International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 10 | Oct 2021 www.irjet.net p-ISSN: 2395-0072

An Efficient and Advance Encryption Technique to Secure Big Data Storage Problem in Cloud Computing using Support Vector Machine

Kamini[1], Prof. Avni[2]

[1]*Student Master of technology, Department of Computer Science & Engineering Himachal Pradesh Technical University Hamirpur India.*
[2]*Asst. Professor, Department of Computer science & Engineering Himachal Pradesh Technical University Hamirpur India.*

Abstract - : *Big data is large data sets which conventional processing systems are unable to analysis and handle. In the present scenario, big data is facing many challenges regarding the data storage, data theft and unauthorized access. Many researchers are concentrated on developing the security mechanism for big data storage. To overcome the above issue, this paper concentrated on developing the encryption algorithm for storing big data in the multi cloud storage. In this paper, an Efficient and Advance Encryption (EAE) technique to secure big data storage problem in cloud computing using Support Vector Machine (SVM) with Elliptical Curve Cryptography (ECC) is proposed. For the data security, ECC with SVM approach is used along with the cloud computing environment. Firstly, we perform some deployment steps to design a network with three different layers. Then, we start simulation based on the random selection of a transmitter node or user. Transmitter user need to register in cloud platform and then can communicate and this mechanism provide better security. The results obtained from experiments show that the proposed EAE technique work well compare to the state-of arts.*

Key Words: Big data, multi Cloud Environment, Security, Encryption, Decryption, Data storage, ECC, SVM , Machine Learning

1.INTRODUCTION

sere can use the services offered on the internet with the advent of cloud computing without worrying about whether they are presented or managed in such a way that customers only have to pay for the services they provide consumed, as in the case of the use of other services [1]. Cloud computing is an essential component of sophisticated computing technologies. Over the past centuries, computing ideas, computing, and architectures have evolved and strengthened [2]. Many elements are subordinate to the evolution and revolution of technology. Cloud Computing is a computing environment that moves fast as the next stage in developing and deploying the number of distributed applications [3]. To get the highest advantage from cloud computing, designers need to develop processes to optimize the use of paradigms for architecture and implementation. The evolving technology has recently awarded fresh computing models in which assets such as online apps, technology energy, transport, and network infrastructure can be distributed as internet facilities. The most cloud computation suppliers, common service computation system is inspirational characteristics for clients whose requirement for digital assets varies over the moment [4]. In contemporary data hub and cloud computing applications, this consumption is a censorious layout parameter. The electricity and energy produced by software machinery and the linked heating unit are a significant component of these energy costs and high carbon emissions [5]. The entire cloud framework is divided into three subparts namely; Service customer, cloud specific infrastructure, supporting infrastructure as depicted by the blue, yellow and the orange color respectively in Fig. 1.

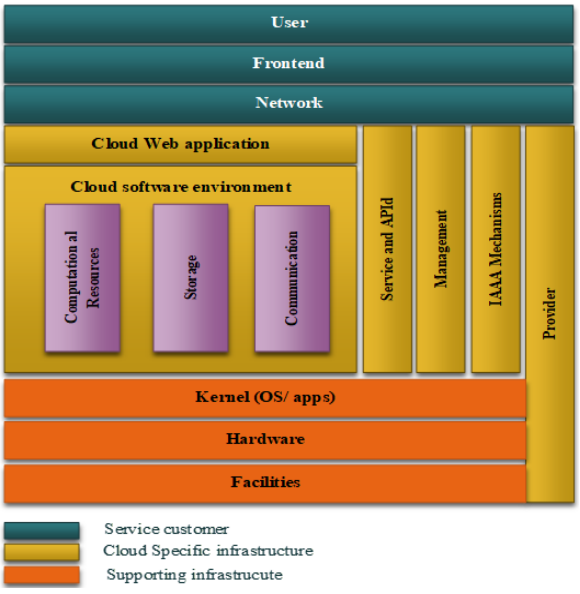


Fig. 1: Cloud Computing Framework

Cloud computing offers multiple facilities according to the user's requirements. Cloud clients such as web browsers, portable apps, thin clients, terminal emulators, thick clients, etc. use these facilities on a pay-per-use model basis.

