CLOUD CRYPTOGRAPHY TO ENSURE SECURITY AND PRIVACY IN CLOUD

Jaishree Jain
Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad, UP, India
jainjaishree@akgec.ac.in

Abstract: **The cloud computing age can be highly beneficial in today's world since it makes use of the internet and essential remote servers to provide and store data and applications. Customers can use such programmers over cloud communications without having to install anything. Furthermore, the surrendered customers' records papers can be accessed and modified via the internet from another computer. Despite the records' and alert's power, having access to, there are various queries nonetheless arising on a way to benefit depended on surroundings that shield records and programs in clouds from hackers and intruders. Cloud Computing Environment (CCE) offers numerous deployment fashions to symbolize numerous classes of cloud owned with the aid of using corporation or institutes. Cloud computing environments, on the other hand, give sources to cloud users through a variety of services such as IaaS, PaaS, and SaaS. Cloud computing is essentially built on the concept of combining entirely physical sources and presenting them as an incomprehensible resource. It is a version for generating the source, checking the programmes, and obtaining the right of entry to the manifesto-fair person's offerings. It is a fashion institution that focuses on deployment fashion and provider fashion. IaaS, PaaS, and SaaS are all examples of service fashion. Public cloud, private cloud, hybrid cloud, and community cloud are all deployment models. There are so many fantastic habitats in cloud computing. A chunk extra approximately a few safety elements of cryptography with the aid of using showcasing a few privateness problems of modern CCE.**

Keywords: **Cloud Computing Environment, Cryptography, Security Quantum key distribution, Privacy Algorithms.**

I. INTRODUCTION

Cloud computing is an advanced network providing all kind of resources as a service. One challenge that is required is Internet that is turned into design. But security risks are also there. The software which is uploaded over the cloud is at great risk. Cloud computing has all of the feebleness related to those net usages. Various information privateness issues in cloud computing occurs over the Internet. False significance of an information utilized in corporations in cloud to 1/3 events is one of the essential troubles which have been found [10]. Encryption needs to be nicely used and the crypto algorithms encompass AES, Rivest-Shamir-Adleman, Data Encryption Standard and three DES. In the presented paper cryptographic algorithms are used so that you can boom safety concern. Cloud Information integrity can help to assure security. There are several sorts of cryptographic algorithms that can be implemented to assure cloud security. Symmetric and asymmetric encryption key algorithms are the two sorts of algorithms. DES, AES, 3DES, and the Blowfish algorithm are examples of symmetric algorithms. Algorithms like RSA and Diffie-Hellman Key Exchange are asymmetric. In the cloud, symmetric and asymmetric key techniques are used to encrypt and decode data. Typically, cloud users make use of a cloud carrier provider's helpful resource allocation and scheduling services. As a result, in cloud computing systems, security is critical.[3][4].

II. RELATED TERMINOLOGY

In the paper [1] the authors discuss the trouble of protecting records at some level in record transmission. The major component almost worrying in this paper is the encryption of the records so that confidentiality and confidentiality can be achieved without problems. Paper [2] affords set of commands that makes use of the offerings of auditor or checker now no longer best to confirm and authenticate the integrity of records saved at far way servers however additionally in fetching and receiving the records returned as quickly as feasible. The major gain of this scheme is using virtual signature to guarantee the integrity of neighborhood records. However, the general system is elaborate and complex as the key and record are also encrypted and decrypted respectively.

Allocating mathematical time addresses one of the most difficult problems in computing. While clients engage with remote computing centres, this record can maintain secrecy [18]. Its power derived from the use of quantum cryptography or Distributed Discrete (DKD) techniques, which are considered the state-of-the-art in encryption and decryption systems [20], [21], as shown in Figure 1. Records are essentially based on fully structured states termed photons over quantum channels. These photons are subsequently transferred as "keys" for secure communication encryption and decryption [11]. The no-cloning theorem benefits from the use of such photons in record transmission.

