Security Concerns & Cryptography in Cloud Computing

Vartika Kulshrestha [1], Prof. Seema Verma[2], Prof. C. Rama Krishna[3]

[1,2]*Dept. of Electronics, Banasthali Vidyapith, Jaipur, India.*

[3]*NITTTR Chandigarh, India.*

Abstract- The "cloud" has turned into a fixture, for almost everything: reinforcement and recuperation (e.g. Dropbox), correspondence (Skype, WhatsApp), profitability (Microsoft Office 365, Google Docs), adaptable use (Netflix), business process (Salesforce), long range informal communication (Facebook, LinkedIn, Twitter), and the sky is the limit from there. Consistently there are more organizations putting away information and running workloads in the cloud. With that development, in any case, additionally comes a bigger focus on your back. Digital Attackers have a tendency to pursue the most minimal hanging natural product from the biggest pool of conceivable targets—making web applications and information an essential core interest. According the Thale's report published in 2018, 67% of the data has been compromised. This paper abridges various associate investigated articles on security dangers in distributed computing and the preventive techniques. The aim of this analysis is to comprehend the cloud parts, security issues, and dangers, alongside developing arrangements that may possibly alleviate the vulnerabilities in the cloud by using RSA cryptosystem.

Keywords*-cloud computing; security; digital attackers; vulnerabilities; RSA cryptosystem.*

I. INTRODUCTION

"The cloud alludes to programming and administrations that keep running on the Internet, rather than locally on your PC. Most cloud administrations can be gotten to through a Web program like Firefox or Google Chrome, and a few organizations offer committed portable applications."

NIST characterizes cloud computing (CC) by portraying five fundamental attributes, three cloud benefit models, also, four arrangement models [1]. The basic attributes are quick flexibility, on request self-service, wide system access and asset pooling. The cloud has four diverse deployment models as per clients' needs. These are; open cloud, reserved cloud, mixture (hybrid) cloud and group cloud [2]. "Gartner characterizes distributed computing as "a style of registering where enormously adaptable IT empowered capacities are conveyed 'as an administration' to outside clients utilizing Internet advances [2]." Cloud suppliers at present enjoy a significant open door in the commercial world. The traders must ensure that the security perspectives ideal will be given to them because they will endure the responsibility if something turn out badly. Distributed computing offers some rare benefits like "*quick arrangement, pay-for-utilize, bring down costs, adaptability, fast provisioning, fast flexibility, pervasive system, more prominent strength, hypervisor insurance against organize assaults, minimal effort calamity recuperation and information stockpiling arrangements, on-request security controls, alteration of ongoing location of framework and fast re-constitution of administrations* [3]". While the distributed computing offers these benefits, until the point that some of the endangerments are better realized, a noteworthy number of the major organizations will be enticed to keep down.

As per a current IDCI overview, 74% of information processing [4] executives and CIO's referred to security as the topmost challenge [5]. To understand this massive latent, professional must discourse the fortification queries upraised by this innovative processing model. Distributed environment made a capable impact in the scholarly community and IT industry. But ambiguities also occurs in IT social order regarding the cloud shifting from obtainable prototypes and how the prototypes refinements influence its receptions. Some watch a CC as a novel particular uprising, while others contemplate it a trademark headway of advancement, low-cost, and philosophy prototype. It can be stated that disseminated processing is a basic perspective, with the possibility of declining the financial expenditure through streamlining and extended working and money related efficiencies. Cloud computing enhance the participation, deftness, and scale, in this way captivating an operational virtual framework [6].

While cloud computing accompanies a several points of interest –information can be accessed on any gadget with a web association, team up with partners on a similar report, store a great deal of information requiring little to no effort – it also accompany numerous entanglements. "Analysts' gauge that in the next following five years, the worldwide market for cloud computing will develop to $95 billion and that 12% of the overall programming business sector will move to the cloud in that period [6]."