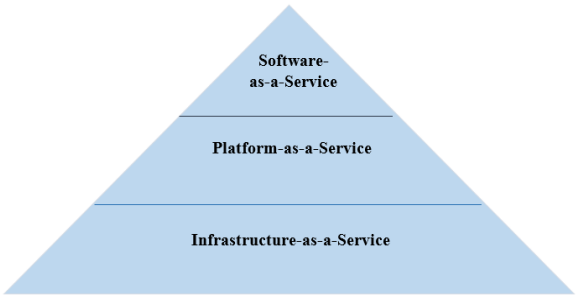


Fig. 2: Layer of Cloud Computing

The facilities are classified as hardware, infrastructure, and server as a service. These facilities are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) as shown in Fig. 2 but all faces the security issues for big data environment. Today, lots of cloud services is depending upon the security and the required for big data storage. These are some of the most important potential data storage issues you'll need to consider:

- *Infrastructure*
- *Cost*
- *Security*
- *Corruption*
- *Scale*
- *UI and accessibility*
- *Compatibility*

Data needs a place to rest, the same way objects need a shelf or container; data must occupy space and also data to be secure. For this prospective, we develop an efficient and advance encryption technique to secure big data storage problem in cloud computing using Support Vector Machine (SVM). Here, the concept of Elliptic-Curve Cryptography (ECC) is used to secure the big data storage. Because, ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields and helps to reduce the encryption decryption time of the system and also provide better security compare to the other with same size of key. The main contributions in this research is listed below:

- Firstly, we presents a brief survey on existing encryption framework for securing big data storage in multi-cloud environment to find out the gaps.
- We proposed an ECC encryption mechanism with cloud environment to solve the big data storage problem.
- To train the proposed frame work, the concept of SVM as machine learning mechanism is used.
- At the last of article, an experimental analysis and comparison of proposed framework with state-of-art works is performed in terms of running time, throughput and avalanche effect.

The rest of research article is systematized as follows. Section 2 describes the survey of existing work and Section 3 describes the methodology. The experiment results and analysis of the proposed framework are explained in Section 4, where, Section 5 explains the conclusion with future possibilities of the research.

2. LITERATURE STUDY

This section of research article illustrates the state-of-art related to the proposed system to identify the challenging factors and existing model's problems. In 2020, ***G Viswanath, and PV Krishna*** had developed a hybrid framework for encryption for securing big data storage in multi-cloud environment. In these days, big data is facing many challenges regarding the data storage, data theft and unauthorized access. To overcome the above issue, authors in this paper concentrated on developing the encryption algorithm for storing big data in the multi cloud storage. The multi cloud storage environment permits the user to store the data in to different cloud storage services. Main aims of authors to develop the secure framework which restricts the insider attacks. The proposed framework contains data uploading, slicing, indexing, encryption, distribution, decryption, retrieval and merging process. The hybrid encryption algorithm was developed to provide the security to the big data before storing it in to the multi cloud. The Simulation analysis is carried with real time cloud storage environments. The proposed algorithm recorded around 2630 KB/S for the encryption process. The results prove the superiority of the proposed algorithm compared to the bench mark algorithms [6]. ***R Hassan et al.*** in 2020 also conducted a research for data encryption based on matrix computations. The proposed solution represents a very strong key since the number of different variants of positive definite matrices of order 8 is huge. In the additional testing of the quality of the random matrix generated, they can conclude that the results of our analysis satisfy the defined strict requirements. This proposed MP encryption method can be applied effectively in the encryption and decryption of images in multi-party communications. In the experimental part of this paper, we give a comparison of encryption methods between machine learning methods. Machine learning algorithms could be compared by achieved results of classification concentrating on classes. In a comparative analysis, they give results of classifying of AES algorithm and proposed encryption method based on Moore–Penrose inverse [7]. In 2021, ***D Suresha et al.*** proposed an enhancing data

