Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/12789
DOI URL: http://dx.doi.org/10.21474/IJAR01/12789

RESEARCH ARTICLE

A SURVEY OF HOMOMORPHIC ENCRYPTION OF DATA IN CLOUD FOR SECURE STORAGE

S. Gnana Sophia[1], Dr. K.K Thanammal[2] and Dr. S SSujatha[2]

1. Research Scholar, S.T. Hindu College, Nagercoil, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012,TN, India.
2. Associate Professor, Department of Computer Science and Applications S.T.Hindu College, Nagercoil Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012,TN, India.

Manuscript Info

Manuscript History
Received: 25 February 2021
Final Accepted: 30 March 2021
Published: April 2021

Key words:-
Fully HomomorphicEncryption(FHE), Partially Homomorphic Encryption(PHE), Partially Homorphic Encryption (PHE), Software as a Service(SaaS), Platform as a Service(PaaS)

Abstract

Cloud computing is the transportation of computing assistance and the opportunity of computer system assets for storing of data and calculating ability without the administration of the user. Against the publishing business and the technical applications of cloud, more probable users are still to join the cloud and the users of cloud can put their less confidential data in the cloud. Loss of security in the cloud is an important problem. The information will be encrypted and gathered in the storage of cloud .The problem here is the informations can be send to or from a cloud in encrypted mode, the servers that function the cloud will not any task on it. In this paper wereviewe the homomorphic encryption techniques, Advantages and disadvantages of various research papers.

Introduction:-

Cloud computing has attained amazing demand nowadays. It provides lower-cost, scalable a site-independent way for maintaining client's data. It has come out as an major criterion which has bring out appreciable security in industry and academia[1]. The computing may be of different types: simple computing and grid computing This cloud computing is an important cautious computing Most of the people use the cloud every day without knowing. Because the cloud service providers distributed all the services from the location remotely[3]. So when the users manage their data on cloud servers, some problems may occur. To divert this problem, all the users have to encrypt the informations first and after that it will be stored in cloud. In spite of many encryption techniques available in the market, homomorphic encryption is the latest concept of security which is used to do the computations on encrypted data, without knowing the private key and without decryption. The client only carries the private key. This method achieves the high security on sensitive information , the key management is not associated by the service provider[5]. Cloud computing has several service models: Infrastructure as a service(IaaS), : This indicate the works distributed to the users, to hire the power of processing and computing resources.

Cloud Service Models:

1. Platform as a service(PaaS) :: Ii produces the run time objective and allows programmers easily to organize test , run and dispose the advantages of web. Because of the scalability is handled by the cloud service provider, the end users are not worry about the management of infrastructure. The providers of PaaS contribute the programming languages, Application frameworks, databases and other tools. Examples are Google App Engine, Force.com, Joyent, Azure.

Corresponding Author:- S. Gnana Sophia
Address:- Research Scholar, S.T. Hindu College, Nagercoil, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012,TN, India.

2. Software as a Service(SaaS): It produce fast access to cloud based utilization of web. The provider controls the whole computing in which we can approach by the use of web browser. This can eradicate the need for install applications on our systems. Examples are MS office 365, Dropbox, etc.,
3. Infrastructure as a Service(IaaS): IaaS clients are answerable to administer the applications, runtime, middleware and data. So the providers of IaaS dominate the servers, hard drives, networking, virtualization and storage. IaaS is the most malleable cloud computing model, easy to brutalize the distribution of storage, networking , servers and the power of processing. This is highly scalable.

