Literature Review or Related work

Current research on cloud security focused on how we can enhance the security of data from hackers or vulnerability. Although concept of cloud computing security is not fresh concept in cloud security, the new problems are still continues to existent. Due to its synchronous resource sharing among all consumers cloud storage is attaining immense popularity day by day. Due to its gain access to all time nature data owners choose cloud storage over other services. Data integrity and data preservation should be authenticated for this purpose in order to enhance security of the system.

This chapter we will have the catch sight of all research work done in field of Advance Encryption Standard, ECC and Diffie-Hellman. In the subject of Advance encryption cryptography Technique, ECC, Diffie-Hellman and SHA-256 in the last decades lot of research has been done, on the basis of different metrics various cryptography algorithms have been evaluated. Using the rewarding characteristics of AES cryptography, ECC, Diffie-Hellman and SHA 256 many cryptography models were renovated which are evidenced effective in massive number of fields. The literature

Survey on cloud security provides the research work where in terms of computation speed and security AES is measure up with diverse algorithms and has been proven with effect. In the end survey comprises the former exposed hybrid AES models where AES is applied with other cryptography algorithms for instance RSA, DES, ECC, Diffie-Hellman and 3DES. Major Highlights on previous research are mentioned below.

**Shukla D.K.** et al. [[1](#_bookmark27)], studied that how AES along with ECC can increase security of the system. For distributing and managing the system excluding the trusted center Shamir secret sharing is used. Even though the proposed combined approach enhances system security, it still takes enormous computational charge as well as taking much time.

Theresults obtained by **Yahia H.S.** in [[2](#_bookmark28)] suggested that for secure cloud services some methods are used that is AES, DES, and Blowfish along with the ECC which uses the significant algorithms. To prevent conflict among bulk users These algorithms be responsible for efficiency and integrity to the data storage and provide data security for each user individually. Furthermore, the service provider is efficient and managed data accessibility appropriately. The cloud computing data services also measured the avalanche impact of plain text and block size of data.

In reference [[3](#_bookmark29)] by **Madhavi** et al., the security strong point of ECC blended with RSA by using the data over 264 bits despite the fact 256 bits of data follow the guidelines of NIST. This working of algorithms shows that compared to the RSA algorithm the ECC works more effectively as it supplies more secure services over decreased data size and for the accessibility of data contains less storage. Different platforms of JAVA used for Experimentation.

Recently, several authors [[4](#_bookmark30),[9](#_bookmark35)] have described the latest solution of ECC. To provide efficient and protected services to diverse users ECC (Elliptic curve cryptography) is used for the encryption and decryption of data. The layered method is used encryption and decryption of data. layered method is comprising of two sections. The first section for the data encryption process it holds the small partitions for the addition of the bits and the size of the keys reduces for efficient accessibility. Meanwhile, the second layer for the encryption of data. It involves of a partition of the elliptical curves. Which are used such as *P*0, *P*1, *P*2, *P*3, *P*4 . . . . . . . . . *P*n. For the encryption and decryption process these steps are used and the security of the data provided by these two layers. In the preceding techniques, security issues and data losses inaugurate. ECC is used to overcome the effect of these issues, to secure the data and prevent the interruption of the data for reasons that occur unethically. In this asymmetric cryptography technique of, data security and improvement of larger datasets can be done effortlessly to provide security services most instantly. At the same time the two operations provided by ECC to access and secure the data over cloud computing.

Another solution is described by **Selvam, J.M.** in [[10](#_bookmark36)] is Polynomial-based hashing elliptical curve cryptography (PHECC), By using the hybrid algorithm which has the implementation of polynomial-based hashing elliptical curve cryptography of cloud computing service. By using the service this technique make sure the supportive following and usage of clients/users. Security of data in cloud can be beneficial from the hybrid cloud algorithm which is suitable for the present situation and delivers high security. The elliptical curve along with the polynomial-based hashing subsequent the hybrid algorithm has provided crucial security measures to both the users and the system for efficient and enhanced facilities. As the data are encrypted and decrypted the data integrity is maintained with the help of this technique; as soon as it uploads on the cloud, using PHECC a precise hash value is assigned. Using the elliptical curve Data are encrypted and decrypted in PHECC while by using polynomial hashing and hybrid algorithms the hash value is generated. Therefore, over cloud services the integrity of data for uploading and downloading is achieved.