protection in cloud computing using key derivation based on cryptographic technique. This paper has proposed a technique to enhance the data protection using key derivation based encryption technique. The proposed mechanism provides confidentiality, authentication and modification for the data stored in cloud. To provide data protection, a mechanism is designed to derive three separate secret keys from a single master key and each key is used for specific operation. The experimental results show that, the proposed method uses lower computational costs, while deriving the secret keys. The scheme also enhances data security by increasing the size of the keys and restricts hackers in cracking the secret keys [8]. ***B. Arputhamary, and A. Benita*** in 2020, developed a hybrid encryption of big data security using improved elliptic curve cryptography. A hybrid cryptographic technique is proposed in this paper to enhance data protection during network transmission, and its implementation an d results are published. The proposed secure cryptographic technique promises to use the Enhanced ECC and AES technologies to include the highly secure cypher generation technique. Using JAVA, the implementation of the proposed technique is given and its efficiency in terms of space and time complexity is calculated and compared with conventional ECC cryptography. During comparative performance analysis, the proposed cryptographic technique established the successful and enhanced cypher text. Simulation results shows that AES algorithm is best for authentication and ECC algorithm used for security has better performance than other techniques. Since ECC has not any known security weak points till now, it can be considered as an excellent standard encryption algorithm. The experimental results reveal that the proposed method offers better performance over previous work [9].

3. PROPOSED MODEL

In this chapter, methodology of the proposed "an Efficient and Advance Encryption (EAE) technique to secure big data storage problem in cloud computing using SVM." is explained. The procedural steps of proposed system are defined as follows:

Proposed EAE simulator: Firstly design simulator for the simulation of proposed EAE system using the hybridization of ECC and SVM in cloud computing environment with the help of Graphical User Interface (GUI) in MATLAB 2016a or higher version software and it is shown in the Fig. 3.

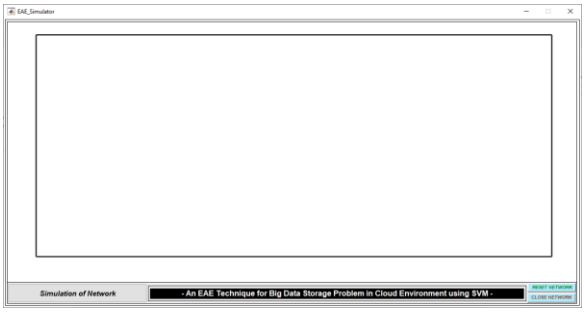


Fig 3: EAE Simulator with Area=1000m²

In the above figure, developed EAE system is shown and a push button is insert left side for the simulation of the network according to the rounds. Here, two more button is inserted named as RESET NETWORK and CLOSE NETWORK. RESET NETWORK button is used for the complete refreshment of the simulator and CLOSE NETWORK button is used to close the network. After that, total area of simulation is divided into three layers named as Layer 0, Layer 1 and Layer 2. In the Fig. 4, division of entire network into multiple layers is shown with blue color line and each line is named as the layer 0, 1 and 2.

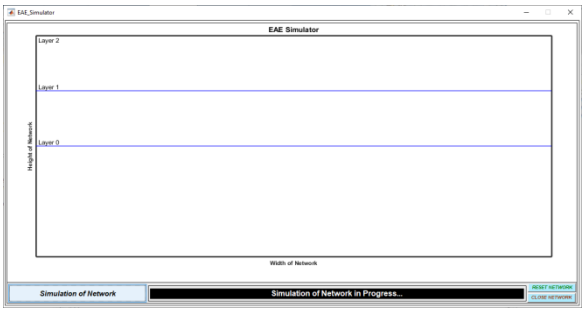


Fig 4: Division of EAE Simulator

Deployment of users as nodes in the simulator: After the EAE simulator designing, we deploy sensor nodes within the simulation area that is shown in the Fig. 5 after the network division into layers.

