International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Implementation of Different Cyptographic Strategies in Cloud Environment

Anil Gupta, Durgesh Kumar Mishra

Abstract—Cloud computing is hosted technology used to deliver services over internet. These services are broadly classified based on type of hosting i.e. infrastructure, platform and software. Public environment and internet connectivity make it vulnerable and unsafe for communication and storage. Confidentiality is one of the major principles to keep data privacy and protection at high level. Cryptographic techniques are used to achieve confidentiality and integrity of information during unsafe communication. This research paper observes that various cryptographic algorithms known as symmetric key cryptography and asymmetric key cryptography can be used to protect information and make it unreadable for unauthorised users. This research paper implements different security algorithms and observe their performance based on computation time over different input sizes. The complete research work concludes a comparative study and recommends different security approaches for different situations.

Keywords—Cloud computing, cloud security, confidentiality, cryptographic technique

I. INTRODUCTION

As specified by the MIT Technology, the expression "Cloud Computing" was apparently first used in 1990s. Most innovation specialists listed cloud computing as one of the most powerful IT patterns of the 21st century. In the era of recent decades, cloud computing has altered undertaking IT to the fact where most associations presently take a "cloud-first" way to deal with their innovation needs. Cloud servers with many advantages in terms of offering storage and resources as well as disadvantages in terms of security. In this paper, we are discussing some of the important concept by investigating relevant studies. Some of the security parameters are discussed below:

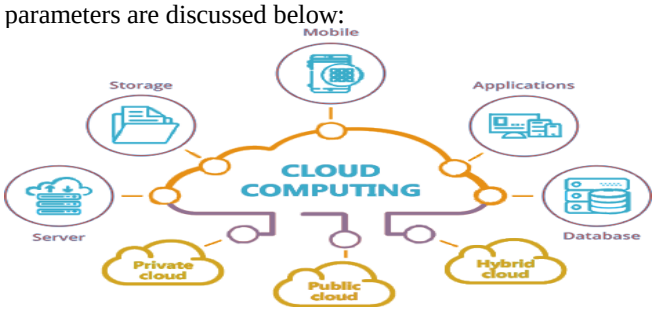

Fig. 1.Cloud computing

Manuscript published on January 30, 2020.
* Correspondence Author
Anil Gupta*, Department of CSE, Mewar University, Chittorgarh (RJ), India. Email: anil_sg@yahoo.com
Durgesh Kumar Mishra, Department of CSE, Department, Sri Aurobindo Institute of Technology (SAIT), Indore, MP India.
Email: drdurgeshmishra@gmail.com

A. Confidentiality:

Cloud computing is perhaps the most new topic and security is a significant part of cloud computing (CC). In CC, client's information stored on remote servers which might be functioned by others and can be accessed through intruders over Internet. There are high possibilities that the information might be challenged. Subsequently, secrecy of information became a major issue. Organization alludes to the anticipation of the unapproved access of the information and consequently ensuring that only the client who has the authorization can get to the information. This is one of the significant highlights of security. In this paper, we do an investigation of the issues identified with confidentiality in cloud computing and concisely talk about thoughts behind certain ways to deal with secure and improve the secrecy in cloud security.

Confidentiality is one of the five milestones of Information Assurance. The other four are verification, accessibility, respectability and nonrepudiation. With regards to personal system frameworks, enables approved clients to get to sensitive and ensured information. Explicit instruments guarantee privacy and defend information from unsafe intruders.

B. Cryptographic Technique:

Cryptographic techniques are utilized to guarantee confidentiality and integrity of information within the existence of an enemy. Under the security needs and the vulnerabilities involved, different cryptographic strategies, for example, symmetric key cryptography and asymmetric key cryptography can be utilized during transportation of the information. The essential elements of cryptography are encryption, decryption and hashing. So as to encode and decode messages, both the side need to share a common secret (Private) key. Usually, this key shows authentication which is in the form of password, that is utilized by the different algorithms of cryptography.