Hybrid algorithms for RSS along with ECC are used by **Manaa, M.E.** in research paper [[11](#_bookmark37)]. Once the data are decreased, For the digestion and signing of the message some elements are assigned to the elliptical curve authorities which are signature. Every now and then, By ECC is used for this purpose to encrypted data. The process of encryption and decryption are completed in the same fashion. Based on their excellence Hybrid algorithms analysis for RSS and ECC are done.

The result obtained by **Astuti** in [[12](#_bookmark38)] suggested that through different mediums data encryption and decryption over the transmission are secured. In that research paper The integrity, confidentiality, and integrity of the data are mentioned. For the authentication and confidentiality the technology used of the data is the Irondale encryption algorithm along with the EAP-CHAP over the internet for the usage of cloud computing services.

In different latest devices Authentication of data is essential such as IoT devices. In these storage spaces more confidential information with High-capacity data is stored, which is why authentication is essential with these devices. To perform the cryptographic operations power of processor must be high on that device. To achieve the execution of protocols and authentication of data these devices are used by Clouds [[13](#_bookmark39),[14](#_bookmark40)].

Key management proposed by **Yee Wei Law** et al. [[15](#_bookmark41)] has described a model that was made for the smart grid named after the measurement system that area has wide. Public key infrastructure is used for the authentication and the secure communication of data to implement the protocols with different devices. Through the traditional public key infrastructure also the problem can be solved.

IaaS is storage cloud that gives an adequate degree of flexibility and adaptability to the buyer associations for its storage requirements in utilizing the virtualized climate. For different administrations and models IaaS is the essential level. Factors and ward are the other two categories of installment these are on the data transmission required and the measure of capability limit required. In the cases of the massive majority, the capacity limit, which is the first prerequisite, it has numerous classes of installments that are dependent upon the limit. As such, when the complete requirement surpasses 1 TB, the expenditure of 1 GB when 1 TB does not surpassed by the entire prerequisite is not the as same as the expenditure of 1 GB [[16](#_bookmark42),[17](#_bookmark43)].

For cloud computing services privacy protection and security are discussed in [[18](#_bookmark44),[19](#_bookmark45)] are essential challenges. Meanwhile, in outsider the CSP is a non-confided, without encryption in examination of secrecy concerns we cannot accumulate crude information. In the proposed work, in cloud a capacity and solid information transmission with the help of cross breed cryptosystem is talked about. At the same time the ECC and AES are applied to improve the classification and trustworthiness of the framework, to the cloud information through which we can apply both deviated and symmetric encryption to add additional security. Consequently, a well-organized AES- and ECC-based encryption strategy deals with the expected model, which has more and is safer computational power.

**Saeed** at el. [[20](#_bookmark46)] and **Al-Dhuraibi** at el.[[21](#_bookmark47)] have demonstrated the capabilities of cryptography in distributed storage in terms of providing security. By exploring the normal cryptography techniques including AES, RSA and ECC then this was done. In any case, in the demonstration of these procedures with respect to the variations, this study provided the solution to the issue of identifying secure and an effective encryption technique. Some methods of encryption can guarantee security, yet for encryption and decryption they take quite a while. Different strategies might provide an efficient encryption, in the other way around, yet the need for security they experienced the ill effects.