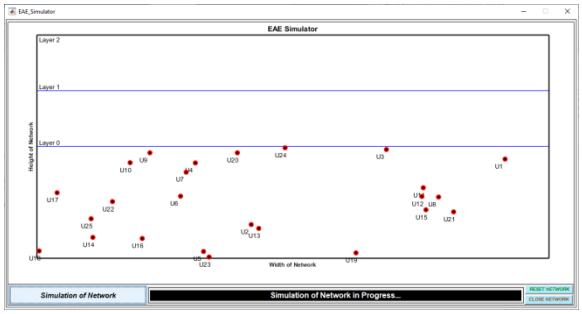


Fig 5: Users as Nodes Deployments in Simulator

After the deployment of sensor nodes in the network, we initially provides some basic parameters to each node's coverage area, where coverage area of sensor node is

calculated using the 25% of entire network area. To implement the proposed methodology some basic configurations are required with MATLAB software and hardware. In the below Fig. 6, the connectivity of each sensor nodes with the Control Unit (CU) of Cloud Computing Environment is shown. So, we can say that, in the layer 0 basic action is performed and all deployed sensor nodes sensed the data communicate with the CU for further processing in layer 1.

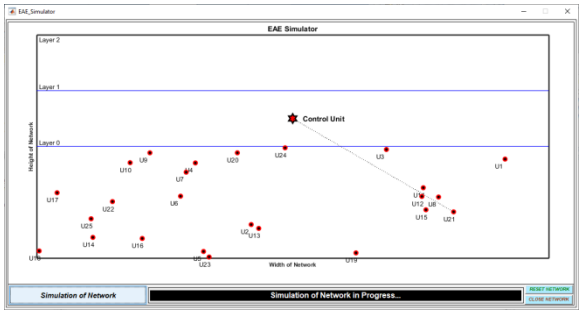


Fig 6: Connectivity of Sensor Nodes with CU

In the above figure, dotted black color line represents the conetivity of sensor nodes with CU and due to unstbale visualization, only one connection is shown and all reamining are eliminated automatically. After that, we follow a assumption to be a tramitter sensor node that is randomly.

Based on the above assumption, a sensro nodes are select ed as tranmitter nodes namsed as U20. Transmitter sensor node or user are marked with green color and named as T_X Node. After that, each transmitter sensor nodes sensed the data and tramitted to the CU for future computing in CU or fog computiing environmnet that helps to minimize the network simulation time and maximize the network utilization. At the CU side, all data are anaylzed and validate for further processing toward the cloud environment and to upload the data on cloud user should have a valid registration ID otherwise need to sign up on cloud patform.

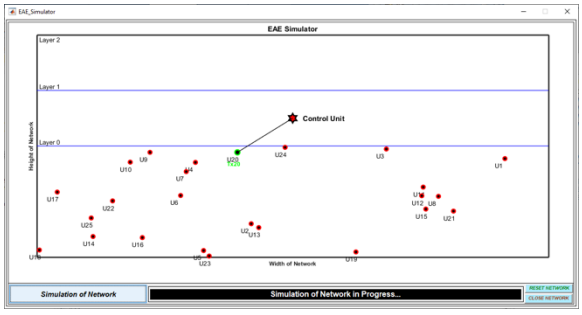


Fig 7: Transmitter Sensor Nodes in EAE System

When sensed data is processed by the CU or cloud computing environment user need to select a valid choice for data uploading on cloud to manage the EAE system sucsefully.