1) Symmetric Key: This encryption technique is known as single key based light weight encryption technique. This technique uses to convert planetext to ciphertext using single key. The key might be indistinguishable or there mightbe a little change to go between the two key. The key refer mutual serececy between the parties that are utilized to keep up private data.

- BLOWFISH: Blowfish is a single key base symmetric key cryptographic algorithm used as alternative for DES and IDEA for encryption purpose. It can have variable key length from 32 bits to 512 bits key. It was developed by Bruce Schneier in 1993 and adopted by multiple security system.

- AES: It is known as advanced encryption standard algorithm uses to develop cipher block of 128 bit with secure and cost effective execution.
- RC6: It is the successor of RC4 and RC5 developers and uses parameterized calculation. It can uses 2040 bit key for encryption.

2)*Asymmetric Key:* This cryptography technique is more secure than single key cryptographic technique which uses public and private key for encodes & decodes information. Shared key is known as public key and secrete key is known as private key. Encryption by one key needs another key for decryption. The keys are basically outsized in numbers that have been combined together yet are not indistinguishable. One key from the pair can be communicated to everybody, it is known as the share key. Any of the keys from both the key can be utilized to encrypt a message; the contrary key is utilized for decryption.

- RSA: RSA is a public-key cryptosystem and is broadly utilized for secure information transmission. In such a cryptosystem, the encoding key is share and decoding key is private key which is different. In RSA, this asymmetry achieve by the factorization of the result of two huge prime numbers, the "considering issue".
- ECC: Elliptic-curve cryptography (ECC) deals with open key cryptography dependent on the mathematical structure of elliptic curves over limited fields, it works on smaller keys. Elliptic bends are appropriate for key understanding, computerized marks, pseudo-irregular generators and different undertakings.

II. LITERATURE SURVEY

M. Thangapandiyan et al. In [1] proposed modifies elliptic curve cryptography algorithm to offers privacy to sensitive data. Separate keys are generated here for admin and user and the modified ECC uses for both encoding and decoding. When we access the information, both the admin and the user have to verify their identity. The recipients perform the Modified ECC algorithm and create private key for decoding information including characteristics. It is guarantees high level of information essence in CC.

Rohini et al. In [2] worked on security parameters to classify levels of authentication and storage level. As an ever-increasing number of organizations are putting away their information in cloud, concerns are developing about how safe this condition is. Cloud Security fuses numerous security confinements from the perspective of the client and cloud suppliers. Hybrid RSA approach is used by author for encrypting data and MD5 is used to calculate integrity.

Salma et al. In [3] abstracted significance of distributed computing turns out with the security of information openness, unwavering quality and dependability of data. The check and consent is progressively important to get to data as "cloud" through the world. Study made on security of document encryption using AES algorithm. Till now nothing effective assault than AES however since of a higher expanding of cyber crime in future it may be conceivable assault on it like savage power assault & arithmetical assault. Henceforth, the exploration introduced on Dynamic AES (DAES) & Blowfish algorithm. This strategy determines the security of transferred document on the cloud with a solid encryption technique & furthermore the protection and solid quality of submitted data of the client with thinking about execution of speed.

Wu Feng Sheng et al. In[4] Data security degree under the cloud computing stage straightforwardly influence the client's information security issue, and the utilization of encryption calculation that gives predominant qualities can compensate for impediments brought about by depending on programming security procedure, which is increasingly powerful and stable to conquer the trouble and challenge looked by the data security. In this paper, through considering the fundamental contemplations of the elliptic curve encryption calculation, an improved technique from the part of dynamic is planned dependent on elliptic curve cryptographic algorithm of cloud information insurance innovation to guarantee the framework running securely and proficiently, and the wellbeing test is made in Matlab programming. Test results show that the planned cloud information encryption innovation dependent on ECC calculation has high security and running velocity, and it can successfully ensure the security and soundness of cloud stage information.