The author **Hosam** at el. [[22](#_bookmark48)] introduced by utilizing public cloud innovation a configuration that depends on different key fragments that allow share touchy information and put away to the security model. Decoding motor is utilized in AES with a 256-bit encryption on the cloud to scramble the information that will be transmitted. For scrambling mass information AES has communicated incredible consequences at high paces. For information security Steganography measures are utilized. In steganography sensitive information gathers inside other information, on cloud in this way enlarging the information size to be put away. As a corollary to that the transfer speed is incremented and capacity used in cloud is diminished, this approach may not be conventional in all situations.

**Shantha** et al. [[23](#_bookmark49)] and **Varghese** et al. [[24](#_bookmark50)] have demonstrated that ECC processor possesses just 11 cuts used in 8-bit. A review was done on the duplication strategies, from which Stall, Karatsuba, and Montgomery’s individual proliferation techniques were perceived to be effective. Among the three increase strategies and the investigation of the three amplification techniques were performed, space-effective duplication strategy was picked by Karatsuba duplication. The Karatsuba augmentation approach acquires a smaller number of cuts in contrast with former strategies. Since involvement of lower request bits as of now a smaller number of cuts so decreasing for higher request bits it will be helpful.

Another latest solution described in reference paper [[25](#_bookmark51)–[27](#_bookmark52)] they introduced a cryptographic procedure two-level and a model for the enhancement of information security in cloud processing. Both uneven and symmetric encryption calculation (AES and ECC) utilizes through this model to enhance the safety measures of information in contradiction of intruders, from approaching the genuine information the model denying them, therefore respectability of the information, empowering privacy, and to perform cryptographic tasks time taken, and additional in cloud computing the trust level of clients is developing and in the cryptographic interaction the utilization of more modest keys of ECC is speeding up.

**Reference 37 made by me**

The results obtained by **Aryan** et al. [37] In this paper they demonstrated that, On Diffie-Hellman algorithm To reduce the probability of attacks, they have improved the Diffie- Hellman algorithm to a next level. By using the concept of the Diffie -Hellman algorithm they extended the Diffie –Hellman algorithm to obtain a stronger secret key and between the sender and the receiver that secret key is further exchanged for each message so that, key would be generated that is a new secret shared key. By taking the first secret key’s primitive root the additional secret key will be generated.

**Reference ECDH**

The results obtained by **P. Patil** et al. [40] demonstrated comparative analysis between several symmetric techniques and towards the end it is bring to a close that as compared to other symmetric techniques AES requires medium memory size and the strong point of the algorithm is excellent in perception of security.

Another comparison is described by **P. Prajapati** et al. [41] Accomplishes evaluation between various encryption techniques for example DES, AES, and RSA on the behalf of diverse metrics some of them are computation time and memory requirement. As a corollary to that for encryption AES require less time as compare to RSA and DSA.

The consequences find out by **P. Mahajan** et al. [42] Implemented AES, DES and RSA three cryptography techniques and on the basis of simulation time they compared their performance. The results are for encryption and decryption on different datasets has proved that AES necessitates less time.

The most fascinating methodology to this issue has been demonstrated by **Y. Wang** et al. [43] Proposed a model based on the random generation of numbers for timing evaluation. They also proposed a method to calculate consumption of time through well-known cryptography algorithms. These three algorithms are AES, RSA, and DES.

One of the first examples of cloud security is presented by **V. R. Pancholi** et al. [44] intended for AES is considered as best technique in cryptography as well as secure data storage on cloud. It also provides shield adjacent to different types of attack such as recovery attack, differential attack, square attack and key attack.

**P. Kumar** et al. [45] demonstrated that to break the security of algorithm to AES more computational time is required after accumulating additional rounds (Nr) 16. It also compared AES with another algorithm like TDES, DES, and proved that AES is faster.

**A. K. Mandal** et al. [46] a comparison study presents in this reference paper. This comparison study is done for DES and AES which concludes that if your requirement is less memory so the better algorithm is AES. It requires 10.2 MB for the identical file size and DES requires 43.3 MB, the simulation time of DES is also greater than AES.

