Securing Web Application Data in Cloud Environment: A Comprehensive Review

[1]R.S.Kanakasabapathi, [2]Dr. J.E.Judith

[1]Research scholar, [1]Department of Computer applications, [2]Associate Professor, [2]Department of Computer science and engineering, [1,2]Noorul Islam college of higher education, Kumarakoil, India.

[1]kanakasabapathi2420@gmail.com

Abstract In the corporate environment, cloud computing plays a very important role in education and the Internet, which is accessible to individual users. Data security plays an important role in today's world. In the IT environment, data security and data protection prevail in areas such as government, industry and commerce to ensure data security in the future. As new data security challenges emerge in the cloud, more attention is paid to the confidentiality, reliability, and integrity of data. This study provides an overview of the results of cloud computing security research. For this study, we have collected over 50 articles from industry standard journals on this topic, including Springer, IEEE, Elsevier, and Taylor Francis. Each research report describes several methods for improving cloud security using modern technologies.

Keywords: Cloud computing, security, standard journals, algorithms.

I. INTRODUCTION

Distributed calculation is one of the most popular mechanical points of the day. It has grown to have a wide range of impact on data innovation, business, improved planning, and information storage. Performance enhancement is a key impact. This increase in performance is not due to the development of individual equipment, programming, etc [1], [2], [3]. The various components of a distributed computing system include front-to-back and cloud management, such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service. -A availability and internet access. External cell phones, cell phones that provide access to a distributed processing system. Performance, virtual machines and security systems lag behind. Each terminal is connected via an internet association. If the information is stored in the cloud, there is no problem in losing it. When information is stored in the cloud, various duplicates or duplicates of our information will be created and shared among employees.

Protecting the threat of cloud usage means making the information available to an un-authorized person [4]. Cloud-based resource sharing poses new security challenges, especially with regard to the classification of downloaded information [6]. Conventional cloud formats ensure the confidentiality of information by encrypting the information, isolating the hypervisor during the provision of visitors from the virtual machines [7]. Encryption of information readiness is the best way to solve the problem of cyber security of the cloud site; the recognizable evidence of the recipient will certainly confirm the information and their accuracy and will ensure the security and reliability of the application information [8], [9], [10]. These security measures are used to protect information, comply with legal requirements, ensure customer protection, and develop customer inspection rules for individual customers.

II. APPLICATIONS OF CLOUD COMPUTING IN VARIOUS FIELDS

In-depth analysis has shown that the typical client always runs four cloud applications, controlling four. In addition, the survey found that 41% of organizations openly hide the heavy burden. As our core load shifts to the cloud, distributed computing security is gradually monitored. This figure is also confirmed in the Forbes 2017 report, which shows that 80% of IT financial plans will be spent within 15 months to achieve the goal of the cloud, that 49% of organizations will delay cloud operations [11], [12], [13].

Cloud computing in medical field: The cloud system improves compatibility, as everything can be made easier in one place. Thus, the specialist can enter the test, call the laboratory and quickly update the patient record in a completely independent section. Distributed calculation can be useful for ordinary professionals.

Cloud computing in business: Cloud-based administrative programmers, application managers, and others can use these administrative tools through the web interface, which limits the problem from a large, powerful database.

Cloud computing in education: Networking paves the way for better learning, communication and collaboration in learning. In addition, it offers a workspace programming

DOI : 10.35291/2454-9150.2020.0660

environment that limits hardware issues. One of the advantages of distributed processing is that an external organization can be more complex in terms of monitoring individual information.

Cloud computing in IT sector: According to IDC, the global transactions of the Grid Computing administration in 2010 exceeded $ 21.5 billion, and it is projected that from 2015 they will amount to $ 72.9 billion. Many of them are crossroads, more reliable. "They are gradually enabling the creation of cloud systems that will focus on the investment, affordability, and cost-effectiveness of management."