Homomorphic encryption

HE was invented for the concept of "Privacy Homomorphism"[8]. The main desire of Homomorphic Encryption is that the encryption of plaintext after addition or multiplication is equal to the ciphertext after encryption.[15]

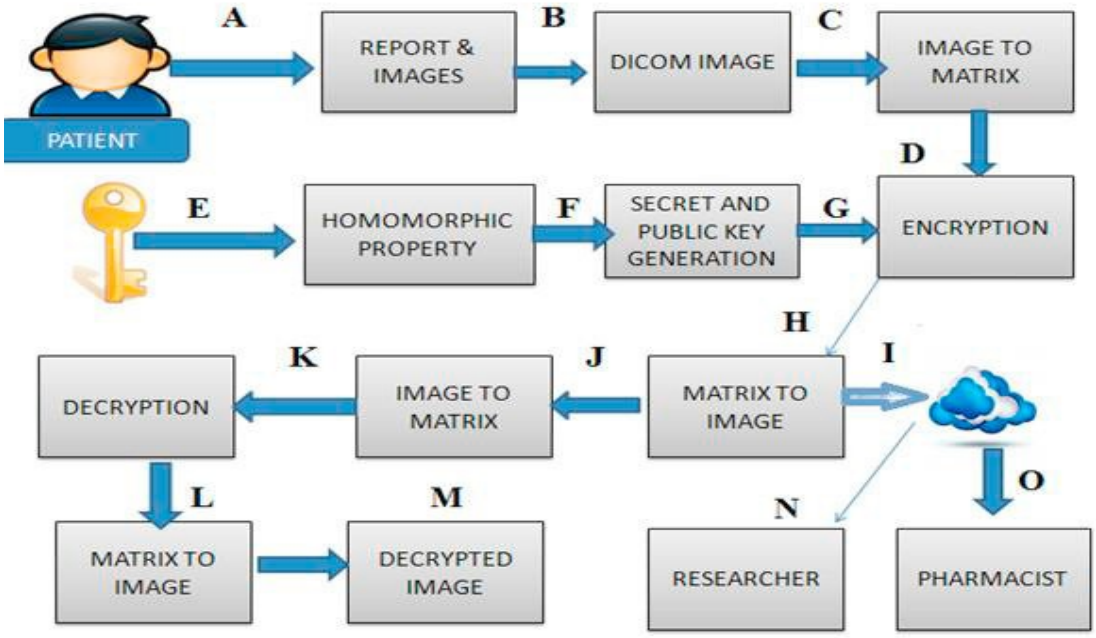

Figure I:- Working of HE.

A. The records, scan and X-ray images of patient's data are mentioned.
B. The images are gathered in the standard format called the DICOM.
C. Image is reformed into matrix to do the process of encryption.
D. These matrix elements are directed one by one to the proposed formula.
E. The process of Key generation takes place here.
F. The public and private keys are generated based on the property of homomorphic
G. Then these framework are catched to perform the encryption.
H. The encrypted matrix is transformed to image.
I. Then the encrypted image can be stored.
J. This one is transformed to matrix.
K. This one is catched by the formula of decryption one by one.
L. Then this decrypted matrix is converted to image.
M. Then we have to obtain the original image
N. The researchers are using encrypted images.
O. These are used by the pharmacist

Types of Homomorphic Encryption

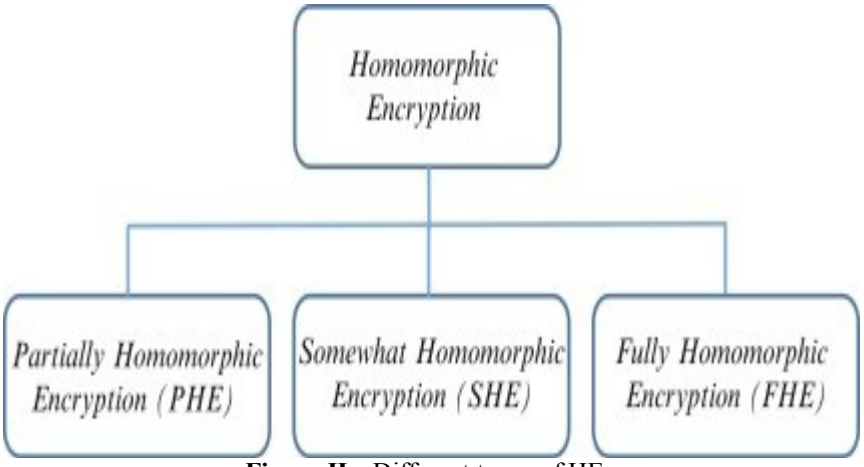

Figure II:- Different types of HE.

