International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Design and Implementation of Strong Authentication Model to Improve Performance of Cloud Computing in Hybrid Cloud Environment

Anil Gupta, Durgesh Kumar Mishra

Abstract: ***Cloud computing became a part of everyday life. We allow us to support the device with accessibility across platforms regardless of the location. It has become vulnerable to several security threats because of public environment and internet participation. At this point the attack by hackers can break down the security and leak the information. Data is recognized in the cloud computing as an important corporate asset which must be safeguarded from unwanted internal or external threats. Data encryption provides data protection on sensitive data but also raises computation and memory overhead during large data processing on cloud.Cloud computing also requires low overhead operation to keep the computation as soon as possible. To authenticate the client we apply modified Kerberos protocol.***

Keywords: Cloud, Cloud Computing, Data Protection, Kerberos protocol.

I. INTRODUCTION:

Cloud is an open, virtual storage platform and computing environment. It provides an Anytime, Anywhere, Anything over the Internet, one-stop service to end users. The cases that consumer data leaks from the cloud storage platform continue to emerge, anyway. Protection must be the priority concern to boost cloud effectiveness because internet development increases the attacks on cloud computing. Before, data leak was very unusual and data hacked due to human error, for example damaging physical devices such as laptop, pen drive, floppy disk. Some other forms of data theft is through the use of cloud computing weaknesses, through unknowingly clicking the wrong link. Organizations suffering from data leak or theft may not know the reason behind this, or have made no effort to find it. Data leak, data theft, and modification by robbers are increasing day by day in recent years. This unauthorized access of people's sensitive data forces the government to start data privacy laws like GDPR (General Data Protection Regulation). It is very important to provide protection to the cloud computing because cloud computingare open to the internet and also cloud computing is online data sharing, and most of the unauthorized access and manipulation of data is done through it. One of the studies shows 77 percent of web applications have at least one vulnerability in security. In order for attackers to install the malware successfully, to remotely control the uncovered computer without coming into the notice and to find the data to steal requires a large amount of time which increases the chances of being caught. As a result, attackers try to access sensitive information by using the cloud computing security vulnerabilities. Such types of attacks are more effective and efficient. The vulnerabilities of the cloud computing give the attackers some way to freely access the data stored on that server.

Revised Manuscript Received on March 30, 2020.

***** Correspondence Author

Anil Gupta*, CSE Department, Mewar University, Chittorgarh (RJ), India, Email: anil_sg@yahoo.com

Durgesh Kumar Mishra, CSE Department, Sri Aurobindo Institute of Technology (SAIT), Indore, MP India, Email: drdurgeshmishra@gmail.com

LITERATURE REVIEW:

The literature Review describes the work is done by others. A brief review of the work already done in this field is cited below:

M. Abdullah Khalid et al. In [1] the proposed hybrid security protocol, consolidates asymmetric key cryptography attributes that provide a simple way to share key and symmetric cryptography that is easier to calculate and faster. In the proposed work user id password with captcha, IP and MAC address verification; OTP verification and Kerberos authentication are used for more security. The proposed work reduces the text size of the cipher and the time to encrypt / decrypt. That provides a good and easy method to verify data transmission. In general it has a few decent focal points, such as the standard of straightforwardness and high safety. Additionally it decreases the rate of packets dropped. Contrasting the proposed half-and - a-half calculation with a couple of different calculations has shown that the HCA generally acquires the best results. The hybrid model does not provide for data integrity.

PROBLEM STATEMENT:

The complete project issue describes the need for protection parameter where safety is important for saving any sensitive data. Sensitive data can be personal data or detail related information that nobody should know. Another concern is the issue of trust where third party organizations automate their data for use by consumers. User does not rely on third parties or it frequently happens that thirdparty providers are not reliable. Authentication and authorization are the major security issues that need to be solved in such a way that only the approved person is eligible for authentication and access. The user, who performs an unauthorized activity, is the malicious attacker or robbers that must be preserved and diagnosed for future security purposes at the right time.