III. PROBLEM DOMAIN

“Privacy is a state in which one is not observed or disturbed by other people” Privacy protection policy is an approach to isolate the sensitive information from unauthorized access. Cryptographic techniques are used to convert human readable text into non readable format. Security keys are used to make every transaction unique and generate different cipher text. Security algorithms always introduce extra computation and second level of effort to make things unreadable.

The study of existing solutions address that security algorithms always increase overhead of encryption and decryption. Asymmetric Key cryptographic algorithms not only need heavy computation and extra memory overhead but also look out for extra communication and bandwidth for key exchange. The study of cloud applications address that security can not be tolerate or take it granted due to open communication environment. This research paper attempts to compare all security algorithms and address their performance in terms of computation time. Relevant study represents security in cloud using algorithms and techniques, where known algorithms are picked and experimentation is performed by evaluating them better. The study speaks about multiple algorithms and refers that this algorithm is better than that algorithm but not specified about the algorithm which best fits for which application.

We made a study by investigating that which algorithm is better for cloud environment. Also, investigating for multiple verticals in cloud multiple perception.

IV. PROPOSED METHODOLOGY

Proposed methodology evaluates on five major objective: confidentiality, authentication, integrity, access control and non-repudiation. We are concentrating on confidentiality. Confidentiality and integrity are relevant to each other and are applied together. So we are investigating for the best algorithm while applying security in cloud. The important thought while applying security in cloud is to achieve major principles in cloud. Firstly, service level agreement is signed in cloud (for what to do and what not to do). Secondly, to achieve cryptography at client end. Third communication and fourth at storage level.

The three important level on which the work proposed is client side, communication side and server side. If we want to achieve confidentiality in cloud security then we have to add cryptographic technique. While using cryptographic technique, key based cryptography is proposed. Key based cryptography is of two type: symmetric key and asymmetric key.

Advantage of using symmetric key cryptography is there is no need to exchange key between server and client which saves the effort and bandwidth consumption while exchanging key and removes third party dependency for key exchange. Relatively, it is more veteran in time and memory vice. Key compromised is the basic drawback of symmetric algorithm where anyone can access data but now with the upgradation in technique it is not easy to compromise key simply, it is not simple and easy to get key compromised. Another drawback is if there is confidentiality then authentication cannot be achieved and if there is authentication then confidentiality cannot be achieved. Symmetric key have many popular algorithms like AES, RC6 and BLOWFISH. So these three algorithms are implemented in proposed work.