**A. A. Hasib** et al. [47] proposed a novel hybrid approach by combining RSA and AES. Behind AES and RSA it also gave the mathematical theory. Also it covers hindrances related to computation and with the preventive measures different possible attacks.

The hybrid approach proposed by **K. Rege** et al. [48] Introduced the most interesting approach to cloud security issue a hybrid approach to secure transmissions on Bluetooth where AES keys are also encrypted by RSA and the advantages of both AES and RSA is taken by this approach as a result this hybrid approach is highly secure.

This paper presented by **R. R. Ahirwal** et al. [49] introduced an approach where for encryption and decryption of data ECC plays an important role although Diffie-Hellman key exchange is there for setting up a secure session, using the shared secret that provide security.

**A. Pourali** et al. [50] investigated an approach where for E-commerce payment by using AES and ECC a secure reproduction of SMS model is prepared. Several mobile E- commerce models have been considered and after application of AES-ECC the supreme one among them has been chosen.

**L. Wang and Q. Yang** et al. [51] suggested a system with using AES-ECC a hybrid approach which has enhanced the formation of digital signature and excellent authentication. Also in terms of versatility and flexibility the strategy has been proven good.

**N. Jha and B. Patel** et al.[52] introduced to provide the forward secrecy in web applications using HTTPS.Also they used elliptic curve cryptography along with Diffie-Hellman an unidentified key agreement protocol for forward secrecy in Google HTTPS.

**REFRENCES FROM(ARPIT GUNJAN)**

**Chauhan** et al.[53] present during communication to maintain privacy of information and confidentiality that hybrid cryptography is better approach. For strong encryption they also proposed a hybrid algorithm. They declare that there are numerous algorithms are available for cryptography but there have also certain shortcomings all of them. This Proposed algorithm is invented of two symmetric algorithm techniques known as AES and DES, with combination of these two. By using 128 bit keys proposed solution is implemented. Using java technology the proposed solution is implemented. At this point, as per requirement they provide facility to select security algorithm which may be hybrid algorithm, AES or DES. The whole work concludes that possibility is too poor on hybrid model of an algebraic attack and for encryption approach it gives strong strength.

**Shankar** et al. [54] concentrate that for encryption and decryption process RSA is one of the most common algorithms. Subsequently, for processing and task scheduling one of the most common useful algorithms is Round-robin scheduling. To extend level of security Authors proposed a technique to integrate Round robin scheduling algorithm blended with RSAA algorithm. Based on priority to generate cipher text RSA algorithm uses in this approach system. According to the priority, receiver receive message as well as decrypt that message. The probability of man-in-middle attack and timing attack are reduces in proposed method.

**Subasree** et al. [55] investigate that a group of interconnected nodes is computer network. To modify the content of packet and compromise the network security there are a number of security threats attempt. To maintain level of security the most fundamental security principle are used such as Authentication, integrity and Confidentiality. To maintain communication private and maintain security the certain security algorithms is required. Proposed algorithm integrates Dual RSA algorithm blended with Elliptic Curve Cryptography and Message Digest MD5. By using a combination of both asymmetric and symmetric cryptographic techniques for better security along with integrity this new security protocol has been invented.

**Tianfu** et al. [56] state that due to public network and huge connection the internet is one of the most hazardous communication medium. One the of essential requirement is Information protection. To achieve security during communication at present a number of security algorithms are proposed. There also have some certain good point and certain bad point in all of them. They proposed a hybrid model for enhance the strength of encryption algorithm. Proposed model is grouping of DES and AES. Both algorithms itself are very much capable for encryption as they are symmetric key technique. A strong level of security at encryption end would be given by Integration of DES and AES. With proposed solution in results a significant improvement has been observed.