The algorithms suggested by the Previous System work either on confidentiality or integrity or authentication. This type of protection criteria have not been reached at the same time in any of the previous work. Researchers first use the primary encryption which suffers from the issue of extra computation time.

However, it provides less security than Kerberos authentication. The proposed study often fails to achieve authentication and honesty. Hence, the best techniques for securing data in cloud computing were implemented to overcome these proposed work problems. The methodology proposed will give the best and quickest way to secure data in cloud computing. Therefore, confidentiality, integrity and authentication are applied in a single framework, by incorporating the proposed work user, certain criteria can be accomplished in all, where users can obtain protected and original data, authenticated and allowed access, and confidentiality to upload or download their data.

METHODOLOGY

The proposed solution describe the secure process like some authentication scheme such as user ID password, mobile verification, security token, OTP verification, Kerberos server and through security question in one authentication model. The objective of proposed model is to improve the performance of authentication by reducing the security overhead.

This work identify that following popular techniques are used to authenticate the identity of user before serving the services.

Username & Password technique
Security Question
Third Party authentication using Security Token
OTP Verification using Mobile Phone
IP & MAC Verification
Server Verification using Kerberos

This work examine that there are multiple cases when user will try to get login into system. Here, few most popular cases are considered to proposed authentication layer in particular situation. Case 1: Registered User Login from Registered Computer Machine in Private Network This is the safest situation when user will used inside premises registered computer to get login into machine or ERP Solution to access the services. Proposed solution identifies that only username and password technique can be suffered with brut force attack and considers being vulnerable. This system proposed that integration of captcha with login process can ensure the human interaction and raise the level of security within network. IP and MAC address verification: This technique will increase the level of security as background process. It will retrieve user machine IP and MAC address and verify with registered credentials. It will ensure that only registered machines can be used to access the services.

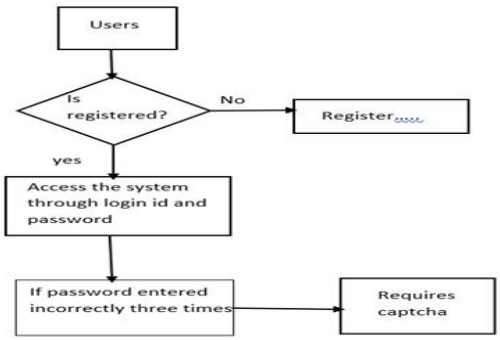

Fig 1: Block diagram of Authentication

Proposed solution address that username and password technique with captcha and IP-MAC verification technique to improve the security strength and overcome the overhead.

Following Steps will evolve to implement authentication.

1. Username & Password Technique
2. Captcha Verification to ensure human interaction
3. IP & MAC Verification to identity of registered machine

Case 2: Registered User Login from Registered Computer Machine in Public Network

This may be vulnerable situation because user is trying to get login from public network. Agree users' machine is registered and safe but the network he is going to use is vulnerable and can be used to compromise information. Existing systems proposed to use Third party authentication using one time password. To implement this feature either we have to used security token or mobile device. Security token could not only need extra amount to purchase device but will also required to carry it all time. Mobile integration could help to reduce this cost as well carrying extra device.

A one-time PIN code is a code that is valid over a mobile phone for just one login session or transaction. It is often used in two-factor authentication or 2FA to provide the user with an extra layer of security when using an ATM machine or when attempting to login to a service from another computer. But every time OTP need consume of money 10-25 paisa. This process is used by registered user and unregistered system.

Following Steps will evolve to implement authentication.

1. Username & Password Technique
2. Captcha Verification to ensure human interaction
3. IP & MAC Verification
4. OTP Verification using Mobile Phone Device

Case 3: Registered User Login from Unregistered Computer Machine in Private Network

If registered user is trying to get login from unregistered system but within premises in private network, a mobile verification will automatically prompt to authorized user and improve the level of authentication.