Partially Homomorphic encryption (PHE) allows to select only the functions of mathematical which can be observed on encrypted values. Ie, only one operation either addition of multiplication which can be performed an multiple number of times on the ciphertext[8]. PHE with multiplicative operation is the basement of RSA algorithm, and it is used to authorize safe connection through SSL/TLS.

A **Somewhat Homomorphic Encryption** is one which can supports either addition or multiplication, and these operations can be performed a number of times.

Fully Homomorphic Encryption (FHE): The functionality is more with isolation to carry information secure and available at the time of same . This is accomplished by using both addition and multiplication many number of times and looks secure multi-party calculation by more energetic. It can grasp irresponsible calculations on our ciphertext.

Related Work

Homomorphic encryption is the modification of data into cipher text. Without modifying the encryption, homomorphic encryptions allow complex mathematical functions to be achieved on the date after encryption. The aim of homomorphic encryption is to enable computing of encrypted data. Data may also stay private as it is being processed, allowing valuable activities to be drifting out with data existing in unauthenticated environments.

Researchers	Year	Method	Performance	disadvantages
Min Zhao E et al	2019	Fully homomorphic encryption algorithm and Hill encryption algorithm	It improves computational efficiency	The length of the public key is so long
ElbasherElmahdi, et al	2020	Enhanced homomorphic cryptosystem	It provides a higher packet delivery ratio and throughput	It reduces the time it takes from start to finish to extend this scheme to emergency applications.
ShamsherUllah, et al	2020	Kernel homomorphic encryption	It's used to keep sounds and mistakes out of the decryption process.	It reducing feature of security and computations overheads
Saha, T. K., et al	2019	Homomorphic encryption algorithm	It improves the security efficiency	By separating the archive, the protection effectively manages databases with a huge number of records.
Kim, H.-I., et al	2017	k-nearest neighbor (kNN)	It reduces query processing cost	It does not improve performance

		query processing techniques		
Li, J., et al	2020	Homomorphic encryption	It solves non-linear function's computation for ciphertexts	It does not improve the encryption scheme
Wang, X.	2016	BGN homomorphic encryption	ORF MLD protocol also increases with the number of users	Computational complexity
A.M. Vengadapurvaja, et al	2017	Homomorphic crypto algorithms	It assists us in determining the method's efficacy.	It is impossible to extract the mathematical essence of the pixels.
Zhang, J., et al	2017	Homomorphic encryption scheme	It reduces storage, communication and computation costs	It takes more time
Liu, Y., et al	2018	Multi-label Learning and Paillier Cryptosystem	It has the ability to safeguard the privacy of both the data owner and the data consumers.	The safe multi-label grouping is still a work in progress.
Lu, Y. and Zhu, M.	2018	Homomorphic encryption algorithm	The algorithms' correctness and computational efficiency are tested.	Computational complexity
Rahman, M. S., et al	2020	BGV Fully Homomorphic Encryption scheme	It cuts the time it takes for the privacy-preserving AI-enabled edge service to run.	During composition, the system must take into account the mobility of edge sensors.
Chillotti, I., et al	2018	Fully Homomorphic Encryption	It does not improve the evaluation of look-up tables and random functions by lowering the expansion factor.	The cost of simulation is very high
Smart, N.P. and Vercauteren, F.	2014	Fully homomorphic scheme and naive decryption method	It's used to parallelize the decryption process.	Complex computation
Cheon, J.H., et al	2015	Chinese Remainder Theorem based fully homomorphic encryption algorithm	It's used to add an error message to a message until it's encrypted.	Computational complexity
Ishimaki, Y., et al	2017	Fully Homomorphic Encryption and Burrows Wheeler Transform	It safeguards the privacy of both the encrypted information and the query.	It excludes the development of a multi-data owner protocol and the upgrading of storage data with a minimal number of correspondence.
Li, R., et al	2019	Fully homomorphic Encryption	It constructs a privacy-preserving anomaly detection method using a single-integer input function.	Less efficient level for the conjunctive and disjunctive
Bos, J. W., et al	2013	Leveled homomorphic encryption, and	It reduces the size of ciphertexts to a single ring element.	It reduces security

