**LITERATURE SURVEY**

**1. A Study on Data Storage Security Issues in Cloud Computing**

**Authors: Naresh vurukonda, B.Thirumala Rao**

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centers. The Cloud service provider (CSP) should ensure integrity, availability, privacy and confidentiality but CSP is not providing reliable data services to customer and to stored customer data. This study identifies the issues related to the cloud data storage such as data breaches, data theft, and unavailability of cloud data. Finally, we are providing possible solutions to respective issues in cloud. The cloud computing architecture stores data and application software with minimal management effort and provides on demand services to customers through internet. But with cloud management customer don’t have trust worthy commitments or policies. This will lead to many security issues with data storage such as privacy, confidentiality, integrity and availability. In this study we focused on data storage security issues in cloud computing and we first provided service models of cloud, deployment models and variety of security issues in data storage in cloud environment.

**2. A Secured Cloud Security Using Elliptic Curve Cryptography**

**Authors: Dr.M.Gobi and Karthik Sundararaj**

Cloud Computing is a modern paradigm which enables utilization of pool of computing resources in the most proficient way. This emerging technology provides great opportunity in support of small and medium scale business houses to grow their business using the computing IT resources with no deployment cost. Cloud computing with well-built security has become a boon in the field of Information Technology. Cloud security is becoming a key differentiator and competitive edge between cloud providers. The prime responsibility of the cloud services provider is assuring security and integrity of

the consumer’s data. The lack of trust on data security is being the key obstacle to the IT sectors to move their data to the cloud. Lot of researches has been done to improve the performance of cloud data security. Hence cloud computing is still discovering several security issues. The high-quality cloud security can be achieved by efficient encrypting techniques. In this paper, we projected a model using Elliptic Curve Cryptography (ECC) to provide efficient data security in Cloud computing.

**3. ECC Algorithm & Security in Cloud**

**Authors: C. Nithiya, R. Sridevi**

Security in cloud computing is an evolving area in today’s world. It is subject of concern for Cloud Technology Services. One of the measures which customers can take care of is to encrypt their data before it is stored on the cloud. This work is intended towards providing security service such as confidentiality in the cloud services which use Elliptic Curve Cryptography (ECC) algorithm instead of familiar and generalized RSA for data encryption because of its advantages in terms of smaller key sizes, lower CPU time and less memory usage. Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques like RSA now in use. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security. Although ECC’s security has not been completely evaluated, it is expected to come into widespread use in various fields in the future. After comparing the RSA and ECC ciphers, the ECC has proved to involve much less overheads compared to RSA.

**4. Effective Secure Data Storage in Cloud by Using ECC Algorithm**

**Authors: S. Sridharan and A. Arokiasamy**

Cloud computing is a rising field in the information technology (IT) industry because of its performance, low cost, high availability and much more. Cloud providers offer several storage services for their users in an efficient manner. Cloud users are allowed to store their data on cloud server using cloud storage and reduce the burden of storing and retrieving in the local machine. The data leakage, lack of proper security control policy and weakness in the data entry are the main worries of the companies. So that a cloud data security models should be able to overcome all the possible issues of cloud computing, so as to provide the benefits of cloud computing and preventing the owner's data from all the risks associated. We intend to propose a secure cloud storage system ECC algorithm for encryption and decryption process. Initially, the user sends a request to the cloud server provider (CSP) for storing a file in a cloud. In this phase we will give one password to the user and verification sign also have some security level questions. Then the CSP will verify that data and accept that file and encrypt that file and stored on the cloud server. If the user wants that file means they send a request to CSP also they will send a password and send a verification signature and some security level questions after they will decrypt the file and send to the user.

**5. An Efficient Ensemble Architecture for Privacy and Security of Electronic Medical Records**

**Authors: Ömer Kasım**

Electronic medical records, one of the sensitive data, are stored in public or private cloud service providers. Cloud systems provide security with firewall and intrusion detection systems, and these systems ensure privacy with access control and end-to-end encryption. However, while sending data to the cloud system, attackers can capture the data with the help of Man in the Middle attacks and vulnerabilities of the storage systems. In the middleware architecture proposed in this study, access control protocol, key distributor and end-to-end hybrid encryption which are based on user roles were innovatively used to overcome security issues in data transmission. In this system, writing and updating requests are encrypted asymmetrically, and reading requests were encrypted symmetrically. This solution distinguishes the proposed method from previous studies. According to this solution the operating performance of the system is increased. In addition, the attacker cannot see the actual data in a cyber-attacks because the sensitive data is distributed to the users with their private keys. This result shows that the access, write and update of electronic medical records are performed with the principles of security and privacy.