1. Username & Password Technique
2. Captcha Verification to ensure human interaction
3. IP & MAC Verification
4. OTP Verification using Mobile Phone Device [If user is trying to get login from unregistered machine]

Case4: Registered User Login from Unregistered Computer Machine in Public Network

This will be most unsafe situation which will required all type of authentication to ensure user with identify and rights of access. Proposed solution suggests that Kerberos integration can help to improve security strength and authorize the allotment of services according their rights.

Kerberos is used for authentication and a session key which can be used for confidentiality and authenticity purpose.

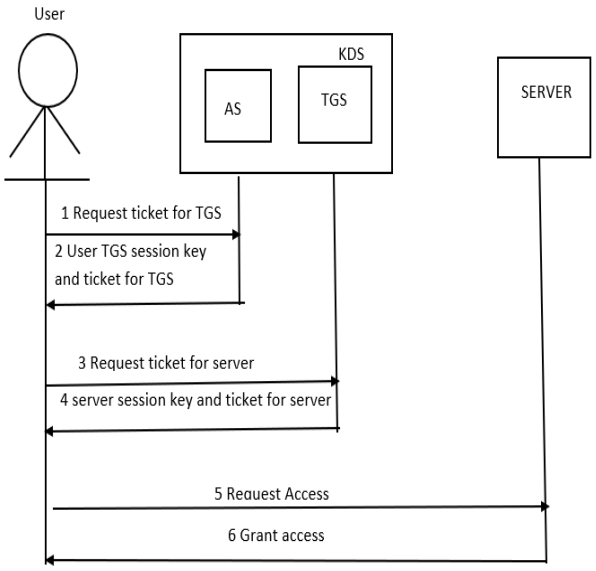

Fig 2: Block diagram of Kerberos authentication

There are three steps involved in Kerberos authentication:

Login:

- User uses a public workstation and enters their name which is sent to the AS (Authentication server) in plain text.
- Now AS (Authentication Server) first generates a username package and a session key (KS) created at random. This package is encrypted with the symmetric key the AS shares with the Ticket Granting Server (TGS).
- This step's output is called a Ticket Granting Ticket (TGT). The TGT can only be opened by the TGS as it has the appropriate symmetric key to decrypt.
- The AS then combines the TGT with the session key (KS) and encrypts both using a symmetric key derived from user's (KA) password.
- The user's workstation asks for a password after receiving the message. When user enters it the workstation generates the password-derived symmetric key (KA) and uses it to extract the session key (KS) and the TGT.

Obtaining a service granting ticket (SGT) –

- User wants to make use of server to communicate after a successful login. To do this user needs a ticket to get in touch with server. At this point, the workstation of user produces a message for the ticket granting server (TGS) containing the TGT, the server ID and the current time stamp encrypted with the same session key(KS).
- Once TGS is satisfied with user's credentials, the TGS creates a KAB session key for user to communicate securely with server. TGS sends it to user twice, once combined with server's Id and encrypted with KS, and again combined with user's Id and encrypted with server's secret key (KB).

User contacts Server for accessing server-

- Now, user will give KAB to server to enter a session with them. Since this exchange is also desired to be secure, User can simply forward Server's secret key to KAB encrypted. This will ensure KAB is accessible only to server. Now server adds 1 to user's time stamp, encrypts the result with KAB and sends it to user.
- Because KAB is known to the user and the server, the user can open this packet and verify that the timeline incremented by the server was actually the one sent to the server.
- User and server can now securely communicate to encrypt messages via the shared secret KAB key.

If the user wishes to communicate with a different server they will need another TGS shared key and specify the name in the message.

1. Username & Password Technique
2. Captcha Verification to ensure human interaction
3. IP & MAC Verification
4. OTP Verification using Mobile Phone Device [If user is trying to get login from unregistered machine]
5. Authentication using Kerberos Authentication Server

To ensure the confidentiality of content and key, ECC and Blowfish algorithm is proposed to integrate as encryption algorithm to provide data privacy.