		FHE		
Chillotti, I. et al	2020	Fully homomorphic encryption scheme over the torus	It provided a dedicated security analysis	It does not improve the encryption scheme
Carpov, S., et al	2019	Multi-value bootstrapping, homomorphic LUT	It increases the evaluation efficiency of multi-output functions	It reduces the time it takes from start to finish to extend this scheme to emergency applications.
Chen, H., et al	2019	Multi-Key Homomorphic Encryption	It's utilized to create a modern hybrid product that combines single-key and multi-key ciphertexts for improved storage.	It produces maximum noise
Cheon, J.H., et al	2017	Homomorphic encryption	It greatly decreases the size of the ciphertext.	The modulus of ciphertext decreases for homomorphic operations, and their scheme can no longer support homomorphic computation at the lowest level.
Li, B. and Micciancio, D.	2020	Fully homomorphic encryption algorithm	It leads to full main recovery with a good chance of success and very short run times.	It contains a wide range of security problems
Gentry, C., et al	2012	FHE	It improves computational efficiency	The length of the public key is so long
Gentry, C., et al	2012	FHE	It requires the secret key's encryption to be stored as a single ciphertext, resulting in a smaller public key.	The approach does not necessitate the use of homomorphic polynomial modular reduction.
Ducas, L. and Micciancio, D.	2015	FHE	It improves the efficiency of Gentry's initial solution.	It is unable to completely use the message space provided by ring LWE encryption.
Bourse, F., et al	2018	Fully Homomorphic Encryption and Neural Networks	It gains reliability at the expense of increased capacity requirements.	Execution time is low

A homomorphic encryption technology for cloud computing which has been developed by Zhao E, et.al [1]. The handling of ciphertext data under privacy protection is made possible by homomorphic encryption technologies. It will retrieve, measure, and amount ciphertext directly in the cloud and return the results to users as ciphertext. This technology, unlike conventional encryption algorithms, does not require regular encryption and decryption between the cloud and consumers, lowering connectivity and processing costs. It was the most important technology for ensuring data protection in cloud environments. Main security problems in cloud systems can be addressed thanks to the homomorphic features of the technology, and cloud infrastructure can further accelerate the advancement of homomorphic encryption technology.

In 2020 Elmahdi, E., et.al [2] proposed through distributing the pieces of the whole message into different paths and using a HE mechanism for cryptography, an expanded AOMDV method to make data transfer safe and stable in the presence of malicious nodes in MANETs. The simulation findings reveal that the scheme has a higher packet distribution ratio and throughput, all of which are desirable characteristics for emergency applications in MANETs.

In 2019 Ullah, et.al, [3] has been proposed a novel kernel homomorphic encryption scheme. The rate of development of sounds, glitches, and computation in the electronic world and cloud computing was growing day by day. The entire negotiation mechanism crashed after the number of noises was surpassed. They add a novel kernel HE schemes to reduce the development of noises and computation. By using kernel and kernel homomorphism, the Ker-HE scheme was used to remove the number of noises. These functions were used to prevent the ciphertext from being too long during decryption and to eliminate any noise or errors.

An effective secluded database inquiry by means of ring-LWE SHE was developed by Saha, et.al [4]. The decryption's ability to retrieve the unique result from the ciphertext determines the consistency of an encryption technique. The correctness of HE schemes was determined by recovering the unique consequence since the ciphertext via authentication after some homomorphic operations.

In 2017 Kim, et.al [5] proposed a modern HE-based stable kNN query processing algorithm They ensure that all encrypted data and user question information are kept private. They also devised an encrypted index method based that executes data filtering without exposing data access patterns in order to obtain high query system throughput. The scheme outperforms the current scheme in terms of query processing costs while maintaining user anonymity, according to a results report.

