flexible, and hierarchical key access mechanism	Ubuntu 20.04.2 64-bit operation system running on Intel Core i7-7567U CPU 3.50GHZ processor.	To improve the security
6	A Parallel and Forward Private Searchable Public-Key Encryption for Cloud-Based Data Sharing	Public-Key Encryption scheme	Security, Search Efficiency,	Laptop (ThinkPad T440, 64 bits Windows 7, 4GB RAM)	Extended this work to the identity-based setting for addressing the key management problem .
7	Hidden Ciphertext Policy Attribute-Based Encryption With Fast Decryption for Personal Health Record System	CP-ABE scheme	Data verifiability, Fast decryption:	Windowsmachine with 3.40 GHz Intel(R) Core(TM) i3-3240 CPU and 4 GB ROM	In future to propose a fully hiding policy with fast encryption
8	Digital Image Security Using Visual Cryptography	RC4 ciphe algorithm, Pixel shufflin Method	Image Security	MATLAB	To decreases the memory requirement for the storage of image
9	Hybrid Cryptographic Technique Using OTP:RSA	OTP (One-time pad), Rivest, Shamir and Adleman (RSA)	Data protection	It executed in java environment	To reduce the computation speed
10	Secure Communication System of Drone Service using Hybrid Cryptography over 4G/LTE Network	AES, ECC, SHA256	Processing Time Analysis, Transmisson Time Analysis, Security Schemes Evaluation	Raspberry Pi 3, Raspberry Pi 4, cloudMQTT	In future to build a Real-Time Secure Communication System that has a smaller transmission time for lightweight devices

11	Feature Based Encryption Technique For Securing Forensic Biometric Image Data Using AES and Visual Cryptography	AES and visual cryptography method	Protect the Biometric image	MATLAB	To improve the quality of the image
12	An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System	block cipher technique (Simon, Speck, HIGHT, LEA(Low-power encryption Algorithm)	Memory occupation, Execution Time,	8 bit AVR (Arduino Uno) micro controller	In future Differential and linear cryptoanalysis of this algorithm can be performed to ensure the robustness of the cipher
13	Secure Data Transfer in Android using Elliptical Curve Cryptography	Elliptical Curve Cryptography	security in text message transfer	Java Standard Edition 7	In future, Extend it to multimedia files, banking applications, Banking related messages
14	A Model for Biometric Security using Visual Cryptography	Visual Cryptography	Security, Confidentiality, Durability	MATLAB	To provide the security by using latest cryptographic algorithm and do research with new ideas which will be beneficial for the society.
15	Quantum Key Distribution and Cryptography Mechanisms for Cloud Data Security	Quantum Key Distribution and Non-Abelian Encryption (QKD-NAE)	Computation Time, Key Generation Time,	MATLAB	To reduce the key size by using various cryptograpic technique
16	Enhanced Elliptic Curve Cryptographic Technique for Protecting Sensitive Attributes in Cloud Storage	Enhanced Elliptic Curve Cryptography, ABE (Attribute-based encryption)	Encryption Time, Decryption Time, Storage Cost, key management	MATLAB	In future work, the confidentiality and integrity is verified by dynamic public auditing system.

17	Improvement in Homomorphic Encryption Algorithm with Elliptic Curve Cryptography and OTP Technique	Diffie Hellman key exchange algorithm, Elliptic Curve Cryptography, OTP	Computation Time, Memory Consumption, Key management	MATLAB	To Reduce the communication overhead for other image types
18	Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm	ECC Algorithm	Safety performance analysis, Security encryption processing speed analysis, Storage space analysis	MATLAB	Need security for ATSM attack
19	Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data	Attribute-Based Encryption	security, Multi-keyword search	IntelR CoreTM i5-4440 CPU@ 3.10GHz processor, 8GB RAM,	To reduce the encryption time by using various algorithm
20	AES And MD5 Based Secure Authentication In Cloud Computing	AES Algorithm, MD5 Algorithm	Authentication of Data	.net environment	In future, build secure operating system so that attacks are easily not depict in cloud computing.

4. CONCLUSION

Cryptography in cloud computing is a new protected cloud computing architecture. It can offer security of information available at the system level, and allows users access to shared services conveniently and accurately. This paper reviewed algorithms, techniques used for parameter analysis used in cloud computing of an existing Cryptography mechanisms. Major papers reviewed about the Cryptography Technique based on performance analysis, computation speed, key management, Memory Consumption. Considering this survey my work will be related to provide a security on cloud data sharing by implementing CBC Techniques.