III. SECURITY NEEDS IN CLOUD COMPUTING ENVIRONMENT

From a cloud provider, security requires resources and High cost. Ignore the security of distributed cyber innovation endangers natural benefits. Security Risks Become More Difficult Distributed Computing Is More Needed Than Necessary [14]. There are different methods to improve security in different computerized learning environments procedures that can aim at information security, for example, personality cloud management, coding, steganography. [15] We emphasize guarantees that confidentiality, honesty, integrity, security and quality issues are protected.

Authentication To avoid data theft, confirmation is required to establish a connection between the two devices by transferring some open private keys through the center.

Integrity: Matching allows you to identify changes in the message by the transmission location.

Confidentiality: guaranteed that information within the device avoids unconfirmed components.

IV. ANALYSIS OF CLOUD SECURITY: A DETAILED REVIEW

Many scholars have discussed cyber security, such as the validity of information and weaknesses in control and regulation. A lot of research has been done on cloud security. Some of these works are explored here.

Distribution calculation refers to the IT industry embedded in the remote server economy that uses the Internet to provide information and programming. The regular server farms in these areas are very large, and often serious. Likewise, ensuring the security of information mining is a major challenge. It is often possible to maintain the confidentiality of information sources while removing interfering documents. In fact, the exchange material cannot be taught on any site. With such a horse, Hammami *et al*. [16] suggested a unified approach to eliminate closed loops as often as possible in the circulatory system. The security of the website information depends on the encryption of data mining. Exhibits Exhibitions by Exhibition Surveys show that our device requires minimal matching, including computational inclusion. It can guarantee the certainty of the information, verify the truthfulness of the information and guarantee the greatest possible knowledge of the movement of information.

In many applications, context labels are associated with enhancement. Calculating a contractual arrangement assumes, for example, that there is only one name, which may be inappropriate in a variety of contexts. Learning different labels is like becoming familiar with labels associated with various labels without a single label. Many multidisciplinary training methods have been proposed today, and unfortunately, not all existing naming methods address the problem of providing data provided on specific occasions. Liu, Y. *et al*. [17] a program is specified for the secure behavior of various encrypted information signals in the cloud. Our products are ideal for distributing multiple external resource labels to cloud employees, meaningfully only for customer referral information asset owners. From a hypothetical information perspective, product information owners can provide users with information security information. Since cloud workers may not be familiar with approaching some valuable information, they can describe the results for different labels. In addition to the complexity of the inclusion figures, the inclusion of correspondence is broken down into details. We conduct stimulation tests to evaluate the computation season of our specific company.

Cloud-designed distribution storage administrations if they wait for information to be valid, reed when hanging or populating information on a distributed computer. However, this poses a number of new information security challenges. The main domain is to ensure that characters are stored in a normal cryptographic environment. It's a problem with the keys. Huang, Q. *et al*. [18] Global Data Security Partnership Property Based Encryption (ABE) introduced code for applying quality-based markup (ABS). To lose responsibility for the management property of basalt, our program uses a different imaging tool which relies on another equivalent line-based code (HABE). What's more, the fractional mark replaces the venture encryption signature, which replaces the vast majority of the preparing usefulness for the client with the cloud specialist provider. Security Analysis Performance examination shows that our framework is secure and productive.

The Health Information Technology for Economic and clinical Health (HITECH) Act 2009 advance the utilization of electronic wellbeing records. EHR improves information access, streamlines refreshing PC information and permits email messages between sellers. Distributed computing offers an assortment of administrations to the medical services division by putting away information in the cloud. Execution, accessibility and security are the three principle highlights of the cloud. In this way, proficient homomorphic cryptographic calculations are required. I.

DOI : 10.35291/2454-9150.2020.0660

Venkatapurvaja *et al*. [19] have clarified the proficient homomorphic encryption strategy for scrambling clinical pictures and performing helpful capacities without abusing secrecy.