In 2020 Li, Jing, et.al. [6] has been proposed establish the homomorphism operations in ciphertext space and propose a novel HE scheme over non-abelian rings. Based on the Conjugacy Search Issue, the scheme can achieve one-way protection. It directly involving authentication using the homomorphism of a 2-order distortion matrix coding function, allowing for a simple homomorphic comparison of ciphertexts against the need to decode any intermediate results.

In 2016 Wang, Xiaofen [7] proposed a one-round meeting position calculation protocol in which the location service provider consults with a semi-trusted cloud server that serves as a computing hub and performs the majority of the calculations. The computing hub, the meeting venue determination server, and participants all protected user location privacy from external and internal attackers. They use smartphones to measure the protocol's mathematical efficiency in order to research its efficiency. The simulation findings, as well as a performance analysis of their protocol to another protocol with similar functionalities, show that their solution was more effective and realistic.

In 2017 Vengadapurvaja, A.M. et.al [8] proposed the effective HE algorithm for encrypting medical images and performing useful operations on them while maintaining confidentiality. Electronic health reports were the safest way to keep track of a patient's records in order to increase the continuity of care. An electronic health record (EHR) was a multimedia record of a patient's medical information. The electronic health record allows us to keep track of a vast variety of records and makes it simple to optimize all facets of patient care, including quality and accurate record updates.

In 2017 Zhang, et.al [9] has developed a generic mechanism for creating a stable cloud storage protocol based on the HE scheme They were the first to investigate the intrinsic relationship between secure cloud storage and HE schemes, and present a Generic way to construct a Secure Cloud Storage protocol, denoted as G-SCS, that can be used for any HE scheme (HES). Under a concept that satisfies the security prerequisite of cloud storage, the proposed G-SCS was stable.

A Secure multi-label data classification over encrypted data has been developed by Liu, et.al [10]. Their approach offloads the multi-label sorting challenge to cloud servers, greatly reducing the storage and computing demands on data owners and customers. Their results can protect the privacy information of data owners and users, cloud servers cannot learn anything valuable about the input data, and multi-label marking effects can be output, according to theoretical proof.

Privacy preserving distributed optimization using homomorphic encryption has been developed by Lu, Y., and Zhu, M [11]. They investigate how a computer operator and a group of agents execute a hierarchical gradient-based algorithm while remaining anonymous. In the one hand, each agent's state and feasible set were private to it and should not be known to any other agent or the system operator; on the other hand, each agent and the data provider owned a set of private functions of the component functions, and each coefficient should not be disclosed to any person who did not initially own it.

Confidentiality maintaining AI-based formulation approach in edge networks utilizing fully homomorphic encryption was developed by Rahman, M. S., et.al [12]. They implement an AI-based formulation method for edge services in the network edge. They also provide a private information AI task scheduling architecture that uses the fully homomorphic encryption (FHE) algorithm to compose encrypted QoS files. They use a simulated QoS dataset to test the efficiency of their privacy-preserving service composition system in many experiments.

Chillotti, I [13], have implemented faster compressed homomorphic procedures and effective circuit bootstrapping. They introduce several methods for improving homomorphic function evaluation, both for totally and leveled homomorphic encryption, in this article. They suggest two packing approaches in TRGSW-based homomorphic schemes to reduce the extension factor and improve the estimation of look-up tables and random functions.

Smart, N.P., and Vercauteren, F., developed fully homomorphic SIMD operations [14]. They demonstrate how to choose variables to allow SIMD processes in this article. As a result, they receive a homomorphic system that supports SIMD processes as well as procedures on massive finite fields of characteristic two. They prove that SIMD procedures can be utilized to parallelize the decryption process, resulting in a significant speedup. Finally, they examine two use cases to show how SIMD operations can be used to execute different tasks: encrypting and homomorphically applying AES database lookup.