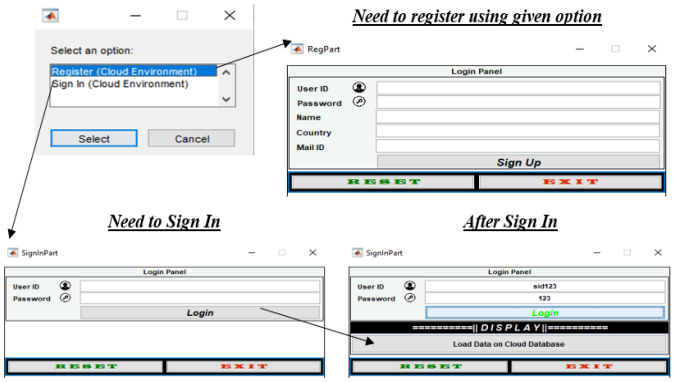


Fig 8: User Validation and Verification in cloud

4. RESULTS AND ANALYSIS

We have discussed the achieved result of proposed an efficient and advance encryption technique to secure big data storage problem in cloud computing using SVM as a machine learning technique and compare with existing work by ***G Viswanath, and PV Krishna*** [6] in terms of encryption time, decryption time, and throughput for both scenario. Firstly, we evaluated the results for single iteration in MATLAB and shown in the below Fig. 9.

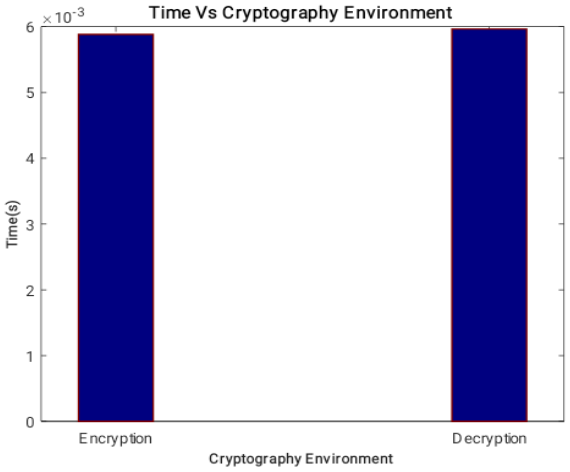


Fig 9: Encryption-Decryption Time

Fig. 9 illustrated the obtained encryption and decrption time for the proposed system using ECC with SVM. We clearly observed that the encryption-decryption time of proposed an efficient and advance encryption technique to secure big data storage problem in cloud computing using SVM is less.

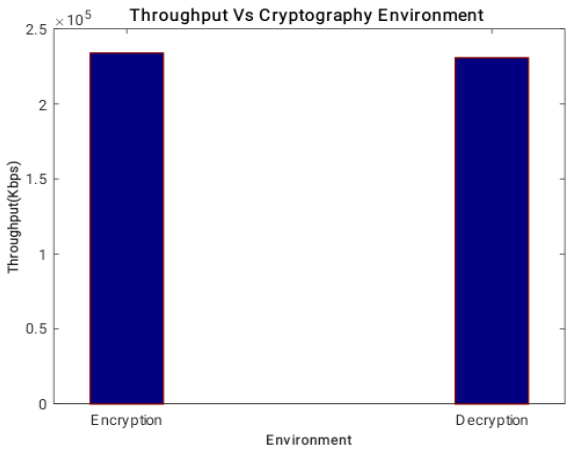
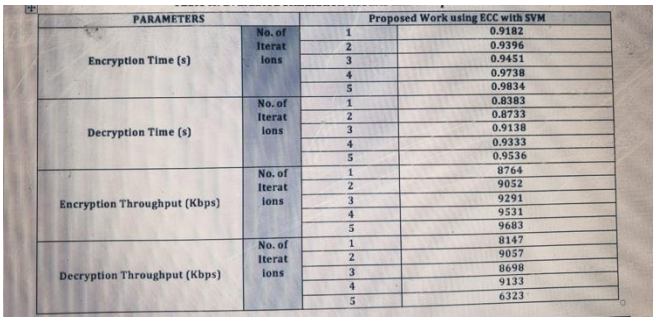


Fig 10: Throughput

Fig.10 illustrated the obtained throughput for the proposed system using ECC with SVM. We clearly observed that the throughput of proposed an efficient and advance encryption technique to secure big data storage problem in cloud computing using SVM is better for sample simulation. But , to validate the efficiency of the proposed an efficient and advance encryption technique to secure big data storage problem in cloud computing using ECC with SVM, we compare the result with existing work. Below table I represents the experiment result for the proposed system for ten iterations.