As organization correspondence, its innovations and the telecare clinical data framework (TMIS) become progressively famous, specialists treat patients without going to medical clinic. Utilization of cell phones, remote organizations and cloud-based design; Patients can gather their physiological data and transfer it to the cloud by means of their cell phones. A licensed specialist gives online help to patients whenever, anyplace. Moreover, DMIS ensures tolerant security and information assurance in correspondence and is perceived by all members before assessing this framework. All the more as of late, TMIS has been furnished with cloud help verification and information security. They accepted their arrangement was resistant to known protection and security highlights. Kumar, V. *et al*. [20] The amendment of the validation convention uncovered that message verification fizzled during the stacking stage, that the meeting key was unrealistic during the stacking period of the wellbeing community and that different security existed, for example, the assault on portrayal, the patient's namelessness and the patient's incapacity. Sign in while tolerant information is stacking. The convention has additionally improved in a comparable setting. The proposed convention against moderate assaults expects to shield the patient from namelessness, reprisal, security properties of known keys, information protection, information protection, message verification, security assaults, duplicating, meeting key security and patient access. Convention offered with related conventions in a similar cloud-based TMIS. The proposed convention guarantees all attractive security prerequisites and oversees execution against preparing and correspondence costs for TMIS cloud uphold.

The usage of distributed computing improves the different prospects with which web specialist co-ops can meet various necessities. Nonetheless, information security and insurance has become a significant issue in controlling many cloud applications. One of the primary issues with information security and insurance is the way that cloud administrators can get to private information. This issue extraordinarily builds client dread and diminishes the utilization of distributed computing in numerous divisions, for example, money and government organizations. Li, Y. *et al*. [21] created based on this necessity and offers a clever cryptographic methodology that doesn't permit cloud specialist organizations to get to incomplete information legitimately. The proposed approach isolates the document and stores information independently on appropriated cloud workers. Another methodology is to decide if information parcels should be part to abbreviate execution times. The SA-EDS (Security-Aware Efficient Distributed Storage) venture model of the proposed venture is essentially upheld by our proposed strategies, including the elective Alternative Data Distribution (AD2) calculation, the effective Secure Efficient Data Distributions (SED2) and productive information disarray (EDCon) calculation. Our test appraisals assess both security and execution, clarifying that our methodology can viably ensure against significant cloud dangers and that satisfactory preparing time is required.

Distributed computing permits you to store and oversee a lot of information. It gives adaptability to get to information whenever, anyplace. Lately, cloud information stockpiling has gotten progressively mainstream among organizations and private clients. Notwithstanding, the cloud is pulling in increasingly more consideration, yet there are worries about information security, information security, dependability and usefulness. To tackle these issues, information encryption in the cloud is upheld. Encryption keeps unapproved clients from getting to information before the information is transferred to the cloud. Various encryption calculations have been created to ensure the information put away in the cloud. Sohal *et al*. [22] have introduced a multi-symmetric key cryptography strategy dependent on DNA encryption. We have completely planned our methodology, yet additionally contrasted it and simultaneous keys (DNA, AES, DES and Blowfish) with existing techniques. Test results show that our proposed calculation beats these conventional calculations regarding robotic content size, encryption time and execution. Subsequently, the proposed new innovation is more productive and offers better execution.

Proprietors of versatile wellbeing administrations and gadgets regularly share their mHealth information with doctors, specialists, experts, and wellbeing experts. Notwithstanding, for security reasons, they by and large like to impart a specific measure of data to every beneficiary dependent on their inclinations. Greene, E *et al*. [23] has presented a Share Health, an adaptable, usable and reasonable framework that permits mHealth information proprietors to set admittance control arrangements and scramble them so just gatherings with suitable consents can encode information. The plan and usage of this framework model makes three commitments: (1) they use access control estimates executed by encryption for information dependent on streams (explicitly mHealth). (2) They perceive the transience of mHealth information streams and backing fractional admittance to all and (3) can be applied to a wide assortment of mHealth gathered information by producer and gadget explicit. Eliminate the mHealth information wells and execute the last strategy for safe end utilities and gadgets.