Case	Security Case	Authentication Technique
1	Registered User Login from Registered Computer Machine in Private Network	• Username & Password Technique • Captcha Verification to ensure human interaction • IP & MAC Verification to identity of registered machine
2	Registered User Login from Registered Computer Machine in Public Network	• Username & Password Technique • Captcha Verification to ensure human interaction • IP & MAC Verification • OTP Verification using Mobile Phone Device • Integration of ECC Algorithm to keep data secure in public network
3	Registered User Login from Unregistered Computer Machine in Private Network	• Username & Password Technique • Captcha Verification to ensure human interaction • IP & MAC Verification • OTP Verification using Mobile Phone Device [If user is trying to get login from unregistered machine]

			public network
4	Registered User Login from Unregistered Computer Machine in Public Network	• Username & Password Technique • Captcha Verification to ensure human interaction • IP & MAC Verification • OTP Verification using Mobile Phone Device [If user is trying to get login from unregistered machine] • Authentication using Kerberos Authentication Server • Integration of ECC & Blowfish Algorithm to keep data secure in	

II. EXPERIMENTAL ANALYSIS:

The results analysis for the complete work describes the performance of the hybrid algorithm proposed in terms of cipher text size, encryption and decryption time taken by the hybrid algorithm proposed. We calculate the time of computation using different size of the paper. The hybrid algorithm proposed is also compared with the algorithms already in place.

Table 1: Total Encryption Time taken by the proposed algorithm in Case 4 Public Network

Size of plain text (kilobytes)	ECC Time ms	Blowfish Time ms	Authentication Time	Total Time Ms
1 kb	210.68	0.98	13.02	224.68
5 kb	184.87	7.76	14.39	207.02
10 kb	469.02	8.06	13.42	490.5
20 kb	510.34	22.05	13.13	545.52
50 kb	1180.45	27.42	13.85	1231.72
100 kb	2010.03	62.09	15.56	2087.68

The above table shows the time taken by the proposed algorithm for encryption. In the above table size of plain text are in kilobytes (kb) and time taken by ECC, Blowfish and message digest are in milli second (ms) where ECC and Blowfish are used for encryption and decryption. Total time required to encrypt the file is shown in the table 1. In Figure it is represented in graphical form to show a statistical view.

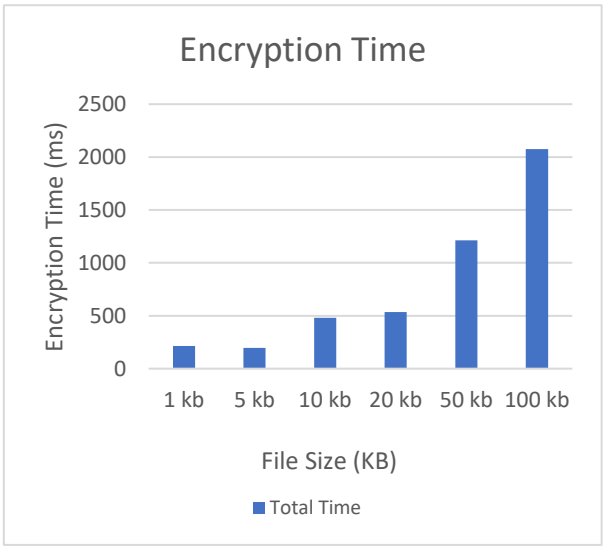

Fig 3: Encryption Time

The decryption time is the time taken by the algorithm to produce the plain text from the cipher text. Similar to the encryption time process, the decryption process as follows. Total time required to decrypt the file is shown in the table 2. In Figure 4 it is represented in graphical form to show a statistical view.