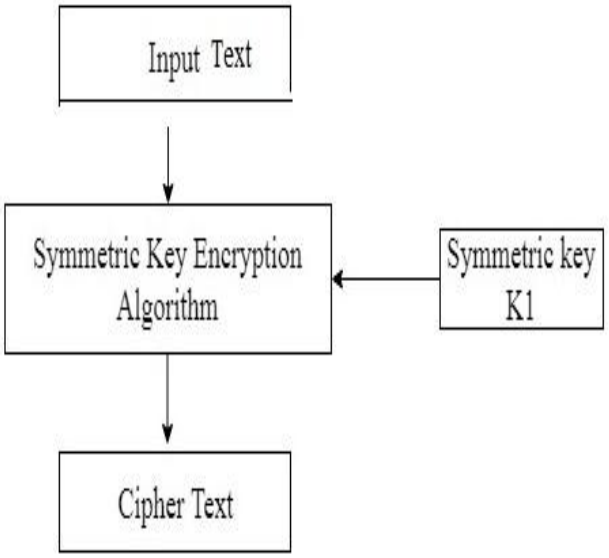

Fig. 2.Encryption using Symmetric Key

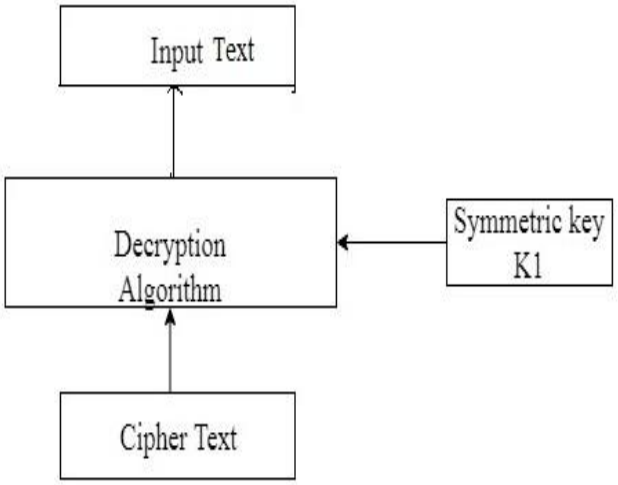

Fig. 3.Decryption using Symmetric Key

Now talking about asymmetric key we can achieve confidentiality & integrity both using the single algorithm. It works on private key and public key where, private key is used to encrypt then authentication is achieved and its public key is used to decrypt. Drawback of asymmetric algorithm is it increases overheads. But using asymmetric both confidentiality and integrity can be achieved using single algorithm. In case if key compromised then also there is no worry because fro encryption private key is used and for decryption public key is used. Private key is with the person who encrypted the data, till the infrastructure is not compromised, the complete concept will not fail. For this we implemented RSA and ECC algorithm.

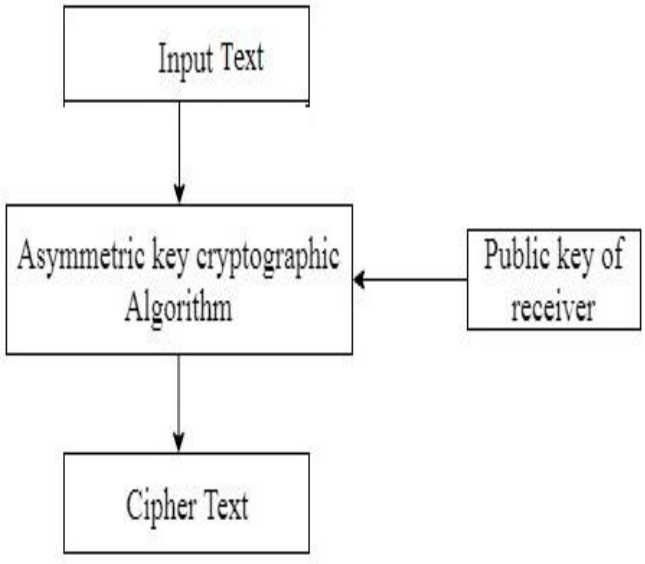

Fig. 4.Encryption using Asymmetric Key

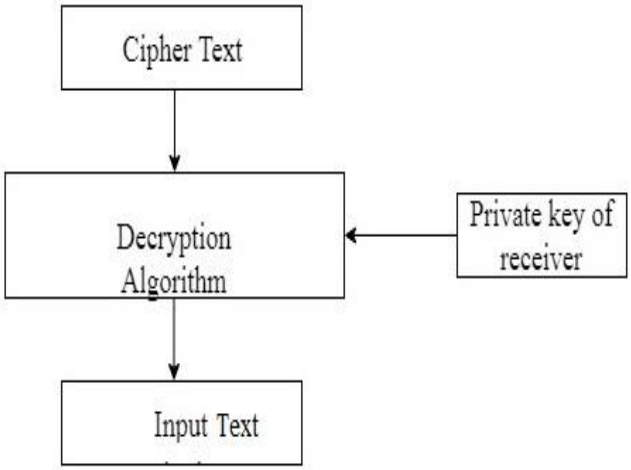

Fig. 5.Decryption using Asymmetric Key

V. EXPERIMENTAL ANALYSIS

Experimental analysis enhance working on different size of data like 1KB, 10KB, 100KB, 1000 Kb and 10,000 KB, and on it different cryptography technique like RC6, AES, BLOWFISH, ECC and RSA is applied for the comparison of performance and evaluate the performance of encryption time and decryption time in terms of milliseconds.