Duplicating IT information is a significant procedure to improve capacity execution in distributed computing. By referring to garbage documents in a solitary duplicate, cloud specialist organizations fundamentally diminish extra

DOI : 10.35291/2454-9150.2020.0660

room and information move costs. In spite of the fact that the conventional waiver approach is broadly acknowledged, there is a high danger of information protection misfortune because of the presence of distributed computing information stockpiling models. To take care of this issue in distributed storage, Fan, Y., *et al.* [24] have examined a safe T-duplicate plan dependent on a confided in execution climate (TEE) was proposed. Each cloud client is doled out a lot of offers. D-duplicate is just conceivable if cloud clients have the correct offer. Also, our program improves the cryptography implanted in client rights and depends on TEE to give secure catchphrase the board, upgrading the capacity of these digital currencies to counter specific assaults of plaintext and ciphertext assaults chose. Security Scan Data demonstrates that our program is secure to help examine duplicating and to ensure the privacy of touchy information. What's more, we actualized a model of our task and assessed the exhibition of our model. Experience shows that the overhead expenses of our task are commonsense in sensible settings.

Electronic wellbeing cloud frameworks are generally utilized today. In any case, the security of these frameworks requires more regard for quiet wellbeing data. A few conventions have been proposed to ensure the e-Health cloud framework, yet a considerable lot of them utilize customary PKI foundation to execute cryptographic calculations. This is exhausting on the grounds that all clients have their own public/private keys and need to recollect them. Personality based encryption (IBE) is an essential cryptographic component that utilizes your character data (for instance, your email address) as a public key. The public key is thusly verifiably perceived and the administration of testaments is improved. The new intermediary encryption is another essential cryptographic component that expects to change over the ciphertext of Representative An into another ciphertext, which is spoken to by delegatee B. Wang, X. A. *et al.* [25] have different personality related cryptographic procedures have been depicted to secure the eHealth framework, including new IPE programs and new character based intermediary re-encryption (IPPRE) programs. The outcomes show that our IPPRE program is valuable for re-encryption, which is utilized to accomplish ease use of the cloud.

Distributed computing is a developing data innovation that utilizes the Internet and focal media transmission workers to store information and applications. With distributed computing, clients can get to information base assets from anyplace on the Internet without agonizing over overseeing genuine assets. This idea can be applied to all divisions, including the wellbeing segment. In such circumstances, information handling and its successful examinations from the cloud are fundamental as information security is classified. Thus, the protection and security of the data framework is at high danger because of security assaults Known Plain content assault (KPA) and Cipher Text assault (CPA). This article portrays the way to deal with information assurance through the information recuperation cycle to address these issues, information recuperation and wellbeing information security. Likewise, numerous analysts have proposed upgrades in the reclamation cycle since it lessens exactness. The answers for this emergency, Annie Alphonsa, M et al. [26] have explored a mixture calculation called Grasshopper Optimization with Genetic Algorithm (GOAGA) for the information sanitization and recreation measure. Moreover, the presentation of this cross breed approach is tantamount to other conventional methodologies as far as refinement and remaking, generally speaking investigation, insights and key affectability, hence approving the administration of the serious methodology.

The capacity and preparing abilities of cell phones control the capacity to trade records between cell phones and public mists. Securing public mists additionally increments saw hazard. Private mists are an effective stage and a client can be found as a solid outsider to improve the security level when utilizing a document from public mists. Yang, L *et al.* [27] has been new program called File Remotely keyed Encryption and Data Protection (FREDP) has been proposed. The undertaking includes three-route correspondence between the cell phone, private mists and public mists. Private mists share the encoded text record with the public cloud until the cell phone and believed outsider private mists scramble the plain content document utilizing distant key encryption. To guarantee security when utilizing information from cell phones, private mists routinely check the uprightness of information in broad daylight mists as outsider suppliers. At last, the cell phone and private mists encode the web text document permitting you to utilize the client information of the cell phone. We likewise dissected the security of FREDP utilizing BAN. FREDP satisfies security guidelines. We are additionally leading an analysis to quantify the viability of the venture.