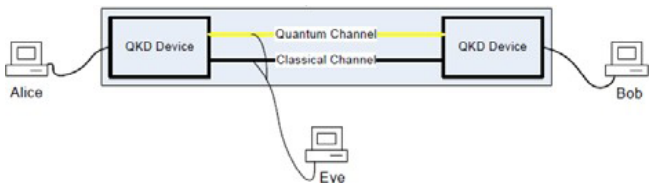

Fig. 1 Schematic of DKD

Researchers are examining the ideal marriage of cloud computing and quantum computing, which protects the security of information stored on remote computer systems or servers. They used a record processing server, such as a quantum computer, to encrypt the majority of records, which successfully hides input, processing, and output records from hostile attacks and [22], [23], [24], and [25]. In a cloud context, encryption and authentication are the most important aspects of fact security. Encryption procedures have grown as one of the most basic concerns in keeping record security within the cloud; reputation fashion predicated exclusively on the record encryption method is outdated. It also protects enterprise documents by employing operational-maintenance encryption and tokenization in all non-public and public cloud communications without compromising functionality, usability, or performance. [28], [29] are two examples. Cipher Cloud has the potential to create unified record security coverage across all clouds, including Google, Amazon, Azure, and others, which clients are likely to have used to acquire records. [14, 15, 16, 17, 18, 19]. Multiple AES-like conscious encryption and tokenization choices, such as layout and attribute-keeping encryption methods, are a cipher cloud advantage. When using the Cipher Cloud Security Gateway to access software, users see the actual records, whereas the records saved in the cloud software are encrypted [30], [31]. By using encryption in the Cloud Security Gateway, Cipher Cloud gets rid of cloud computing inherent security, privacy, and regulatory compliance threats [12]. Cipher Cloud's exceptionally secure encryption protects every layout and feature of record, so cloud packages remain operational, however their actual content material stays locked with inside the company [13]. After then, the system is reversed while personnel get admission to cloud packages via the equipment decrypting records in actual time in order that customers see the real records instead of the encrypted model that is living with inside the cloud.

III. SECURITY & PRIVACY ALGORITHMS IN CLOUD

Cryptography can assist in the early adoption of cloud computing by a significant number of privacy-conscious businesses. The most important aspect of privacy that encryption can provide for cloud computing is that it is secure and stable. Cryptography is the technical expertise of safely storing messages by transforming unreadable data into unreadable bureaucratic data [7].

Cryptography is now thought of as a collection of three algorithms. The symmetric-key algorithm, asymmetric-key algorithm, and hashing [6] are the algorithms in question. Theoretical issues in cloud computing are linked to issues with statistics security, backup statistics, community traffic, document garage devices, and host security. Encryption techniques such as Secure HTTP, Encrypted VPN, TLS, Secure Shell, and others must be utilised for a secure and stable connection between the visitor zone and the host zone, or from hosts to control structures. We'll use encryption to protect you from exploits like man-in-the-middle assaults, bogus attacks, and consultation hijackings. Customers can store data and run applications on top of a computing centre or infrastructure provided by cloud computing. While cloud computing has many advantages, it also creates new security challenges because cloud operators are always present to control data for clients without relying completely on them. We're attempting to design cryptographic primitives and protocols that can be used to cloud computing while maintaining a balance of security, performance, and utility. Users who proudly own the data or linked entities no longer have unauthorised access must have their privacy protected by cloud statistics technology and computation. Cryptography has been widely used to address the aforementioned issues, with some considerations in statistical security, privacy, and cloud computing.

a) Symmetric key algorithms

The symmetric key algorithm employs symmetric univariate keys for both encryption and decryption. Symmetrical structures provide their consumers with a channel device. It ensures that users are authenticated and authorised. The best and best keys for each are used in symmetric-key algorithms.

b) Advanced Encryption Standard (AES)

The Advanced Encryption Standard [3, 5] is a symmetric-key encryption set of principles in cryptography. The block length for each cypher is 128 bits, while the key sizes are 128, 192, and 256 bits, respectively. AES ensures that a set of rules is followed.