As per a Forbes' available report in 2015, cloud-based security expenditure is expected to rise by 42%. According to another exploration, the IT security consumption had expanded to 79.1% by 2015, demonstrating an expansion of over 10% every year. International Data Corporation (IDC) in 2011 demonstrated that 74.6% of big business clients positioned security as a noteworthy challenge [7]. In 2014, data breach has affected the JPMorgon and its stored 83 million consumer's details has been exposed [8]. Recently in 2017, Ransomeware, Notpetya and Bad Rabbit hit the several organizations and cost more than $8 billion. Regardless, without suitable security and protection, these issues can change the viewpoint of cloud adoption and lead into a huge disappointment [9].

II. SECURITY CONCERNS OF CLOUD COMPUTING

Currently more than 50 cloud software applications have been used by the 42% of the organization where as 57% uses the 3 or more cloud infrastructures and 53% of the users uses the cloud platforms [10]. Almost 91% of the consumers uses the mobile payment and 90-95 % are implementing the IoT techniques [10]. This haste to embrace new cloud environment has created the more vulnerabilities. Like in 2017, a huge data breach occurred in Amazon S3 which has affected the financial behemoth Dow Jones and US Republican party [8]. Ransomeware is not the only big security risk [9] to cloud environment – according to the Cloud Security Alliance (CSA) [11][6] there are more, which has been discussed below:

A. Data Breach

Cloud suppliers are the appealing focus for the programmers to assault as enormous information are stored on the cloud. An information breach may be the main objective of a targeted assault or may basically be the consequence of human mistake, application vulnerabilities or poor security rehearses how much extreme the assault is rely on the secrecy of the information which will be uncovered. This could include data not proposed for open discharge, for example, individual wellbeing data, monetary data, by and by identifiable data (PII), exchange mysteries and scholarly property. At the point when information broke happened, lawsuit is filed against these organizations and felonious accusations too. Unusual things, like, stamp destruction and business damage, can impact relationship for an impressive time span.

B. Insufficient Identiy, Credential and Access Management

Cyberattacks and information breach regularly happen because of absence of identity access administration frameworks, inability to utilize multifactor confirmation, frail secret word use, and an absence of progressing automatic turn of cryptographic solutions, passwords and verifications.

C. Insecure Interface and APIs

Application Programming Interfaces (APIs) and software User Interfaces (SUIs) are the foundation of cloud computing associations and coordination among customers and distributed processing. SUIs and must be secured to ensure against both coincidental and noxious endeavors because virtual APIs' IP locations reveal the relationship among customers and the virtual world. Therefore fortifying APIs from irruption or humanoid error is essential to CC security.

D. System Vulnerabilities

Framework vulnerabilities are "exploitable bugs in programs that assailants can use to penetrate a PC framework to steal information, taking control of the framework or upsetting administration tasks." With distributed computing, frameworks from diverse associations are close to each other, and they are offered admittance to collective memory and possessions, making another assault surface.

E. Account Hijacking

If an intruder gains contact to authorizations, they can pry on undertakings and trades, manipulate information, return forged data and divert the customers to ill-conceived sites. Record or administration cases may turn into another base for aggressors. Then attacker can leverage the control of your reputation to dispatch consequent attacks. With stolen certifications, aggressors can frequently access distributed processing administrations, enabling them to trade off the privacy, uprightness and convenience of those executives. Aggressors can use account access to take information, affect cloud administrations and frameworks, harm the notoriety of occupants and that's only the tip of the iceberg, the report states [6].

F. Malicious Insider

CSA says, " A malevolent insider threat to an association, is characterized as a present or previous worker, contractual worker, or different business accomplice who has or had approved access to an association's system, framework, or information and purposefully surpassed or abused that access in a way that negatively influenced the confidentiality, trustworthiness, or accessibility of the association's data or data frameworks [11]."