The prominence of distributed computing has as of late expanded and most organizations have gotten back to re-appropriate their fundamental information and support to the cloud worker. Notwithstanding, redistributing significant information to the cloud presents both security and information security issues. Consequently, encryption procedures assume a significant function in ensuring information in the cloud. Despite the fact that trading information in scrambled organization secures the information, recovering encoded information and recovering information is troublesome. To diminish the remaining task at hand on encoded information, Eltayieb, N., *et al.* [28] have introduced a characteristic based accessible on the web/disconnected encryption program is presented with the accompanying commitments: First, encryption and drop calculations are isolated into two stages. Second, message encryption and characteristic control strategy are done disconnected. Third, we have

DOI : 10.35291/2454-9150.2020.0660

demonstrated that the proposed plot is secure contingent upon the plain content and the chose catchphrases. At last, we clarified the appropriateness of the proposed venture to the canny cloud-based stage. Distributed computing normally requires a versatile arrangement to address a portion of its difficulties.

Cloud information base administrations offer an extraordinary open door for organizations and associations as far as the executives and cost investment funds. Nonetheless, re-appropriating individual information to outside providers conveys a danger of penetrate of privacy and uprightness. Ferretti, L.,*et al*. [29] have presented a unique arrangement dependent on scrambled Bloom channels was proposed, and the cloud administration permitted the client to perceive unapproved changes in their re-appropriated information. Furthermore, the first examination that can be utilized to limit network stockpiling and organization overhead relies upon the structure and outstanding burden of the example information base. Assess stockpiling and organization costs utilizing miniature benchmarks and TPC-C remaining task at hand and undertaking execution quality and their exhibition enhancements dependent on existing arrangements.

In distributed computing frameworks, information is put away on far off workers that can be gotten to through the Internet. Increasingly close to home and touchy information are progressively centered around secure information stockpiling. Information incorporates money related exchanges, significant records and media content. Actualizing distributed computing administrations will lessen working and support costs and the unwavering quality of neighborhood stockpiling. Notwithstanding, because of unapproved access inside the specialist co-ops, clients are progressively worried about the security and wellbeing of their redistributed information. Arrangements that encode all information with a similar information, paying little heed to the level of information secrecy, increment expenses and preparing times. Loai Tawalbeh et al. [30] have explored a protected distributed computing model dependent on information grouping has been presented. The proposed cloud model lessens the overhead and handling costs needed to make sure about information by utilizing diverse safety efforts with various key measurements to guarantee the degree of privacy needed to ensure the information. The proposed model was tried with different encryption techniques and the reenactment results demonstrated the dependability and effectiveness of the proposed structure.

In the written survey, many authors acknowledge that exceptional information security is achieved. Distributed cyber security has always been a major concern for most organizations, which is why most exploration centers focus on distributed cyber security. We went through the in-depth review of this article, but we'll refer to some of the later and relevant ones here. In 30 zones, there are different zones of the cloud in terms of administrations and models, although there are security concerns and agreements. However, none of these studies provided an answer to the safety concerns identified. Confirm by assigning the cloud to a desktop. The cryptographic computation plays an important role in providing secure correspondence throughout the organization. It is an important and fundamental tool for guaranteeing information. Apart from these, there are many different areas that should be updated as compelling tools can be created to increase the level of security in distributed storage. These troubling concerns have led to exploration here. The encryption plan must be protected for computer if it does not meet certain conditions. To address the security challenges, the proposed model would be adequate regulation.

V. RESULT ANALYSIS

This segment analyzes the findings and consequences of new distributed IT security techniques. Existing writing subjected to security screening using various innovations. This part also shows the improvement of new techniques using tables and insights.