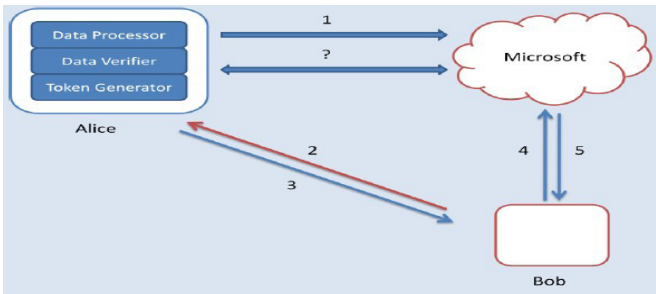

Fig.2 Cipher Cloud Model

Static encryption is used to encrypt the hash code. AES uses a 128-bit block length. The following is a list of its rules:

Initial Round Key Expansion - Round keys have been introduced. Sub Byte Rounds - A non-uniform replacement phase in which each byte is replaced with a different byte according to the table.

Rows are transferred - a phase in which each nation's row is cyclically shifted in a set number of steps. The columns have been combined.

ROUND ADD KEY - Every byte of that nation is merged with the rounding key, and each circular secret employs a key schedule derived from the cypher key.

Sub Bytes, Shift Row, and Add Round Key are all used in the last round. In 1998, the DES rules were harmed by the use of a gadget that cost around $250,000. As the DES rule set moved to mid-1970s technology, Triple DES became too slow for performance and no longer produced green and powerful software programme code. Triple DES is slower since it has three instances of the same number of rounds as DES.

c) Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric key encryption derivative that is a block cypher. The National Institute of Standards and Technology (NIST) discovered it in January 1977. On the encryption side, DES implicitly takes 64-bit plaintext and converts it to 64-bit crypto textual content; on the decryption side, it converts 64-bit cypher textual material to 64-bit plaintext, resulting in a total of 56 bits. Encryption and decryption are both done with the cypher secret.

The initial and final permutations of a permutation (P-box) are used in the encryption technique, as well as the Fiestel Round of 16. Each rounder use a different type of 48-bit circular key.

d) Blowfish Algorithm

Blowfish is also classified as a symmetric block cypher, which can be used instead of DES. It has a variable-duration key, ranging from 32 to 448 bits, allowing it to be used in a variety of settings at home and abroad. Blowfish was created in 1993 by Bruce Schneier as a lightweight, quick substitute for conventional encryption techniques. It's been thoroughly tested since then, and it's rapidly gaining traction as a strong encryption set of principles. Blowfish is free of patents and licences, but it needs be loosened before it may be used by everyone.

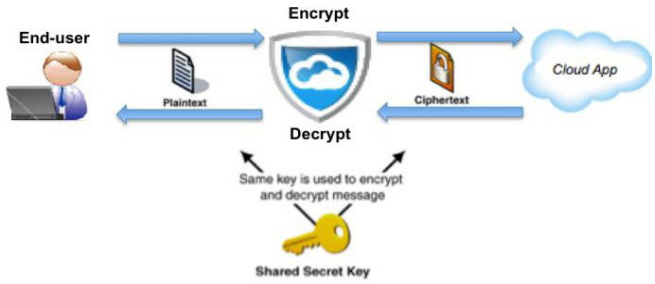

Fig. 3 Cryptographic Cloud Storage Architecture

e*) Asymmetric Key Algorithms*

In comparison to symmetric cryptosystems, this is a relatively new concept. Encryption and decryption are done with different keys. This is a feature that distinguishes this system from symmetric encryption schemes. Each receiver has a unique decryption key, often known as an individual key. The receiver wants to generate a public key, which is an encryption key. This type of cryptosystem typically relies on a third party formally declaring that a specific public key is the best of a specific individual or entity.

f) RSA Cryptosystem

This encryption algorithm is one of the first and most ancient of the various cryptosystems. It is still the most often rented and used cryptosystem. The gadget is known as the RSA cryptosystem since it was created by three students named Ron Rivest, Adi Shamir, and Edelman. This set of rules is no longer a personal-key cryptogram and is now utilised for public-key cryptography.