G. The Advanced Persistent Threarts

Software engineers design these long haul digital (cyber) assaults to give them constant access into a framework. They focus on consolidate phishing, introducing attack codes by methods for USB contraptions, and intrusion by methods of unreliable framework. Once in, the intrusion appears as standard framework development and the aggressors are permitted to act. Careful customers and strong get to controls are the lines of best defend against this sort of attack.

H. Information Loss

Any data obliteration or misfortune can be a perpetual mischief to the business. Cloud data is obligated to an indistinguishable risks from is on premise data: inadvertent cancelation by customers or on the other hand staff of suppliers, common misfortune or harm, or mental activist ambush. It is the cloud supplier’s commitment to make arrangements for human slip-up and to manufacture solid physical server ranches [6].

I. Insufficient Due Dillgence

CSA states that when officials make business techniques, cloud advancements and specialist organizations must be considered. Building up a decent guide and agenda for due perseverance while assessing innovations and suppliers is essential to achieve the success. Associations that hurry to embrace cloud innovations and pick suppliers without performing due constancy open themselves to various dangers [11].

J. Abuse and Nefarious Use of Cloud Services

CSA says that ineffectively secured cloud benefit organizations, free cloud benefit trials, and false record recruits financial fraud uncover distributed computing models to vindictive assaults. Terrible performers may use distributed computing assets to target clients, associations, or other cloud suppliers. Cases of abuse of cloud-based assets incorporate propelling DoS assaults, email spam, and phishing efforts [11].

K. DoS

DoS assaults are intended to keep clients of an administration from having the capacity to get to their information or applications. By compelling the cloud administration to devour over the top measures of limited framework assets, for example, processor control, memory, circle space, or system transmission capacity, aggressors can cause a framework log jam and leave all legitimate administration clients without access to administrations [6].

L. Shared Technology Vulnerabilities

Cloud specialist organizations provide their administrations by IaaS, PaaS or SaaS. Cloud innovation separates the "as-a-benefit" offering without considerably changing the off-the-rack equipment/programming—in at cost of security. Basic parts that include the IaaS supporting cloud administrations arrangement might not have been intended to offer solid disconnection properties for a multi-occupant design or multi-client applications. This can prompt shared innovation vulnerabilities that can possibly be misused in all conveyance models [11].

III. CLOUD COMPUTING SECURITY SOLUTION

Cryptography is usually applied to ensure the security in cloud computing. There are many security issues which need to solve. In order to make cloud more secure, some researchers has used the encryption method to ensure the data security. In public cloud, the government can seize the information if a user shares computing resources with other corporations. To evade this and guard the stored data in public cloud data encryption is done [12]. Gartner mentions the importance of encryption in the article [13][14] and also states that unauthorized access can be avoided by applying encryption on data. In an article [14] author proposes a user-level encryption method to solve the Compliance. RSA and digital signature deliver the security before outsourcing the sensitive data into cloud storages [15]. Symmetric and asymmetric cryptographic approaches prevent data lose and protects data integrity while broadcasting [16][17]. Encryption using HMAC-SHA1 is being used to have complete control over the information to access [12]. Calculate Hash value is an answer for backup associated issues. It checks the keywords in the file before uploading and during the transmission and splits the file into equal size randomly and stores it in the locality [18].

In an article [19] author discusses the SaaS Protection by using homomorphic token. This approach very efficient over byzantine failures and server colluding attacks, data modification. In an article [20] author introduces RSA Based Storage Security (RSASS) to address remote data security, which is based on RSA for storing files in remote servers. This method can also compute large files with different sizes. The author proposes RSA Based Assumption Data Integrity Check [21] to deliver security over hash, 3rd party auditing mechanism. This new method combines both identity-based cryptography and RSA signature. In an article [22] author introduced Efficient Remote Data Possession Checking (RDPC) to have the communication and computation, verification without the need to be compared with the original data and mentions that user needs to store only two secret keys and several random numbers. In an article [23] author combines HLAs and RSA to Remote Data Position with Public Verifiability and this approach delivers the security verification. In an article [24], R. Mazumder et al. discuss the small domain encryption for the small size of information to perform on the IoT devices by using the AES encryption technique. The author proposes AES with Diffie-Hellman Exchange to improve the cloud data security in article [25].