Table 2 Total Decryption Time taken by the proposed algorithm Case 4 Public Network

Size of plain text (kilobytes)	ECC Time ms	Blowfish Time ms	Authentication Time	Total Time ms
1 kb	62.250	7.1287	13.02	61.543
5 kb	240.410	11.876	14.12	120.462
10 kb	679.121	26.754	13.42	174.432
20 kb	1140.024	51.512	15.12	207.706
50 kb	2876.234	80.464	13.02	468.342
100 kb	4675.204	176.577	13.49	624.004

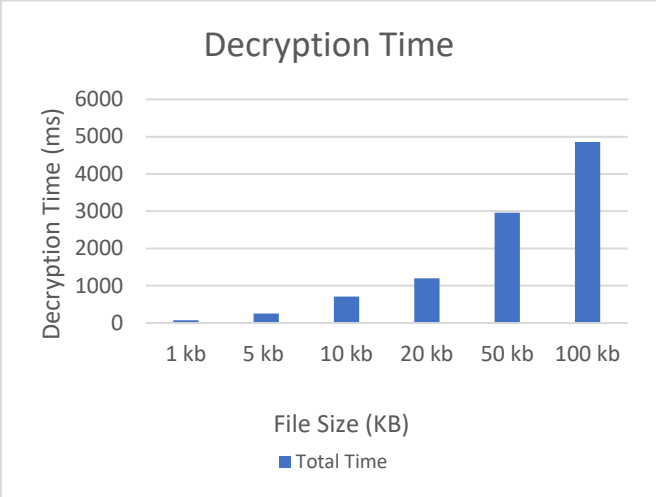

Fig 4: Decryption Time

Comparison with Existing Solution

Comparison of time required in proposed work and existing work to encrypt and decrypt the file is shown below. Algorithms used in proposed work is compared with algorithms used in existing work (HCA + THCA) is shown in tabular form in Table 3 and represented in the form of a graph in Figure 5.

Table 3 Comparison Table of Encryption/Decryption Time of the proposed algorithm with existing algorithms

Algorithms 3	Encryption Time (ms)	Decryption Time (ms)
Proposed Algorithm	155.3089	54.7865
HCA	612	342
THCA	1107	654

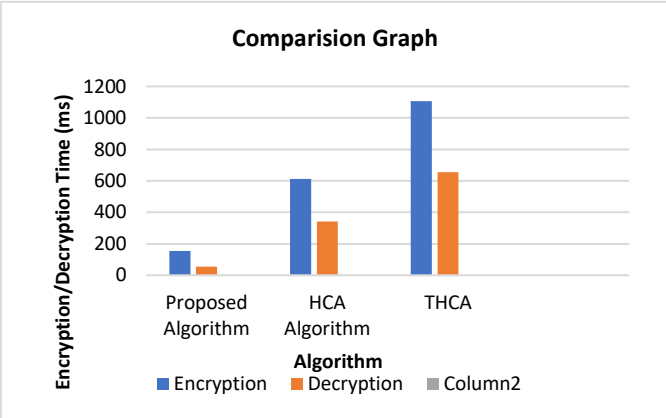

Fig 5: Comparison Graph of Encryption/Decryption Time of the proposed algorithm with existing algorithm

III. CONCLUSION:

This work concludes that we try to ensure authentication, confidentiality and integrity in the proposed hybrid model to protect the data from unauthorized access in web applications. To improve the security structure, we have provide a security model defining different security mechanism to improve performance of cloud environment in different situation along with encryption algorithm, To improve the level of confidentiality, ECC & Blowfish algorithms are implemented.

The complete work concludes that removing of mobile verification and Kerberos from private network help us to reduce lots of effort. Subsequently, integration of IP & MAC address verification help to keep the level of security at higher level and reduce the overhead of cost and time by removing mobile OTP verification.

We observe during Implementation that the encrypted data size is large than the plain text. The encrypted data size can be popular in the future without having to negotiate with encryption and decryption times. With different types of files other than.txt files with example.mp4,.doc, etc., the suggested hybrid model can also be applied. It can be used in the future for specific applications such as military applications, hardware and software companies needing security in their products, large websites with large databases, mobile applications and cloud-based applications.