Table 1: Encryption Time

Data [KB]	AES	RC6	Blowfish	RSA	ECC
1 KB	3	2.5	26	112	85
10 KB	19	16	40	212	115
100 KB	95	62	56	513	390
1000 KB	215	165	66	2356	856
10000KB	1856	1325	104	4569	1669

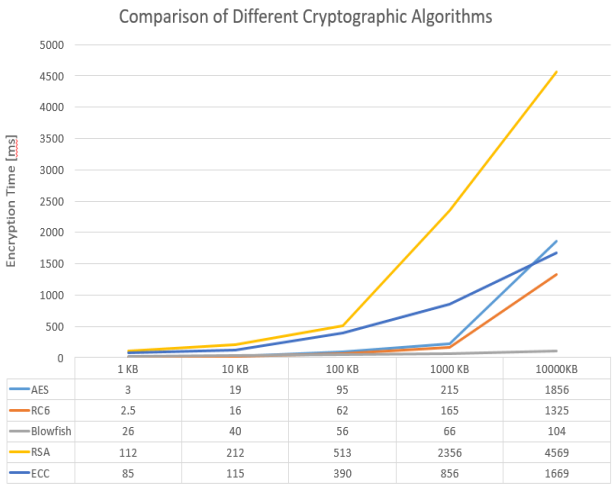

Fig5: Comparison of Encyption Time

Table 2: Decryption Time

Data [KB]	AES	RC6	Blowfish	RSA	ECC
1 KB	4	3	29	186	109
10 KB	23	19	48	289	156
100 KB	101	78	65	796	456
1000 KB	245	195	79	2656	956
10000KB	1986	1675	125	4969	1869

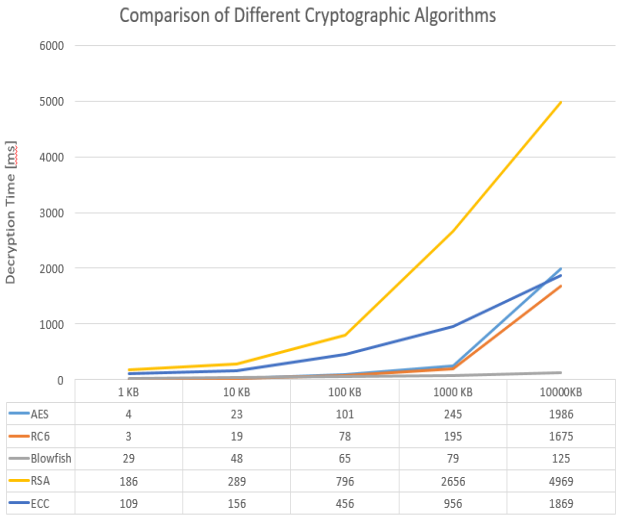

Fig 6: Comparison of Decryption Time

VI. CONCLUSION

In the complete work we exhibited an outline about confidentiality in cloud computing and highlighted upon the significance of preserving the secrecy in the cloud. The point of this review was to feature the confidentiality issues related with cloud computing by utilizing cryptographic technique.

We have developed a cloud based application where we implemented these 5 algorithms (RC6, AES, BLOWFISH, RSA and ECC) using restful API. Here, evaluation is performed by checking the behaviour of algorithm using the same type of data with same size on the same machine configuration. The complete implementation address that symmetric key cryptographic algorithms create less overhead in comparisons with asymmetric key cryptographic algorithms but they are less secure due to single key concept. ECC perform better than RSA and Blowfish perform better that RC6 and AES in symmetric key category. The complete work proposed that in future hybrid cryptographic solution could be develop to achieve high strength security with authentication and integrity.

REFERENCES

1. M. Thangapandiyan, P. M. R. Anand and K. S. Sankaran, "Enhanced Cloud Security Implementation Using Modified ECC Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 1019-1022.