J. Raigoza and K. Jitutri compared the AES and Blowfish algorithms for ASCII values to deliver the better data security [26]. In article [27], author implements the AES encryption algorithm in cloud computing environment to improve the data security and gives a conclusion that AES delivers more security in comparison of DES. W. Weng et al. have implemented and discussed AES based on FPGA to improve the information transfer [28]. Authors discuss the secure framework by using the AES on client side [29] to minimize the cost, memory and time duration and also discuss that information integrity can also be achieved by AES and RSA [30][31]. In an article [32] author discusses the solution for the data segregation that there should be a physical level and application level boundary for an individual consumer's data and also discusses the AWS process to ensure the security of the unauthorized users by using the SSL encryption while transfer.

Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML), and Web services standards are also the feasible solution for organizational security issues. To maintain the identity and access management system in an organization, the author mentions SPML, SAML [33], open id standard [33], OAuth, and XACML to have a secure communication between individuals in diverse cloud computing applications. In an article [14][34] authors discuss the multiple stacks to have the availability of stacks because if one stack fails then there will another one as a supporting substitute. Trusted Third Party (TTP) is one more solution for the organizational availability [13] and it also ensures the policy and trust management within the cloud environment to increase the confidentiality, communication and integrity [35]. The author discusses the privacy-preserving protocols and attribute-based policies [36] for the verification of identity and authentication management.

Data Fragmentation [17] is one more method to prevent intrusion into consumer's privacy. To improve the data security model, the author introduces [37] a hybrid model having three layers: 1st layer OTP authentication, 2nd for encryption, integrity & consumer protection and 3rd to speedy data recovery. In an article [38], the author discusses the fine-grained access control to secure the data in the cloud. In an article [39] author discusses the SSL/TLS, IPsec to have the secure communication in a cloud network.

Attribute-Based Encryption (ABE) [34] is a secure solution to distinct the access device panel and give a consent to consumers to access all information from a solitary site. In an article [40] author discusses the ubiquity and integration of services (UBIS) architecture to fulfil the needs of cloud consumers and to improve the cloud security. The author mentions the secure on-premise implementation in the article [38]. To identity the real attacker of DDoS, the author designed cloud trace back (CTB) [41]. Homomorphic encryption is another data security solution of cloud computing with encoded information without knowing the keys belonging to dissimilar parties. Lauter et al. [42], introduces a model for genomic information processing using homomorphic encryption. A distributed cryptography system proposes a Blockchain concept that is used in Bitcoin [43] to ensure secrecy.

IV. PROPOSED SECURITY APPROACH FOR CLOUD DATA SECURITY

Security will always be the foremost concern in cloud computing. Therefore, to achieve the information security, a framework has been proposed by combining the probabilistic double asymmetric encryption (RSA) with hashing technique. To deliver the security RSA [30] encryption and MD5 hashing technique [31] has been used. In RSA, public key is used for encryption and a secret key is to decrypt the information. Public Key Generation Algorithm Procedure:

“Algorithm 1: Public key generation

Output: a public key (n, e) and a private key d.

1. Generate randomly two large prime numbers p and q, which are kept secret.

2. Compute the modulus $n = p \cdot q$ and Euler’s totient function $\varphi = (p - 1)\,(q - 1)$.

3. Select a random integer e, $1 < e < \varphi$, coprime with φ.

4. Compute the multiplicative inverse of e with respect to modulus φ $(d \cdot e \equiv 1\ (mod\ \varphi))$”

“Algorithm 2: RSA encryption-decryption procedure

Bob encrypts a message m and sends it to Alice; Alice decrypts the message

1. Encryption

a. Bob should obtain the public key (n, e) of Alice.

b. Bob represents the message m as an integer between 0 and $n - 1$.

c. Bob computes $c = m^e\ mod\ n$.

d. Bob sends the cypher text to Alice.