5. REFERENCES

[1] M. Marwan, A. Kartit and H. Ouahmane, "Protecting medical images in cloud using visual cryptography scheme," 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 2017, pp. 1-6, doi: 10.1109/CloudTech.2017.8284702.

[2] S. Lei, W. Zewu, Z. Kun, S. Ruichen and L. Shuai, "Research and design of cryptography cloud framework," 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2018, pp. 147-154, doi: 10.1109/ICCCBDA.2018.8386503.

[3] X. Shen, L. Wang, H. Zhu and Y. Liu, "A Multivariate Public Key Encryption Scheme With Equality Test," in *IEEE Access*, vol. 8, pp. 75463-75472, 2020, doi: 10.1109/ACCESS.2020.2988732.

[4] B. Qin and D. Zheng, "Generic Approach to Outsource the Decryption of Attribute-Based Encryption in Cloud Computing," in IEEE Access, vol. 7, pp. 42331-42342, 2019, doi: 10.1109/ACCESS.2019.2907364.

[5] B. Celiktas, I. Celikbilek and E. Ozdemir, "A Higher-Level Security Scheme for Key Access on Cloud Computing," in IEEE Access, vol. 9, pp. 107347-107359, 2021, doi: 10.1109/ACCESS.2021.3101048.

[6] B. Chen, L. Wu, L. Li, K. R. Choo and D. He, "A Parallel and Forward Private Searchable Public-Key Encryption for Cloud-Based Data Sharing," in IEEE Access, vol. 8, pp. 28009-28020, 2020, doi: 10.1109/ACCESS.2020.2971089.

[7] L. Zhang, G. Hu, Y. Mu and F. Rezaeibagha, "Hidden Ciphertext Policy Attribute-Based Encryption With Fast Decryption for Personal Health Record System," in IEEE Access, vol. 7, pp. 33202-33213, 2019, doi: 10.1109/ACCESS.2019.2902040.

[8] S. Bhatia, S. K. Khatri and A. V. Singh, "Digital Image Security Using Hybrid Visual Cryptography," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2018, pp. 570-576, doi: 10.1109/ICRITO.2018.8748622.

[9] Karthik, Chinnasamy and Deepalakshmi, "Hybrid cryptographic technique using OTP:RSA," 2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2017, pp. 1-4, doi: 10.1109/ITCOSP.2017.8303131.

[10] Febby Ronaldo, Dadet Pramadihanto, Amang Sudarsono “Secure Communication System of Drone Service using Hybrid Cryptography over 4G/LTE Network”2020 International Electronics Symposium (IES)

[11] Q. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan and N. N. Quaynor, "Feature Based Encryption Technique for Securing Forensic Biometric Image Data Using AES and Visual Cryptography," 2014 2nd International Conference on Artificial Intelligence, Modelling and Simulation, 2014, pp. 199-204, doi: 10.1109/AIMS.2014.65.

[12] R. R. K. Chaudhary and K. Chatterjee, "An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System," 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), 2020, pp. 991-995, doi: 10.1109/SPIN48934.2020.9071421.

[13] Taranpreet Singh Ruprah, Vishal S Kore, Yogesh K Mali “Secure Data Transfer in Android using Elliptical Curve Cryptography” 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)

[14] H. Gupta and N. Sharma, "A model for biometric security using visual cryptography," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2016, pp. 328-332, doi: 10.1109/ICRITO.2016.7784975.

[15] M. Thangapandiyan, P. M. Rubesh Anand and K. S. Sankaran, "Quantum Key Distribution and Cryptography Mechanisms for Cloud Data Security," 2018 International Conference on Communication and Signal Processing (ICCSP), 2018, pp. 1031-1035, doi: 10.1109/ICCSP.2018.8524298.

[16] M. Sumathi and S. Sangeetha, "Enhanced Elliptic Curve Cryptographic Technique for Protecting Sensitive Attributes in Cloud Storage," 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2018, pp. 1-5, doi: 10.1109/ICCIC.2018.8782295.

[17] M. K. Sharma and D. Somwanshi, "Improvement in Homomorphic Encryption Algorithm with Elliptic Curve Cryptography and OTP Technique," 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), 2018, pp. 1-6, doi: 10.1109/ICRAIE.2018.8710434.

[18] F. S. Wu, "Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm," 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), 2018, pp. 125-129, doi: 10.1109/ICVRIS.2018.00038.

[19] H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data," in IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484-494, 1 April-June 2020, doi:10.1109/TCC.2017.2769645

[20] 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), 2017, pp. 856-860, doi: 10.1109/I-SMAC.2017.8058300.