REFERENCES:

1. Khalid M. Abdullah Essam H. HousseinHala H. Zayed, “New Security Protocol using Hybrid Cryptography Algorithm for WSN”. 1st International Conference on Computer Applications and Information Security (ICCAIS), IEEE, 4-6 April. 2018
2. Milind Mathur, AyushKesarwani, “Comparison between DES, 3DES, RC2, RC6, BLOWFISH, and AES”. Proceedings of National Conference on New Horizons in IT – NCNHIT 2013.
3. V. Kapoor, Rahul Yadav, “A Hybrid Cryptography Technique for Improving Network Security”, International Journal of Computer Applications, Volume 141, No.11, May 2016.
4. M. Harini, K. Pushpa Gowri, C. Pavithra, M. PradhibaSelvarani, “A Novel Security Mechanism Using Hybrid Cryptography Algorithms”. International Conference on Electrical, Instrumentation, and Communication Engineering (ICEICE), IEEE 2017.
5. Kalyani Ganesh Kadam, Prof. Vaishali Khairnar, “HYBRID RSA-AES ENCRYPTION FOR WEB SERVICES”. International Journal of Technical Research and Applications, Issue 31(September 2015), PP. 51-56.
6. F. Fatemi Moghaddam, S. Gerayeli Moghaddam, S. Rouzbeh, S. KohpayehAraghi, N. MoradAlibeigi, and S. DabbaghiVarnosfaderani, “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments,” in IEEE Region 10 Symposium, Kuala Lumpur, Malaysia, 2014, pp. 508–513.
7. JayrajGondaliya, JinishaSavani, Vivek Sheetal Dhaduvai, Gahangir Hossain, “Hybrid Security RSA Algorithm in Application of Web Service”. 1st International Conference on Data Intelligence and Security IEEE 2018.
8. KirtirajBhatele, Prof Amit Sinhal, Prof Mayank Pathak, “A Novel Approach to the Design of a New Hybrid Security Protocol Architecture”. International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) IEEE 2012.
9. A. Arjuna Rao, K Sujatha, A Bhavana Deepthi, L V Rajesh, “Survey paper comparing ECC with RSA, AES and Blowfish Algorithms”. International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 1, IJRITCC January 2017.
10. Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk, “A New Security Protocol Using Hybrid Cryptography Algorithms”. 9th International Computer Engineering Conference (ICENCO), IEEE 2013.
11. Nair, Nikhitha K., K. S. Navin, and Soya Chandra. "Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing." (2015).

12. Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." INFOCOM, 2010 Proceedings IEEE, 2010.
13. Hyun-Suk Yu, Yvette E. Gelogo, K J Kim, "Securing Data Storage in Cloud Computing", J. of Security Engineering, June 2012, pp.252-259.
14. Khanna, Abhirup. "RAS: A novel approach for dynamic resource allocation." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.
15. Hendre, Amit, and Karuna Pande Joshi. "A semantic approach to cloud security and compliance." 2015 IEEE 8th International Conference on Cloud Computing. IEEE, 2015.
16. KhushbuJakhotia, Rohini Bhosale, Dr.Chelpa Lingam, "Novel Architecture for Enabling Proof of Retrievability using AES Algorithm". Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).
17. Akshay Arora, Abhirup Khanna, Anmol Rastogi, Amit Agarwal, "Cloud Security Ecosystem for Data Security and Privacy". 7th International Conference on Cloud Computing, Data Science & Engineering – Confluence, 2017.
18. V. Kapoor, "A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security", International Journal of Science Research in Network Security and Communication, Vol. 1, Issue 2, June 2013.
19. Amrita Jain, Vivek Kapoor, "Secure Communication using RSA Algorithm for Network Environment", International Journal of Computer Applications, Vol. 118, No. 7, May 2015.
20. B. Hari Krishna, Dr. S. Kiran, G. Murali, R. Pradeep Kumar Reddy, "Security Issues In Service Model Of Cloud Computing Environment".

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.