2. Decryption

a. Alice should use its private key d to recover the message m form the cypher text

$m = c^d\ mod\ n$.”

The proposed model is based on the probabilistic asymmetric cryptography using the random key generation. Here four prime numbers have been used to deliver the factorization complexity which increases the security. All the generated keys are hashed by using the MD5 and stored in the server as shown in the Figure 1 (encryption procedure) and Figure 2 (decryption procedure).

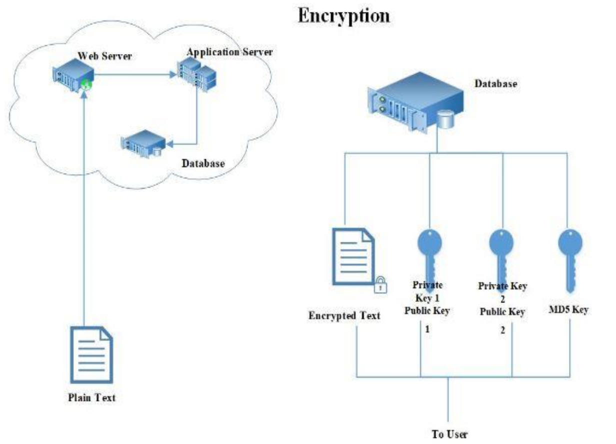

Figure 1. Encryption Procedure of Proposed Scheme

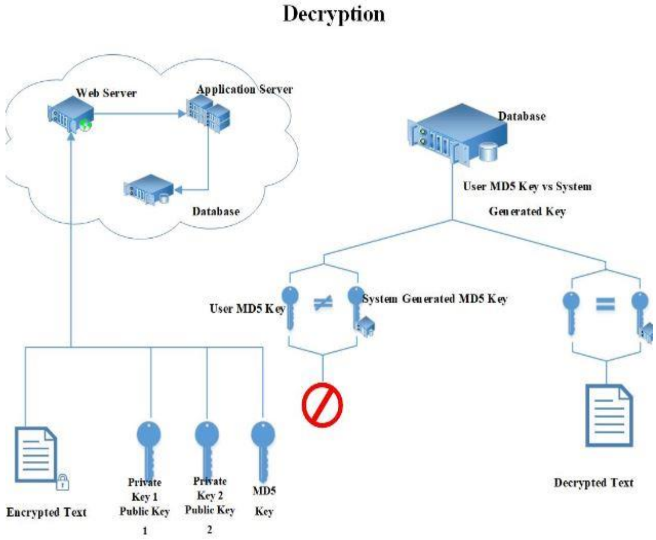

Figure 2. Decryption Procedure of Proposed Scheme

Performance Analysis

The proposed scheme has been tested on Ubuntu LTS 16.04 for the file sizes of 100 bytes, 150 bytes, 200 bytes and 250 bytes and RSA key variants (128-bit key to 1024-bit key) has been used for the implementation to check the performance. Figure 3 shows the encryption time analysis of the proposed scheme whereas Figure 4 represents the decryption time analysis.

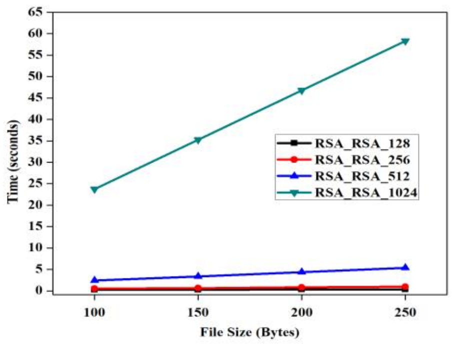

Figure 3. Encryption Time Analysis of Proposed Scheme for RSA key bit size (128-bit to 1024-bit)