It is a set of simple, yet frequently utilised unequal rules. It usually comprises of two keys: a public key and a personal key. The public secret is used to encrypt the messages and is known by everyone. The best way to decrypt messages encrypted with the public key is to use a personal key.

The server uses public key verification in this manner by signing a completely distinct message with its personal key, which is referred to as a virtual signature. The consumer must then sign the document. It next verifies that the server's recognised public key is being used..

g) Hashing Algorithms

i. MD5- (Message-Digest set of rules 5)

A cryptographic hash attribute set of rules that uses a 128-bit hash cost and places a variable-duration message in a 128-bit constant-period output. The entry message is first broken into 512-bit chunks, and then padded so that the entire duration is divisible by 512. The communication is encrypted by the sender using the common public key. The communication is decrypted by the receiver using his personal key.

ii. Cloud Storage

Kamara & Lauter et al. [32] recommended providing a digital personal garage that may satisfy a variety of needs (privacy, integrity, authentication, etc.). The majority of requirements are met by encrypting files stored in the cloud. However, with collaboration technology, such encryption ends in rigour at each search approach and real-time altering through files. Figure 3 depicts the cryptographic garage carrier's structure, which can be utilised to address back-up, archival, fitness document structures, static statistics trading, and e-discovery security issues" [9]. It is made up of three main components: the Data Processor (DP), which reads data before transferring it to the cloud, the Data Verifier (DV), which verifies the data's integrity, and the Token Generator (TG), which allows the bearer issuer to access the files. enables recovery Before sending statistics to the cloud, Alice encrypts and encodes files with metadata (tags, timing, length, etc.) using a statistics processor, then transmits them to the cloud.

B. Proposed Model Main Building Block

This version includes cypher cloud version and cloud statistics encryption, both of which are mostly based on quantum cryptography, so that: I key technology and key control are primarily based on DKD to improve the supply and reliability of cloud computing encryption. Deploy decryption and strategy mechanisms.

(ii) Manipulate heavy computing techniques that aren't compatible with non-public computers.

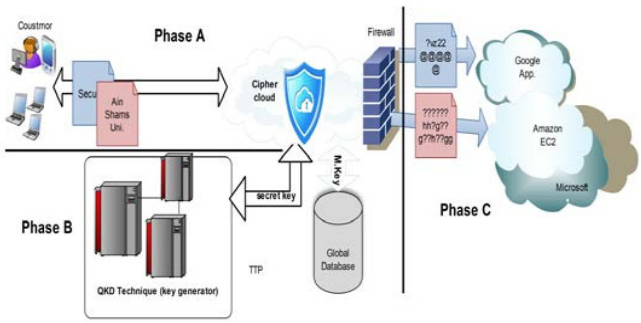

Fig. 4 Framework of Proposed Architecture

The suggested version performs a number of computations before generating data on the fly in a cloud environment; those calculations may be summarised in three easy steps, as illustrated in Fig. 4: Enterprise, DKD, and Open Cloud parts. - EC (Enterprise Control): EC (Enterprise Control) is a term that refer Customers execute various pre-processing activities on the entered data in this area before transferring it to the cloud environment via the following steps:

1. Aspects of the Customer: Stop using Mobile Scope for Users, Enterprises, and Remote Locations.
2. Cipher Cloud: Encryption and decryption issues for data and attached documents. This is further reinforced by the use of encryption algorithms such as AES, DES, and RSA.

DKD: DKD is a practical stationary technique in which all responsibilities are determined using quantum physics and computing factors. Although it is a blend of traditional cryptography, the concept of facts, and quantum physics [26], [27], it is not a natural mathematical progression. Within the proposed version, the DKD is the most significant portion; it has been understood as being dependent on the 1/3 section (TTP), which is responsible for key technology, key control, and key distribution. These keys are used to encrypt user-uploaded files or documents, which are mostly based on a set of fully symmetric encryption principles (AES). Furthermore, it has been taken into consideration thus far because it lies in the midst of the planned version, it is extremely difficult to notice or exploit. It is, however, simple to use and maintain, and it eliminates the computational layout complexity that classical cryptography entails.
Open Cloud Phase: This is the ideal portion for absorbing and calculating the percentage of files, packages, or attached documents on the Internet, such as Google Apps and Amazon EC2.