2. Rohini and T. Sharma, "Proposed hybrid RSA algorithm for cloud computing," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 60-64.
3. Salma, R. F. Olanrewaju, K. Abdullah, Rusmala and H. Darwis, "Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms," 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), Makassar, Indonesia, 2018, pp. 18-23.
4. F. S. Wu, "Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm," 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Changsha, 2018, pp. 125-129.
5. Akhil K.M, Praveen Kumar M, Pushpa B.R, "Enhanced Cloud Data Security Using AES Algorithm". 2017 International Conference on Intelligent Computing and Control (I2C2).
6. B. Lee, E. K. Dewi and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," 2018 27th Wireless and Optical Communication Conference (WOCC), Hualien, 2018, pp. 1-5.
7. K. Rani and R. K. Sagar, "Enhanced data storage security in cloud environment using encryption, compression and splitting technique," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-5.
8. S. Ojha and V. Rajput, "AES and MD5 based secure authentication in cloud computing," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 856-860.
9. P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1635-1638.
10. I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 172-175.
11. P. N. Hemanth, N. A. Raj and N. Yadav, "Secure message transfer using RSA algorithm and improved playfair cipher in cloud computing," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 931-936.
12. A. Bansal and A. Agrawal, "Providing security, integrity and authentication using ECC algorithm in cloud storage," 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 2017, pp. 1-5.
13. S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 267-271.
14. S. Mudepalli, V. S. Rao and R. K. Kumar, "An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 267-271.
15. V. P. Bansal and S. Singh, "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs," 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), Chandigarh, 2015, pp. 1-5.

AUTHORS PROFILE

Anil Gupta has received MCA from Devi Ahilya Vishwavidyalaya, Indore, India in 1998, Technical Master degree in IT from AAI-DU Allahabad, India in 2005 and BE (Bachelor of Engineering) in CSE from RGPV Bhopal, MP in 2014. He is doing PhD on "Design of Novel Strategy to provide Security in Cloud Computing". He completed 22 years in teaching. He enjoys teaching subjects like Computer Architecture, Computer Networking, Network & Information Security, Computer Graphics and Cloud Computing. His four research papers are selected in International Conferences and Journals and ten research papers in National conferences. He is interested to work in the area of Security in Cloud Computing and Network Security. He is a active member of CSI India.

Dr. Durgesh Kumar Mishra did Technical master degree in Computer Science from DAVV, Indore, MP in the year 1994 and Doctorate degree in Computer Engineering in the year 2008. Currently working as Professor (Computer Science and Engineering) and handle the responsibility of Director of Microsoft Innovation Centre at Shri Aurobindo Institute of Technology (SAIT), Indore, India. Dr. Durgesh Kumar Mishra is also a visiting faculty at IIT-Indore, India. He completed more than 24 years in the field of teaching and 10 years in research. Dr. Mishra has completed his PhD under the supervision of Dr. Manohar Chandwani on "Secure Multi-Party Computation for Preserving Privacy". He wrote more than 90 papers international/national journals in refereed category and conferences including IEEE, ACM conferences. He has been the organizer of many such conference like WOCN, CONSEG and CSIBIG in the capacity of conference General Chair and editor of conference proceeding. Dr. Mishra's publications are listed in DBLP, Citeseer-x, Elsevier and Scopus. He is awarded as Senior Member of IEEE and held many positions like Chairman, IEEE MP-Subsection (2011-2012), and Chairman IEEE CS Mumbai Chapter (2009-2010). In CSI, selected as Chairman CSI (Division IV) Communication at National Level from year 2014 to 2016. He delivered his invited talk in Singapore, Nepal, Taiwan, Bangladesh, UK, France and USA. Dr. Mishra authored a book "Database Management Systems". He has been a consultant to sales tax and labor department of Govt of MP, India. He has been awarded with "Paper Presenter award at International Level" by CSI. He presented his presentation on Security and Privacy at MIT Boston. He also chaired a panel on "Digital Monozukuri" at "Norbert Winner in 21st century" at BOSTON. Dr. Mishra became the Member of Bureau of Indian standards, Govt. of India for IS domain.