In 2015 Cheon, J.H, et.al, [15] has proposed FHE over integers based on CRT. In this article, they return to one of their ideas, the third scheme, which is based on the Chinese Remainder Theorem and rang homomorphically. This system was known to be broken by just a single pair of known plaintext/ciphertext. They will, however, deal with this issue by using a common method to inject an error into a message before encryption. They introduce a stable improvement of their proposal by demonstrating that under the approximate GCD presumption and the sparse subset sum assumption, the scheme is totally homomorphic and stable against the chosen-plaintext attacks.

In 2017, Ishimaki, Y., et al. [16] introduced a private substring retrieval protocol based on HE that protects both the stored information and the query's confidentiality. They demonstrated that FHE's substring quest can be completed in a reasonable amount of time and that their Batch Recursive Oblivious Transfer ensures that the analyst knows little more than the server's searched result.

Li, R., et al. [17] suggested a LUT protocol for analyzing any single-integer input variable in order to create a privacy-preserving anomaly identification scheme on a smart grid with FHE in 2019. Integer encoding, which was more effective than bitwise encoding, was supported by the protocol. Since they used the LUT protocol, the assessment period was independent of the purpose. Other structures that need a single input complex function evaluation depend on FHE were also supported by this protocol.

In 2013, Bos, J. W., et al. [18] suggested a new FHE scheme based on the Stehl e and Steinfeld scheme, which eliminates the HE scheme's non-standard evaluative small computational ratio prediction. Their new structure eliminates modulus flipping and holds ciphertexts to a single ring variable in size. They've also proposed a more realistic version of their scheme that doesn't depend on the decisional small polynomial ratio assumption.

I. Chillotti et al. [19] have given a comprehensive description of the TFHE construction, from an analytical LWE and GSW perspective to a realistic and functional implementation. This paper presents a torus-based quick FHE scheme (TFHE) that revisits, generalizes, and strengthens the FHE based on GSW and its ring variants. Finally, they include an additional functional study of LWE-based systems, in which the protection parameter was specifically related to the LWE error rate and the entropy of the LWE hidden key, as well as explicit variable sets and timing comparisons for all of their structures.

In 2019, Carpov, S. [20] proposed a bootstrapping protocol based on the TFHE system of split test integrals that can be utilized to analyze multi-value parameters and improve the performance of multi-output function evaluation. This approach can be easily generalized to other FHEW-based bootstrapping protocols, they note. They demonstrate how to develop and choose TVF to optimize the evaluation of consequences of different in a single bootstrapping call in this paper. They examining the configuration of FHEW-based bootstrapping algorithms and comparing the noise overhead performance and modularity.

Chen. H, et al. [21] suggest an RGSW-like cryptosystem and two strategies for multiplying single-key encryption into a multi-key RLWE ciphertext in 2019. The first algorithm has two phases: multi-key RGSW ciphertext processing and multi-key external product formation. Their second hybrid product algorithm took a radically different approach to achieve the same features. The most significant technological achievement was the development of a new hybrid product that combines single-key and multi-key ciphertexts to improve storage, computation complexity, and noise development.

Cheon, Jung Hee, and colleagues [22] presented a procedure for effective estimated calculation on HE in 2017. The basic idea was to consider authentication noise to be a kind of error that occurs throughout the estimated calculations. They still keep their authentication representation small sufficiently in comparison to the ciphertext material properties for homomorphic operations such that the computation result was always smaller than q. They have an issue with the fact that the bit size of a message grows gradually with circuit depth without rounding. They propose a new technique called rescaling that tries to manipulate the communication of ciphertext to solve this problem.

Li, et.al. [23] suggested new security concepts in 2020, expanding the standard IND-CPA protection supposed to catch the passive protection criterion for (homomorphic) approximate encryption strategies. The need for appropriate authentication notions for approximate encryption tells us that correctness and security were two important aspects of cryptographic schemes that must be considered simultaneously.