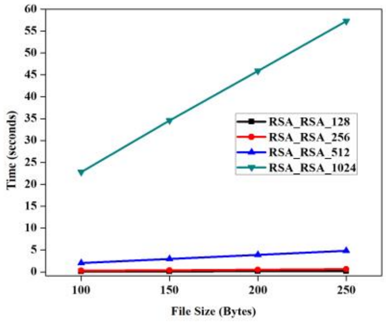

Figure 4. Decryption Analysis of the Proposed Scheme for RSA key bit size (128-bit to 1024-bit)

From the graphical analysis, it can be concluded as the file size increase time also increase. The proposed scheme is secure as it is using double RSA with hashing technique and all the random generated keys are random and stored at server. RSA key variants indicate the complexity of the algorithm. The proposed scheme delivers the client access confidentiality, key accountability and information confidentiality.

V. CONCLUSION

Cloud computing is an appealing and developing innovation for business world which deliver the software and hardware over web on request. Cloud computing delivers the numerous favorable benefits but there are challenges and security issues with respect to information transfer and information stockpiling over the web. As clients don't know where their information has stored and how much it is secured. In the proposed scheme delivers the user verification, approval and secure information storage.

ACKNOWLEDGMENT

I acknowledge Mr. Sayyam Jain and Khushbu for their help and support.

REFERENCES

[1] Georgios Skourletopoulos et al., "Big Data and Cloud Computing: A Survey of the State-of-the-Art and Research Challenges," *Advances in Mobile Cloud Computing and Big Data in the 5G Era (Springer).*2017. DOI 10.1007/978-3-319-45145-9_2.

[2] G. Ramachandra, M. Iftkhar and F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing," *3rd International Workshop on CyberSecurity and Digital Investigation, Procedia Computer Science*, vol. 110, pp. 465-472, 2017.

[3] K. Xie *et al.*, "Distributed Multi-dimensional Pricing for Efficient Application Offloading in Mobile Cloud Computing," *IEEE Transactions on Sevices Computing.* vol. 1374, no. 1, 2016.

[4] M. Ma, D. He, N. Kumar, K. R. Choo, and J. Chen, "Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics.* vol. 14, no. 2, pp. 1–9, 2018. ISSN: 1551-3203.

[5] M. Ali, S.U. Khan, A.V. Vasilakos, "Security in Cloud Computing: Opportunities and Challenges," *Information Sciences*, vol. 305, pp. 357-383, 2015

[6] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," *Future Generation of Computer Systems*, vol. 25, pp. 599-616, 2009.

[7] Shazia Tabassam, "Security and Privacy Issues in Cloud Computing Environment," *Journal of Information Technology and Software Engineering*, vol. 7, no. 5, pp. 1-6, 2017.

[8] Limor Wainstein, "6 big data and cloud security concerns to watch in 2018," in Privacy/Security, 2018. [Accessed May 12, 2018]

http://bigdata-madesimple.com/6-big-data-and-cloud-security-concerns-to-watch-in-2018/

[9] IANS, "Human error responsible for most data breach on Cloud: IBM," April 5, 2018.

https://economictimes.indiatimes.com/tech/internet/human-error-responsible-for-most-data-breaches-on-cloud-ibm/articleshow/63625807.cms [Accessed May 12, 2018]

[10] Thales Report, "2018 Thales Data Threat Report: 94% of organizations using cloud, IoT and other transformative technologies, data breaches at all-time high," January 25, 2018.

https://www.prnewswire.com/news-releases/2018-thales-data-threat-report-94-of-organizations-using-cloud-iot-and-other-transformative-technologies-data-breaches-at-all-time-high-300587802.html [Accessed May 12, 2018]

[11] Steve Haase, "12 biggest cloud security threats in 2018," InsecureTrust, April 3, 2018.

https://www.insuretrust.com/the-12-biggest-cloud-security-threats-in-2018/ [Accessed May 12, 2018]

[12] L. Ertaul, S. Singhal, and G. Saldamli, "Security Challenges in Cloud Computing," California State University, East Bay. Academic paper, 2009.

http://www.mcs. csueastbay. edu/ lertaul/Cloudpdf, 2009.