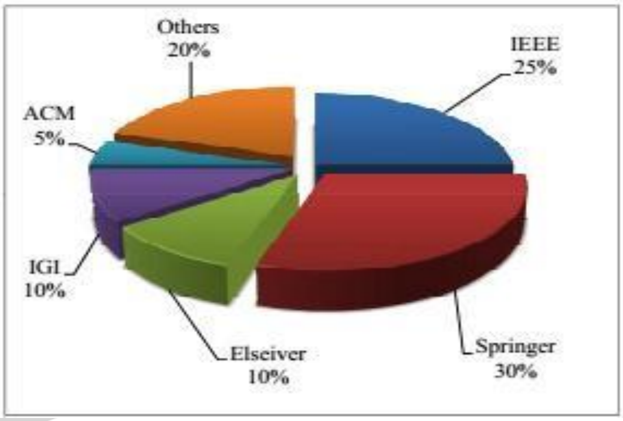

Fig.1: Percentage of published articles based on cloud computing security

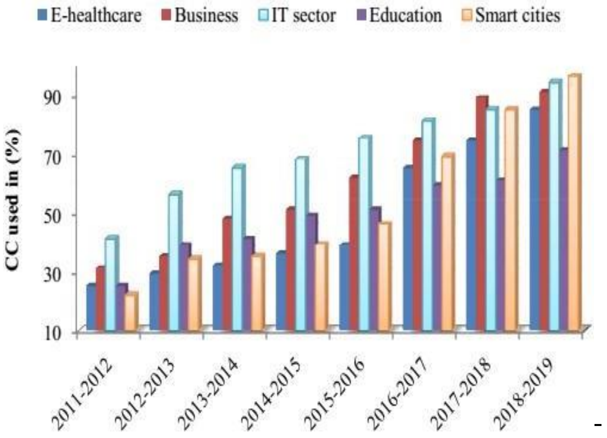

Fig.2: Cloud computing research used in percentage as year by year

The investigation found that the articles came from various journals including IEEE, Springer, Elsevier, IGI and ACM. Figure 1 shows the number of items distributed through Distributed Computer Security. Distributed

DOI : 10.35291/2454-9150.2020.0660

computer research is developing gradually. Figure 2 shows the research articles included in the newspapers according to year 2 (2011-2019). Cryptographic strategies and techniques are updated annually.

A. *Most significant parameters involved in this study*

Table 1: Parameter analysis

Reference No.	Techniques used	Finding Parameters
[16]	HE ECC	Execution time
[18]	ABE ABS	Decryption time Signing in time of user
[19]	HE	Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)
[28]	An attribute-based online/offline searchable encryption scheme	Encryption time Decryption time Sharing time
[30]	AES and 3DES	Processing time
[21]	AD2 Algorithm, SED2 Algorithm and EDCon Algorithm	Execution time
[22]	Multifoldsymmetric-key cryptography technique based upon DNA cryptography	Encryption time Cipher text Computational time

Table 2: Parameter analysis

Author name	Encryption time (sec)	Decryption time (sec)
[16]	0.18-0.56	0.26-0.48
[18]	0.32-0.45	0.36-0.74
[28]	0.12-0.56	0.31-0.53
[30]	0.22-0.69	0.41-0.69
[22]	0.12-0.32	0.15-0.22