Gentry, C, et al. [24] proposed the construction of FHE schemes for defense in 2012. To achieve low overhead, they employ Smart-Vercauteren and BrakerskiGentry-Vaikuntanathan's batch homomorphic evaluation methods which demonstrated that homomorphic operations can be applied to "filled" ciphertexts that encode vectors of plaintext elements. They apply to permute/routing strategies to effectively transfer plaintext components around these vectors in this paper. As a result, they can execute general arithmetic circuits in batches without ever having to “unpack” the plaintext vectors. It takes more computation to handle encrypted data homomorphically than it does to transfer unencrypted data.

Gentry, C, et al. [25] proposed a simplified solution in 2012 that partially by passes the homomorphic modular-reduction bottleneck by dealing with a modulus similar to a power. Their solution was simpler to define and execute than a conventional binary circuit, and it was likely to be quicker in operation. It was also ability to handle an authentication of the secret key as a single ciphertext utilizing their methodology from this work.

Ducas, L., and Micciancio, D. [26] proposed a method for bootstrapping homomorphic encryption. They introduce a new method for homomorphically computing basic bit operations and refreshing (bootstrapping) the resulting output in less than half a second on a personal computer in this article. They offer a thorough theoretical description of the scheme (based on the worst-case hardness of regular lattice problems) and discuss how well their prototype implementation performed. The key benefit of their recent homomorphic NAND procedure was that it generates far less noise than previous approaches.

Bourse, F., et al. [27] established Quick homomorphic evaluation of deep discretized neural network. They introduce FHE DiNN, a new paradigm for homomorphic evaluation of neural networks whose complexity was purely linear in the network depth and whose parameters can be set beforehand, in this article. They view the problem from a scale-invariant perspective. Every neuron's performance was refreshed by bootstrapping in their system, FHE DiNN, allowing arbitrarily deep networks to be homomorphically examined

Conclusion:-

The existing literature study were studied in this paper. The cloud computing security based on homomorphic encryption is the latest concept. This paper analyzed the problem of homomorphic encryption, method, and their performance . This topic is considered as the major issue in the environment of cloud computing. Data hacking provides more problems for users on cloud storage.

References:-

[1] Ismail, U. M., & Islam, S. (2020). A unified framework for cloud security transparency and audit. Journal of Information Security and Applications, 54, 102594.