**Cloud security algorithm()**

**Yahia Alemami** et al. [59**]** In this study, a set of encryption algorithms was compared in terms of data encipherment capacity, security, memory usage, and for securing cloud information from hackers to determine the optimal algorithm’s encipherment time. Encryption algorithms that compared in this paper are (advance encryption standard (AES), Blowfish, data encryption standard (DES), international data encryption algorithm (IDEA), and Rivest-Shamir-Adleman (RSA) encryption. After comparison the results show that IDEA and RSA are less secure than Blowfish, AES and DES. The least amount of memory space required by the Blowfish algorithm. The AES algorithm is faster than other algorithms , takes the least encipherment time and can encrypts a huge amount of data.

**More** et al. [60] suggested for secure cloud information a crypto framework, to cloud coordinated activities and information sharing to provide protection and additional security which integrates byte rotation encryption algorithm (BREA) and attribute-based encryption (ABE). The attributes of the ABE algorithm is by the information to be uploaded will be recognized. In determining the category of information to be enciphered the BREA will aid these attributes. After determining information type of the file the BREA will execute thre phase of encoding. These are single phase, multi phase, or hybrid phase encoding. Subsequently, the encoding of the data, to decode the encoded text the ABE will allow the user through generating a random key. In cloud-based banking systems this proposed technique has been used.

This paper is demonstrating security issues by **Sajay** et al. [61] indicated that related to cloud computing security is the fundamental issue. In the cloud, the prototypes of security are verification, confidentiality, information integrity, and information recuperation. The proposed technique, by applying an encipherment algorithm to improve the security of cloud information which is a combined algorithm, containing Blowfish encipherment and homographic encipherment, uses cryptography and Python programming to enhance the cloud security. To the main layer the homographic encipherment is applied, to the input text which is applied and is then to the second layer it is passed, which is the Blowfish encipherment layer. By utilizing encipherment algorithms the proposed algorithm provides a better stockpiling and security strategy over the cloud architecture. The consequences indicate that if the challenges of security are fixed, then in the cloud when storing data small and large enterprises will be secure.

**Goyal and Kant** et al. [62] have demonstrated a novel hybrid algorithm for protecting cloud data and in practice it used. The proposed hybrid algorithm combines AES, SHA-1 (a hashing technique), and ECC.

**Kumar and Shafi** et al.[63] it was shown that they used a modified RSA technique to enhance the security of data for cloud storage. The key limitation of this research is that RSA algorithm has been already cracked by quantum computer algorithms.

**Teng** et al. [64] aimed to by using master choreography along with column mixing to modify a AES. the Hadoop platform were used for conducted experiments.

The most effective approach to cloud security has been proposed by **Abroshan** et al.[65] aimed to combined an elliptic curve-based technique along with an enhanced Blowfish algorithm. By using the two techniques to encrypt the data the security and performance both are improved with this proposed model.

**Awan** et al. [66] proposed an improved 128 AES method and enhanced its features to accelerate the process of encryption. The improved technique of AES uses better load balancing, less power, and improved resource management and trust on the network. Nevertheless, there are still some interesting and relevant problems to be addressed.

Another solution is described in **Kumar** [67] have demonstrated a novel approach using the autonomic resource provisioning and scheduling (ARPS) framework blended with the spider monkey optimization (SMO) algorithm. The CloudSim framework was used to assessed The effectiveness of the proposed approach. In terms of processing time, cost, and energy consumption it accomplishes good results.

**Mata** et al. [68] made use of hybrid cryptographic techniques by combining AES and Belowfish in their research work. Progressively to increases the security of data storage in cloud computing introducing more complicated functions.

**Dubey** et al. [69] have demonstrated that for IoT applications to allocate the best possible resources by combining the features of two algorithms that is cuckoo search optimization (CSO), and particle swarm optimization (PSO).These are metaheuristic-based methodologies. The suggested hybrid algorithm may allocate the services more effectively That showed by simulation outcomes.