IV. SECURITY CHALLENGES IN CLOUD

When it relates to privacy and security, the cloud poses significant risks. People should certify, just like merchants, that the cloud of harassment is free of issues such as knowledge loss or data theft.

There is a possibility that a malicious user or hacker would enter the cloud under the guise of a normal user, affecting many of us who are infected or using the afflicted cloud. Cloud computing can be used in a variety of scenarios:

i. Data theft
ii. Data integrity
iii. Security issue
iv. Loss of sensitive data
v. Corrupt code
vi. Data abbreviation
vii. Data security at the business level
viii. Data security at the user level

The present generation of cloud computing features give no privacy against untrustworthy cloud operators, therefore vital data such as medical records, financial records, or high-impact corporate data are not asked to be stored.

To deal with this, we have a tendency to employ a variety of approaches that vary from theory to practise. The most

typical application of coding is to provide confidentiality by abstracting all useful information from plaintext. Coding transforms useless knowledge into something that can't be accessed.

To solve this challenge, we're developing cryptosystem algorithms that make it easier to do a range of calculations on encrypted raw data, ranging from traditional computations to special-purpose computations. Fully homomorphic encryption, searchable encryption, organised encryption, and practical encryption are all examples of homomorphic cryptography research.

a. Storage proofs. A buyer must check whether the cloud operator's Data Victimization Proof of Storage has been tampered with. It is frequently avoided by shoppers who save a clone of the information associate in nursing, despite the fact that it does not require any data to be stored back. In reality, the work is excellent.

b. ***Secure Storage system.*** We get a tendency to strive to design cloud storage systems that protect client data from a hostile cloud provider in terms of confidentiality, security, and integrity. The systems will need to be high-functioning and use the newest cryptanalytic coding techniques such as homomorphic encryption, searchable encryption, verifiable computation, and proof of storage, among others, to ensure confidentiality without sacrificing security.

V. CONCLUSION

Cloud computing is a rapidly evolving technology that has become the new trend, with many companies and large corporations migrating to the cloud. However, due to security concerns, the insulation is lagging behind. Cloud security is the ultimate edifice that can smash the flaws in huge multinationals', corporations', and organizations' cloud acceptance.

In the cloud, there are numerous security algorithms that can be used. DES, Triple-DES, AES, and Blowfish are examples of fundamentally symmetric algorithms. Symmetric algorithms are used in DES and AES because they are relatively secure. AES is more difficult to implement than DES. The algorithms used by RSA and Diffie-Hellman Key Exchange are very different.

Cryptography can be used for cloud security in a variety of ways. Cryptography will be utilized for cloud data access control, cloud data trust management, verifiable computing, cloud knowledge authorization and authentication, and secure data storage, to name a few applications.

Aside from these, full lattice based mainly cryptography and ID based cryptography are two major areas in the gifting world that ensure cloud data security. In this area, there is still a lot of research to be done.

REFERENCES

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing,"2009,

[2] http://www.wheresmyserver.co.nz/storage/media/faq-files/clouddef- v15.pdf, Accessed April 2011.

[3] Frank Gens, Robert P Mahowald and Richard L Villars. (2009, IDC Cloud Computing 2010).

[4] IDC, "IDC Ranking of issues of Cloud Computing model," ed, 2009, http://blogs.idc.com/ie/?p=210, Accessed on July 2011.

[5] Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases Version 3.0," 2010.

[6] Cloud Security Alliance (CSA). (2010). Available: http://www.cloudsecurityalliance.org/

[7] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109-116.

[8] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

[9] Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009, pp. 517-520.

[10] Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[11] S. Subashini, Kavitha, V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. In Press, Corrected Proof.

[12] Lohr, Steve. "Cloud Computing and EMC Deal." New York Times. Feb. 25, 2009. pg. C 6.