**6. A New Secure Model for Data Protection over Cloud Computing**

**Authors: Amr M. Sauber, Passent M. El-Kafrawy, Amr F. Shawish, Mohamed A. Amin, and Ismail M. Hagag**

The main goal of any data storage model on the cloud is accessing data in an easy way without risking its security. A security consideration is a major aspect in any cloud data storage model to provide safety and efficiency. In this paper, we propose a secure data protection model over the cloud. The proposed model presents a solution to some security issues of cloud such as data protection from any violations and protection from a fake authorized identity user, which adversely affects the security of the cloud. This paper includes multiple issues and challenges with cloud computing that impairs security and privacy of data. It presents the threats and attacks that affect data residing in the cloud. Our proposed model provides the benefits and effectiveness of security in cloud computing such as enhancement of the encryption of data in the cloud. It provides security and scalability of data sharing for users on the cloud computing. Our model achieves the security functions over cloud computing such as identification and authentication, authorization, and encryption. Also, this model protects the system from any fake data owner who enters malicious information that may destroy the main goal of cloud services. We develop the one-time password (OTP) as a logging technique and uploading technique to protect users and data owners from any fake unauthorized access to the cloud.

**7. A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions**

**Authors: Fursan Thabit, Sharaf Alhomdy Sudhir Jagtap**

With the rapid development of distributed system technologies, one of the biggest challenges facing the digital world is ensuring the security of sensitive and confidential data during transport and storage, which are considered the most critical challenges facing cloud computing. There are many techniques to enhance data security on cloud computing storage environment. Encryption is the most significant method for data protection. Therefore, many available encryption algorithms are used to provide security, integrity, and authorized access using many methods such as DNA. However, they still have some limitations. In this paper, a novel variant of cryptography techniques is designed to improve cloud computing security by using two layers of encryption. The first layer is inspired by Shannon’s theory of diffusion and confusion by the involvement of logical operations, such as (XOR, XNOR, shifting) with split the original plaintext and key into equal parts. The second layer is inspired from structures of genetics based on the Central Dogma of Molecular Biology for cryptographic purpose through simulation of the natural processes of genetic cryptography (translation from binary to DNA bases), transcription (regeneration from DNA to mRNA), and translation (regeneration from mRNA to protein). The experimental results enhanced data security that can be used to secure applications on cloud computing. The proposed algorithm’s experimental results presented a strong security level, an apparent enhancement of cipher size and execution time compared to existing techniques widely used in cloud computing.

**8. A novel data classification-based scheme for cloud data security using various cryptographic algorithms**

**Authors: Mohd Naved Ul Haq and Narender Kumar**

Digital technologies had an effect on people's lives. The majority of these digital devices rely on cloud storage to meet their memory needs. Hundreds of thousands of images, videos, and audio files are being transferred to cloud storage. Thousands of people around the world access these media every second. Unauthorized access to these media must be avoided. One of the weak points for data breaches is the user-end encryption. This paper suggests a strategy for improving cloud data protection by combining the AES and blowfish encryption and decryption algorithms. AES-256 is used as the first layer, followed by blowfish as the second layer, in the hybrid solution. The output of the first layer is input to the second layer and the final result is analyzed. The proposed method also discusses other combined approaches such as AES with other traditional algorithms but the proposed method gives significant results compared to other approaches.

**9. A Review on Clouds Security Based Encryption and Decryption Techniques**

**Authors: Shruti Bhawsar, Kushal Joshi**

Today, large amounts of electronic data have been created, and the work of organizations that need data recovery services can suffer from various natural or man-made disasters, which can lead to huge data losses. Encryption and spatial encryption performance and average response time have been estimated based on the size of the data file. RSA encryption is often used in cloud storage. It allows cloud services to search encrypted data directly. Cloud Server provides storage and search services. To perform efficient searches, the cloud uses verification keys to maintain privacy protection or meet authentication requirements and provide equivalent proof of encrypted documents based on tokens. Most security issues are caused by people deliberately creating malicious or malicious purposes. This Paper reviews and examines some Encryption and Decryption technologies. As a result, the better solution to the symmetric key encryption and the asymmetric key encryption is provided.

**10. A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography**

**Authors: Rose Adee and Haralambos Mouratidis**

: Cloud computing is a rapidly expanding field. It allows users to access computer system resources as needed, particularly data storage and computational power, without managing them directly. This paper aims to create a data security model based on cryptography and steganography for data in cloud computing that seeks to reduce existing security and privacy concerns, such as data loss, data manipulation, and data theft. To identify the problem and determine its core cause, we studied various literature on existing cloud computing security models. This study utilizes design science research methodology. The design science research approach includes problem identification, requirements elicitation, artifact design and development, demonstration, and assessment. Design thinking and the Python programming language are used to build the artifact, and discussion about its working is represented using histograms, tables, and algorithms. This paper’s output is a fourstep data security model based on Rivest–Shamir–Adleman, Advanced Encryption Standard, and identity-based encryption algorithms alongside Least Significant Bit steganography. The four steps are data protection and security through encryption algorithms, steganography, data backup and recovery, and data sharing. This proposed approach ensures more cloud data redundancy, flexibility, efficiency, and security by protecting data confidentiality, privacy, and integrity from attackers.