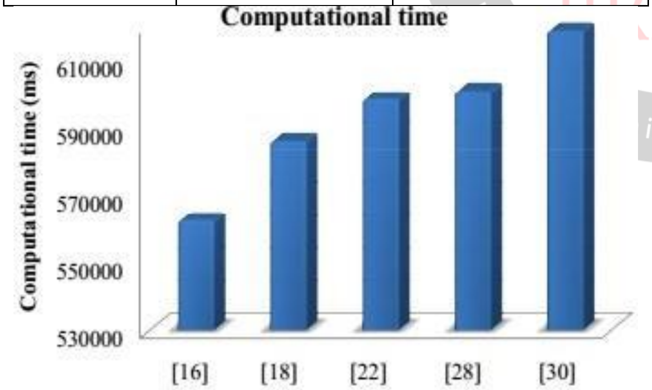

Fig. 3: Computational time analysis

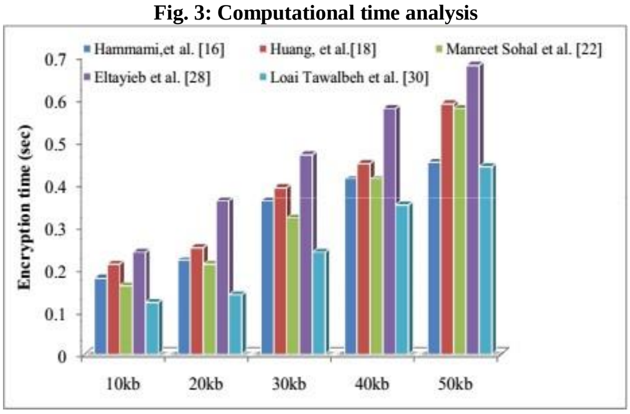

Fig. 4: Encryption time analysis

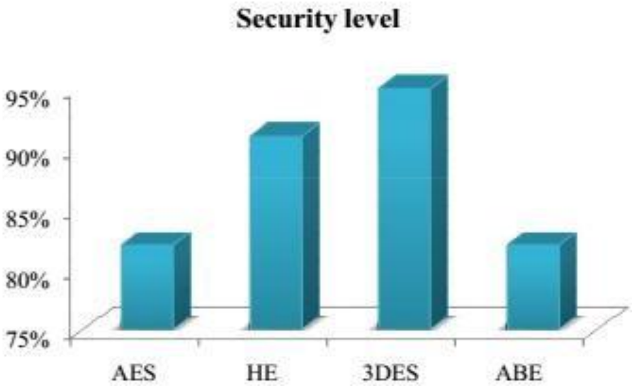

Fig. 5: Security level analysis compared with existing algorithms

Tables 1 show the finds and techniques used different papers are analyzed. Moreover, in table 2, performance of the each algorithm has been analyzed in terms of encryption time and decryption time. Data privacy, encryption and decryption strategies are mainly used. Figures 3, 4 and 5 examine the encryption time, preparation time, and security level of existing recordings and further developments. Many security frameworks are updated as cryptographic calculations. Our review shows the security problem from a specific and practical point of view. Our study differs in conduct, scope and recorded conversation. The latest safety precautions are also taken. The goal is to create an efficient, secure, reliable and productive cloud framework. We are studying and prescribing different ways to address the problems recommended in the letter. As per our audit, we performed another cryptographic computation to achieve better execution by reducing preparation time compared to existing strategies.

V. CONCLUSION

Distributed computing is one of the most common innovations of old age. It has profoundly influenced data innovation, business, program design and information storage. One of the key results is to strengthen one's skills. This expansion of execution does not mean that the cost of equipment, programming and individual preparation will increase. Numerous analysts and experts strive to identify threats, vulnerabilities, attacks, and other issues related to cloud security and protection, and to provide insight into administrative structures, approaches, proposals and installations. . Furthermore, efforts in different regions will help address security threats that develop in the fog. As the two advances rapidly improve, the issue of security must be understood or, unless otherwise limited, to achieving a superior model of reconciliation. Further investigation, in the form of preliminary investigations, may be needed to address the safety concerns raised during this investigation.

REFERENCES

[1] Singh, S., Jeong, Y.-S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, 200–222.

[2] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M.,

DOI : 10.35291/2454-9150.2020.0660

Sarkar, P. (2018). Cloud computing security challenges & solutions-A survey. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).

[3] Khan, N. and Al-Yasiri, A., 2016. Identifying cloud security threats to strengthen cloud computing adoption framework. Procedia Computer Science, 94, pp.485-490.

[4] Kumar, M., Sharma, S. C., Goel, A., & Singh, S. P. (2019). A comprehensive survey for scheduling techniques in cloud computing. Journal of Network and Computer Applications.

[5] Vafamehr, A., & Khodayar, M. E. (2018). Energy-aware cloud computing. The Electricity Journal, 31(2),40–49.

[6] Chauhan, S. S., Pilli, E. S., Joshi, R. C., Singh, G., & Govil, M. C. (2018). Brokering in interconnected cloud computing environments: A survey. Journal of Parallel and DistributedComputing.

[7] Patidar, S., Rane, D., & Jain, P. (2012). A Survey Paper on Cloud Computing. 2012 Second International Conference on Advanced Computing & Communication Technologies.