PARAMETERS		Proposed Work using ECC with SVM	
Encryption Time (s)	No. of Iterations	1	0.9182
		2	0.9396
		3	0.9451
		4	0.9738
		5	0.9834
Decryption Time (s)	No. of Iterations	1	0.8383
		2	0.8733
		3	0.9138
		4	0.9333
		5	0.9536
Encryption Throughput (Kbps)	No. of Iterations	1	8764
		2	9052
		3	9291
		4	9531
		5	9683
Decryption Throughput (Kbps)	No. of Iterations	1	8147
		2	9057
		3	8698
		4	9133
		5	6323

Fig 11: Evaluated Simulation Results and comparison

The simulation results evaluation is shown in the above fig 11, but to validate the proposed system, we need to compare with the existing work scenario. So, we compare the proposed model efficiency with work presented by the by ***G Viswanath, and PV Krishna*** [6] in terms of accuracy in table 1.

Parameter	proposed	GViswanath	PVKrishna
Encryption time(s)	**0.95202**	**1.81**	**1.81**
Decryption time(s)	**0.90246**	**1.94**	**1.94**

Table 1. Comparison of system

Encryption Throughput (Kbps)	**9264.20**	**2285**
Decryption Throughput (Kbps)	**8271.60**	**2264**

Table 2. Comparison

Above Table II shows the comparison of proposed an efficient and advance encryption technique to secure big data storage problem in cloud computing using ECC with SVM as a machine learning with existing work by ***G Viswanath, and PV Krishna*** [6]***,*** in 2020. The effectiveness of proposed system is clearly shown in the table and for better representation, their graphs are shown in the Fig. 11

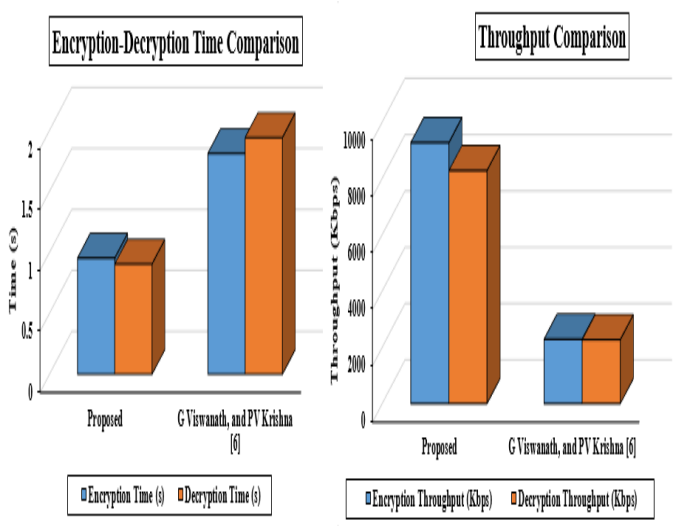


Fig 11 comparison of system

Above Fig. 11 represents the comparison of proposed system and with ***G Viswanath, and PV Krishna*** [6] on the basis of Encryption Time (s), Decryption Time (s), Encryption Throughput (Kbps) and Decryption Throughput (Kbps) as a performance parameters. The significant increase in throughput is recorded from existing work and the conclusion of the proposed work is given in the below section of this article.