[13] T. Bhatia and A.K. Verma, "Data Security in Mobile Cloud Computing Paradigm: A Survey, Taxonomy and Open Issues," *The Journal of Supercomputing (ACM digital library)*, vol. 73, no. 6, pp. 2558-2631, June 2017.

[14] Michael Armbrust, Armando Fox, Rean Gri_th, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, "A View of Cloud Computing," *Communications of the ACM*, vol. 53 pp. 50- 58, April 2010. ACM ID: 1721672.

[15] Ainul Che Fauzi, A. Noraziah, Tutut Herawan, and Noriyani Mohd. Zin, "On Cloud Computing Security Issues," *Intelligent Information and Database Systems*, pp. 560-569, 2012.

[16] Xiaoqi Ma, "Security Concerns in Cloud Computing," *Fourth International Conference on Computational and Information Sciences (ICCIS)*, pp.1069-1072, 2012.

[17] Iliana Iankoulova and Maya Daneva, "Cloud Computing Security Requirements: A Systematic Review," *Sixth International Conference on Research Challenges in Information Science (RCIS)*, pp.1-7, 2012

[18] Rongzhi Wang, "Research on Data Security Technology based on Cloud Storage," *13th Global Congress on Manufacturing and Management, GCMM, 2016,* Procedia Engineering 174 (2017) 1340 – 1355, 2016

[19] K. K. Chauhan, Amit K. S. Sanger and A. Verma, "Homomorphic Encryption for Data Security in Cloud Computing," *International Conference on Information Technology*, pp. 206-209, 2015. DOI 10.1109/ICIT.2015.39.

[20] M. Venkatesh, M. R. Sumalatha, and C. SelvaKumar, "Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing," *International Conference on Recent Trends In Information Technology (ICRTIT)*, pages 463-467, 2012

[21] Zhang Jianhong and Chen Hua, "Security Storage in the Cloud Computing: A RSA-Based Assumption Data Integrity Check Without Original Data," *International Conference on Educational and Information Technology (ICEIT)*, vol. 2, pp. V2-143, 2010

[22] Lanxiang Chen and Gongde Guo, "An Efficient Remote Data Possession Checking in Cloud Storage," *International Journal of Digital Content Technology and its Applications*, vol. 5, no. 4, pp.43-50, 2011

[23] Wenjun Luo and Guojing Bai, "Ensuring the Data Integrity in Cloud Data Storage*," IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS)*, pp. 240-243, 2011

[24] R. Mazumder, A. Miyaji and C. Su, "A Simple construction of encryption for a Tiny Domain Message," *51st Annual Conference on Information Science and Systems (CISS), IEEE,* Baltimore, MD, USA, March 22-24, 2017

[25] P. Rewagad and Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," *International Conference on Communication Systems and Network Technologies*, pp. 437-439, 2013

[26] Jaime Raigoza and K. Jituri, "Evaluating Performance of Symmetric Encryption Algorithms," *International Conference on Computational Science and Computational Intelligence, IEEE*, pp. 1378-1381, 2016

[27] S. Rajput, J. S. Dhobi and L. J. Gadhavi, "Enhancing Data Security using AES Encryption in Cloud Computing," *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems,* vol. 2, *Smart Innovation, Systems and Technologies,* vol 51. 2016.

[28] Wei Wang, Jie Chen and Fei Xu, "An Implementation of AES algorithm Based on FPGA," *9th IEEE International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2012.