[13] McAllister, Neil. "Server virtualization." InfoWorld. Feb. 12, 2008. Retrieved March 12, 2008.

[14] http://www.infoworld.com/article/07/02/12/07FEvirtualserv_1.html

[15] Markoff, John. "An Internet Critic Who Is Not Shy About Ruffling the Big Names in High Technology." New York Times. Apr. 9, 2001. pg.C6

[16] G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, http://www.theregister.co.uk/ 2009/03/16/azure_cloud_crash/

[17] P. Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec Corporation, January 2007, http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats. pdf

[18] G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal,March 26, 2010

[19] L. Youseff, M. Butrico, D. D. Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop, held with SC08, November 2008.

[20] http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf
[21] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik. Scalable and e_cient provable datapossession. In Proceedings of the 4th international conference on Security and privacy in communication netowrks (SecureComm '08), pages 1{10, New York, NY, USA, 2008. ACM.
[22] Hodges, A. (2005), 'Can quantum computing solve classically unsolvable problems"
[23] H.K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrary long distances. Science 1999; 283(5410): 2050-2056.
[24] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/
[25] L. Lydersen, Wiechers, C., Wittman, C., Elser, D., Skaar, J. and Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photonics 4, 686, 2010.
[26] K. Inoue, Quantum Key Distribution Technologies. IEEE Journal of Selected Topics in Quantum Electronics, vol. 12, no.4, July/August 2006.
[27] http://ewh.ieee.org/r10/bombay/news4/Quantum_Computers.htm
[28] http://www.bbc.co.uk/news/scienceenvironment-16636580
[29] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm
[30] G. Brassard, T. Mor and B. C. Sanders, "Quantum cryptography via parametric downconversion", in Quantum Communication, Computing, and Measurement ,P. Kumar, G. Mauro D'Ariano and O. Hirota (editors), Kluwer Academic/Plenum Publishers, New York, 2000, pp. 381.
[31] P. D. Townsend, \Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems", IEEE Photonics Technology Letters, Vol. 10, 1998, pp. 1048.
[32] J. Brodkin. Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartnerseven-cloud- computing-security-risks-853, 2008.
[33] C.C.A: CipherCloud Gateway Architecture, www.ciphercloud.net.
[34] M. v. Dijk and A. Juels. On the impossibility of cryptography alone for privacy-preserving cloud computing. In Hot topics in Security (HotSec'10), pages 1{8. USENIX Association, 2010.
[35] Kamara and Lauter . CS2: A Searchable Cryptographic Cloud Storage System,IJSIR,2012.
[36] G. Ateniese, S. Kamara, and J. Katz. Proofs of storage from homomorphic identi_cation protocols. In Advances in Cryptology - ASIACRYPT '09, volume 5912 of Lecture Notes in Computer Science, pages 319{333. Springer, 2012.

ABOUT THE AUTHOR

Jaishree Jain is an Assistant Professor Computer Science & Engineering Department, Ajay Kumar Garg Engineering College, Ghaziabad, affiliated to AKTU, Lucknow, Uttar Pradesh, INDIA. She has 11 years teaching experience in CSE & IT Departments that include Chandigarh University, Punjab and college of AKTU, University, Lucknow since July 2010. She had done her B.Tech. in Information Technology from Uttar Pradesh Technical University, Lucknow. She had qualified GATE two times in 2007 & 2008 with 94.86 percentile. She had done her M.Tech. in Software Engineering from MNNIT, Allahabad. She had published about 27 research papers in SCI/SCOPUS/ UGC-Care/ UGC/National and International Journals Conferences and Chapter published in International Book. She had also been published one patent in August 2018. Her research interests include Image Processing, Cloud Security, and Steganography. She is also the reviewer of Journal of Supercomputing which is listed in Springer Journal and reviewed many papers till now. She is the member of professional bodies' i.e. life time member of ISTE, lifetime member of ICSES and member of Engineering Council of India (ECI) and position entitled as a "Professional Engineer" by ECI. INDIA.