5. CONCLUSUION AND FUTUR WORK

In this paper, an efficient and advance encryption technique to secure big data storage problem in cloud computing using ECC with SVM as a machine learning. Here, the concept of ECC along with the SVM is used to train the system that helps to provide the better throughput and encryption-decryption time of the system. Here, SVM helps to select a set of appropriate date set from the uploaded file or selected file by the users or nodes and then pass to ECC as an input data that helps to achieved better training for the encryption and

decryption. Because, we know that the encryption time is directly proportional to the system over all throughput. Form the experimental analysis, we observed that the Encryption Time (s), Decryption Time (s), Encryption Throughput (Kbps) and Decryption Throughput (Kbps) of proposed system is better than the existing work by ***G Viswanath, and PV Krishna*** [6] in terms of performance parameters. The results have shown that the proposed model has outperformed state-of-the-art methods on performance parameters in terms of Encryption Time (s), Decryption Time (s), Encryption Throughput (Kbps) and Decryption Throughput (Kbps). In future here can use ECC algorithm for securing data as well as audio and video data. Because, in the area of security, research area of speech is very wide. The Android platform of Smartphones is a powerful platform and is used in 80% of Smartphones today. The sensors that come with the mobile devices further give a context to cloud applications and opens up a new set of possibilities.

References

[1]. Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Khan SU (2015) The rise of "big data" on cloud computing: review and open research issues. Inf Syst 47:98–115

[2]. AlZain, MA. Eric P, Ben S, James AT (2012) Cloud computing security: from single to multi-clouds. In: 2012 45th Hawaii international conference on system sciences. IEEE, pp 5490–5499

[3]. Fu Z, Sun X, Liu Q, Zhou L, Shu J (2015) Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Trans Commun 98(1):190–200

[4]. Li R, Xu Z, Kang W, Yow KC, Xu CZ (2014) efficient multi-keyword ranked query over encrypted data in cloud computing. Future Gener Comput Syst 30:179–190

[5]. Xia Z, Wang X, Sun X, Wang Q (2015) a secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distrib Syst 27(2):340–352.

[6]. Viswanath, G., & Krishna, P. V. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, 14(2), 691-698.

[7]. Hassan, R., Pepic, S., Saracevic, M., Ahmad, K., & Tasic, M. (2020). A Novel Approach to Data Encryption Based on Matrix Computations. Comput. Mater. Contin, 66, 1139-1153.

[8]. Suresha, D., & Karibasappa, K. (2021, April). Enhancing Data Protection in Cloud Computing using Key Derivation based on Cryptographic Technique. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 291-299). IEEE.

[9]. Arputhamary, B., & Benita, A. (2020). Hybrid encryption of big data security using improved elliptic curve cryptography.

[10]. Haseeb, K., Saba, T., Rehman, A., Ahmed, I., & Lloret, J. Efficient data uncertainty management for health industrial internet of things using machine learning. International Journal of Communication Systems, e4948.

[11]. Pachala, S., Rupa, C., & Sumalatha, L. (2021). An improved security and privacy management system for data in multi-cloud environments using a hybrid approach. Evolutionary Intelligence, 14(2), 1117-1133.

[12]. Sonia, P., & Malika, R. (2021). A Hybrid Cloud Security Model for Securing Data on Cloud.

[13]. Kaliyamoorthy, P., & Ramalingam, A. C. (2021). GM-NAINO: Global Mutation based Novel Artificial Immune Network Optimization for Enhancing Data Security in Public Cloud Storage System

[14]. Prakash, V., Singh, A. V., & Khatri, S. K. (2019, June). A New Model of Light Weight Hybrid Cryptography for Internet of Things. In 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 282-285). IEEE.

[15]. Izhar, S., Kaushal, A., Fatima, R., & Qadeer, M. A. (2017, November). Enhancement in data security using cryptography and compression. In 2017 7th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 212-215). IEEE.

[16]. Thangapandiyan, M., Anand, P. R., & Sankaran, K. S. (2018, April). Enhanced cloud security implementation using modified ECC algorithm. In 2018 International Conference on Communication and Signal Processing (ICCSP) (pp. 1019-1022). IEEE.