[8] Gordon, A. (2016). The Hybrid Cloud Security Professional. IEEE Cloud Computing, 3(1), 82–86.

[9] Ramachandra, G., Iftikhar, M. and Khan, F.A., 2017. A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, pp. 465-472.

[10] Kaur, J., Sehrawat, A. and Bishnoi, M.N., 2014. Survey paper on basics of cloud computing and data security. Int J Comput Sci Trends Technol, 2(3), pp.16-19.

[11] Chopra, M., Mungi, J. and Chopra, K., 2013. A survey on use of cloud computing in various fields. International Journal of Science, Engineering and Technology Research, 2(2), pp.480-488.

[12] Sagar B.Jadhav, Dr. Rajesh Prasad, "Review of Cloud Computing and Its Application", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January2013.

[13] Rajivkumar Mente, and Amol Kale, "Cloud Computing and Its Effects in Various Fields", International Journal of Advance REsearch in Science and Engineering, Vol. 06, No.11, 2017.

[14] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28–42.

[15] UniKL, M.I.I.T., Almasri, A.H., Zuhairi, M.F., Darwish, M.A. and Yafi, E., 2018. Privacy and Security of Cloud Computing: A Comprehensive Review of Techniques and Challenges.

[16] Hammami, H., Brahmi, H., Brahmi, I., & Ben Yahia, S. (2017). Using Homomorphic Encryption to Compute Privacy Preserving Data Mining in a Cloud Computing Environment. Lecture Notes in Business Information Processing, 397–413.

[17] Liu, Y., Luo, Y., Zhu, Y., Liu, Y., & Li, X. (2018). Secure Multi-label Data Classification in Cloud by Additionally Homomorphic Encryption. InformationSciences.

[18] Huang, Q., Yang, Y., & Shen, M. (2017). Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. Future Generation Computer Systems, 72,239–249.

[19] Vengadapurvaja, A.M., Nisha, G., Aarthy, R. and Sasikaladevi, N., 2017. An efficient homomorphic medical image encryption algorithm for cloud storage security. Procedia computer science, 115, pp. 643-650.

[20] Kumar, V., Ahmad, M., & Kumari, A. (2018). A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol for Cloud-assisted TMIS. Telematics and Informatics.

[21] Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, 387, 103–115.

[22] Sohal, M. and Sharma, S., 2018. BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. Journal of King Saud University-Computer and InformationSciences.

[23] Greene, E., Proctor, P., & Kotz, D. (2018). Secure sharing of mHealth data streams through cryptographically-enforced access control. SmartHealth.

[24] Fan, Y., Lin, X., Liang, W., Tan, G., & Nanda, P. (2019). A secure privacy preserving deduplication scheme for cloud computing. Future Generation Computer Systems, 101, 127–135.

[25] Wang, X. A., Ma, J., Xhafa, F., Zhang, M., & Luo, X. (2017). Cost-effective secure E- health cloud system using identity based cryptographic techniques. Future Generation Computer Systems, 67, 242–254.

[26] Annie Alphonsa, M. M., & MohanaSundaram, N. (2019). A reformed grasshopper optimization with genetic principle for securing medical data. Journal of Information Security and Applications, 47, 410–420.

[27] Yang, L., Han, Z., Huang, Z., & Ma, J. (2018). A remotely keyed file encryption scheme under mobile cloud computing. Journal of Network and Computer Applications, 106, 90– 99.

[28] Eltayieb, N., Elhabob, R., Hassan, A., & Li, F. (2019). An Efficient Attribute-based Online/Offline Searchable Encryption and Its Application in Cloud-Based Reliable Smart Grid. Journal of Systems Architecture.

[29] Ferretti, L., Marchetti, M., Andreolini, M., & Colajanni, M. (2018). A symmetric cryptographic scheme for data integrity verification in cloud databases. Information Sciences, 422,497–515.

[30] Darwazeh, N.S., Al-Qassas, R.S. and AlDosari, F., 2015. A secure cloud computing model based on data classification. Procedia Computer Science, 52, pp.1153-1158.

DOI : 10.35291/2454-9150.2020.0660