[29] N. Surv, B. Wanve, R. Kamble, S. Patil and J. Katti, "Framework for Client side AES Encryption Technique in Cloud Computing," *IEEE International Advanced Computing Conference (IACC)*, Bangalore, India, June 12-13, 2015

[30] B. Thiyagarajan and R. Kamalakannan, "Data Integrity and Security in Cloud Environment using AES Algorithm," *IEEE International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, India, February 2014

[31] N. Shimbre and P. Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm," *IEEE International Conference on Computing Communication Control and Automation (ICCUBA),* Pune India, February 26-27, 2015.

[32] S. Subashini and V. Kavitha, "A Survey On Security Issues In Service Delivery Models Of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp.1-11, January 2011

[33] W. Jansen and T. Grance. "Guidelines on Security and Privacy in Public Cloud Computing. NIST Draft Special Publication," *U.S. Department of Commerce,* Special Publication 800-144, 2011

[34] Syed A. Hussain, Mehwish Fatima, Atif Saeed, Imran Raza and Raja K. Shahzad, "Multilevel Classification of Security Concerns in Cloud Computing," *Applied Computing and Informatics*, vol. 13, no. 1, pp. 57-65, 2017

[35] Dimitrios Zissis and Dimitrios Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems*, (0), 2010

[36] H. Takabi, J.B.D. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *Security & Privacy, IEEE*, vol. 8, no. 6, pp.24-31, 2010

[37] Zhang Xin, Lai Song-qing, and Liu Nai-wen, "Research on Cloud Computing Data Security Model based on Multi-dimension," *International Symposium on Information Technology in Medicine and Education (ITME)*, vol. 2, pp.897-900, 2012

[38] Feng Liu, Weiping Guo, Zhi Qiang Zhao, and Wu Chou, "SaaS Integration for Software Cloud," *3rd IEEE International Conference on Cloud Computing (CLOUD)*, pp.402-409, 2010

[39] Jianyong Chen, Yang Wang, and Xiaomin Wang, "On-demand Security Architecture for Cloud Computing," *Computer*, vol. 45, no. 7, pp.73-78, 2012

[40] A. Hammami, N. Simoni, and R. Salman, "Ubiquity and QoS for Cloud Security," *41st International Conference on Parallel Processing Workshops (ICPPW)*, pp. 277-278, September 2012

[41] Bansidhar Joshi, A. Santhana Vijayan, and Bineet Kumar Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," *International Conference on Computer Communication and Informatics (ICCCI)*, pp.1-5, 2012.

[42] K. Lauter, A. Lopez-Alt, and M. Naehrig, "Private Computation on Encrypted Genomic Data," Tech. Report. MSR-TR-2014-93, June 2014.

[43] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." pp.1-9, March 2009. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986

AUTHOR'S BIOGRAPHY

Vartika Kulshrestha received her MS in Wireless Sensors & Embedded System from the University of Bradford, the United Kingdom in 2009. She is currently a PhD student in Banasthali Vidyapith. She is a life member of Indian Science Congress. Her research interest includes cloud computing, IoT, Big Data, WSN, Network Security, Cyber Security.

Seema Verma received her MSc in Electronics from Banasthali Vidyapith in 1993, PhD in Electronics from Banasthali Vidyapith in 2003. She is currently a Professor in Electronics and Dean of Aviation. She is a Fellow of IETE, life member of Indian Science Congress and International Association of Engineers (IAENG). She has authored two books and more than 100 research papers. She has many projects from UGC and AICTE to her credit. Her research interest includes coding theory, TURBO codes, WSN, Aircraft networks, Network Security & VLSI Design.

Rama Krishna Challa received his M.Tech from CACUT, Cochin in 1995, PhD in Computer Science Engineering from IIT Kharagpur in 2009. He is currently a Professor and Head of Computer Science Engineering Department in NITTTR Chandigarh. He has authored more than 100 research papers. His research interest includes Wireless Communication & Networks, Computer Networks, Distributed Computing, Cryptography & Cyber Security.