[2] Ahamad, D., Alam Hameed, S., & Akhtar, M. (2020). Ahamad, D., Alam Hameed, S., & Akhtar, M. (2020). A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. Journal of King Saud University - Computer and Information Sciences.
[3] Mondal, A., &Goswami, R. T. (2020). Enhanced Honeypot Cryptographic Scheme And Privacy Preservation For An Effective Prediction In Cloud Security. Microprocessors and Microsystems, 103719.
[4] Sen, A., &Madria, S. (2020). Application design phase risk assessment framework using cloud security domains. Journal of Information Security and Applications, 55, 102617.
[5] Venkatesh, A. and Eastaff, M.S., 2018. A study of data storage security issues in cloud computing. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(1), pp.1741-1745.
[6] Halabi, T., &Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. Journal of Information Security and Applications, 33, 55–65.
[7] Zhao E, Min; Geng, Yang (2019). Homomorphic Encryption Technology for Cloud Computing. Procedia Computer Science, 154(), 73–83.
[8] Elmahdi, E., Yoo, S.-M., &Sharshembiev, K. (2020). Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. Journal of Information Security and Applications, 51, 102425.
[9] Ullah, Shamsher; Li, Xiang Yang; Hussain, Muhammad Tanveer; Lan, Zhang (2019). Kernel homomorphic encryption protocol. Journal of Information Security and Applications, 48(), 102366–.
[10] Saha, T. K., Rathee, M., &Koshiba, T. (2019). Efficient private database queries using ring-LWE somewhat homomorphic encryption. Journal of Information Security and Applications, 49, 102406.
[11] Kim, Hyeong-Il; Kim, Hyeong-Jin; Chang, Jae-Woo (2017). A secure kNN query processing algorithm using homomorphic encryption on outsourced database. Data & Knowledge Engineering, (), S0169023X17303476–.
[12] Li, J., Kuang, X., Lin, S., Ma, X. and Tang, Y., 2020. Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. Information Sciences, 526, pp.166-179.
[13] Wang, X. (2016). One-round secure fair meeting location determination based on homomorphic encryption. Information Sciences, 372, 758–772.
[14] Vengadapurvaja, A. M., Nisha, G., Aarthy, R., &Sasikaladevi, N. (2017). An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security. Procedia Computer Science, 115, 643–650.
[15] Zhang, J., Yang, Y., Chen, Y., Chen, J., & Zhang, Q. (2017). A general framework to design secure cloud storage protocol using homomorphic encryption scheme. Computer Networks, 129, 37–50.
[16] Liu, Y., Luo, Y., Zhu, Y., Liu, Y., & Li, X. (2018). Secure Multi-label Data Classification in Cloud by Additionally Homomorphic Encryption. Information Sciences.
[17] Lu, Y. and Zhu, M., 2018. Privacy preserving distributed optimization using homomorphic encryption. Automatica, 96, pp.314-325.
[18] Rahman, M. S., Khalil, I., Atiquzzaman, M., & Yi, X. (2020). Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption. Engineering Applications of Artificial Intelligence, 94, 103737.
[19] Chillotti, I., Gama, N., Georgieva, M. and Izabachène, M., 2017, December. Faster packed homomorphic operations and efficient circuit bootstrapping for TFHE. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 377-408). Springer, Cham.
[20] Smart, N.P. and Vercauteren, F., 2014. Fully homomorphic SIMD operations. Designs, codes and cryptography, 71(1), pp.57-81.
[21] Cheon, J.H., Kim, J., Lee, M.S. and Yun, A., 2015. CRT-based fully homomorphic encryption over the integers. Information Sciences, 310, pp.149-162.
[22] Ishimaki, Y., Imabayashi, H. and Yamana, H., 2017, May. Private substring search on homomorphically encrypted data. In 2017 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 1-6). IEEE.
[23] Li, R., Ishimaki, Y. and Yamana, H., 2019, June. Fully homomorphic encryption with table lookup for privacy-preserving smart grid. In 2019 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 19-24). IEEE.
[24] Bos, J. W., Lauter, K., Loftus, J., &Naehrig, M. (2013). Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme. Lecture Notes in Computer Science, 45–64.
[25] Chillotti, I., Gama, N., Georgieva, M. and Izabachène, M., 2020. TFHE: fast fully homomorphic encryption over the torus. Journal of Cryptology, 33(1), pp.34-91.

[26] Carpov, S., Izabachène, M. and Mollimard, V., 2019, March. New techniques for multi-value input homomorphic evaluation and applications. In Cryptographers' Track at the RSA Conference (pp. 106-126). Springer, Cham.
[27] Chen, H., Chillotti, I. and Song, Y., 2019, December. Multi-key homomorphic encryption from TFHE. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 446-472). Springer, Cham.
[28] Cheon, J.H., Kim, A., Kim, M. and Song, Y., 2017, December. Homomorphic encryption for arithmetic of approximate numbers. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 409-437). Springer, Cham.
[29] Li, B. and Micciancio, D., 2020. On the security of homomorphic encryption on approximate numbers. IACR Cryptol. ePrint Arch, 2020, p.1533.
[30] Gentry, C., Halevi, S. and Smart, N.P., 2012, April. Fully homomorphic encryption with polylog overhead. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 465-482). Springer, Berlin, Heidelberg.
[31] Gentry, C., Halevi, S. and Smart, N.P., 2012, May. Better bootstrapping in fully homomorphic encryption. In International Workshop on Public Key Cryptography (pp. 1-16). Springer, Berlin, Heidelberg.
[32] Ducas, L. and Micciancio, D., 2015, April. FHEW: bootstrapping homomorphic encryption in less than a second. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 617-640). Springer, Berlin, Heidelberg.
[33] Bourse, F., Minelli, M., Minihold, M. and Paillier, P., 2018, August. Fast homomorphic evaluation of deep discretized neural networks. In Annual International Cryptology Conference (pp. 483-512). Springer, Cham.