One of the first examples of hybrid model is presented in **Arpit Agrawal** [70] This research paper proposed a hybrid model to attain confidentiality by RSA algorithm, authentication by private key encryption and integrity for SHA-1 in identical manner. Algorithm would be used to develop hybrid security model are Diffie-Hellman, RSA, Private Key Encryption, SHA-1 and RC5.

The results obtained by **Saba Rehman** in [71] This paper proposed a optimized and secure scheme for data distribution despite the fact that maintaining data security and data integrity over the cloud. The proposed system primarily functions by combining the ECC and the Advanced Encryption Standard (AES) method to make sure data integrity and authentication. The experimental results showed that when compared with existing approaches the proposed approach is yields better results and efficient.

The most interesting approach to cloud security issue has been proposed by **Samiksha Sharma** [72]tothe model different variable sizes text files are taken as input. Advance encryption standard (AES) used for performed Encryption and decryption whereas for a session set up between client and server ECDH would help in securing the communication by generating key for AES. Also Diffie-Hellman provided security between client and server by established a shared secret after successful key agreement. Eventually, on the basis of different metrics analysis of proposed model is done like storage, encryption time, decryption time, correlation and avalanche effect. Proposed methodology has been proven effective in reducing the gaps exposed in the previous literature.

|  |  |  |  |
| --- | --- | --- | --- |
| Refs. | Tools/Technology | Methodology | Shortcomings |
| [1] | JAVA in Eclipse IDE | AES-ECC blended with Shamir secret key | About the private key of any user CSP does not have any information. |
| [2] | MATLAB | Comparison of different existing algorithms | For encryption large key size necessitated. |
| [3] | Euler’s Phi function | Two-layered approach | Group operations of ECC with GDLP cannot be controlled to multiplication. |
| [5] | JAVA | Polynomial-based hashing elliptical curve cryptography | The size of the encrypted messages is increased in PHECC because they have to encrypt the hash values as well. |
| [6] | PYTHON | with EAP-CHAP Irondale encryption algorithm | EAP-CHAP consumes high computational power. |
| [7] | MATLAB | WAM (Wide Area Measurement) Smart grid model | To secure communication Smart grid requires different devices of data in local area measurements. |
| [8] | XSS | Model-based approach | Smaller security layer around the security wrapper. |
| [9] | iFogSim | Point Multiplication in Hybrid approach | Less data security in cloud computing. |
| [10] | JAVA in Netbeans | Hybrid algorithm and experimental time evaluation | On cloud data of large amount is vulnerable because in cloud storage the user authentication process is very slow, so to process their authentication the largest part of users require different mediums |
| [11] | Python | Holistic Security Model (AES 256-bit) | To sniffing Data are susceptible and to cloud storage during transmission prying eyes from user. Attackers can gain access to victim’s data and can compromise cloud segmentation. |
| [12] | Verilog Programming Language | 8-bit Elliptic Curve Crypto-processor | Karatsuba multiplier is deprived of bi-linear combination so ECC-based lightweight devices are less secured because of it. The decryption process cannot be upholder by this and it has less scalability. |
| [13] | in the Kali Linux AESCrypt and OpenSSL | AESCrypt Two-layered approach | for ECC operation limited fields are available |

Different levels of security, attacks and their impact on system can be seen in Table 4.

Table 4. Security issues and system attacks [16].

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Issues** | **Attacks by Vendors** | **System Attacks** | **Impacts on System** |
| At Virtualization Level | storage Engineering is at risk by social behavior | DM attacks,VM Escape, DDoS | Interruption by system or unknowns, alteration of the system |
| At Application Level | Session Authentication policy Management | Scripting by cross-site, Injections of SQL, | Confidentiality of the system, Hijacking of the system |
| At Network Level | Misconfiguration of firewalls | DNS system, Reuse of IP and sniffing | Faults of traffic and Exposure of network |
| At Physical Level | Power control losses | Phishing and System malware | Hardware adjustment and theft |