Review of Computer Engineering Research
2020 Vol. 7, No. 1, pp. 12-19
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/journal.76.2020.71.12.19
© 2020 Conscientia Beam. All Rights Reserved.

CLOUD SECURITY VULNERABILITIES AND SOLUTION MODEL

Shouket Ahmad Kouchay

Faculty, King Saud University, KSA.
Email: mail2shawkat@gmail.com

Article History
Received: 28 October 2019
Revised: 3 December 2019
Accepted: 6 January 2020
Published: 13 February 2020

Keywords
Cloud security vulnerabilities
Advanced encryption standard
IAAS
SAAS
PAAS
Cloud computing security technique.

ABSTRACT

Cloud computing is the revolution and solution to the computing world which has paid further attention as an emerging network storage technology. Cloud computing has enormous adaptability in terms of demand or availability of resources. The organization prefers cloud storage services to reduce the overhead of storing data locally. Yet, Data security and privacy are the major issues in cloud computing. Although security is still one of the critical challenges in the world of cloud computing. The security concerns comprise the loss of vital information and privacy loss of any individual who uses cloud networking. This research reviews the cloud Security, its vulnerabilities and proposes a three-layer model of AES encryption for Cloud Computing Security and RSA is used to hide the key of the AES. According to our research, this model is one of the most compact encryption which consumes less storage space with short calculation time. A detailed review of cloud security concerns and resolutions has been discussed in this paper.

Contribution/Originality: This research reviews the cloud Security, its vulnerabilities and proposes a three-layer model of AES encryption for Cloud Computing Security and RSA is used to hide the key of the AES.

1. INTRODUCTION

The internet data usage has not only affected browse the web portals but also to the development of Internet application services resulting in huge volume of internet data. The various cloud related groups and teams are working for better cloud services such as cloud-related vulnerability research group focused in the areas of network, storage and their thorough reasons[1]. Cloud computing has developed as one of the fast rising sectors of the Computer world. It improves the computational capabilities dynamically without investing in new infrastructure, training new employee, or licensing new software's as required [2]. While studying the subject of cloud computing, the researchers describe that cloud has massive potential to handle any IT related activity and deliver it to the right user within time as a service [3, 4]. Cloud technology is often considered as one of the most important discovery in order to handle technological tasks successfully by organizations [5]. The scope for Cloud computing and Internet of Things is great in near future. Security is the important for protecting all web resources and user information [6]. A survey was undertaken on security problems that arise when using cloud network, it turned out that almost 12% of the software industry moved towards cloud networking in the year 2011 to 2016 [7]. The growth turnover will reach about 95 billion USD. Generally, 3 services are delivered by cloud network; these services are based on the 3 layer infrastructure concept such as; SAAS (Software as a Service), IAAS (Infrastructure as a Service) and PAAS (Platform as a Service) [8, 9] as shown in Figure 1.

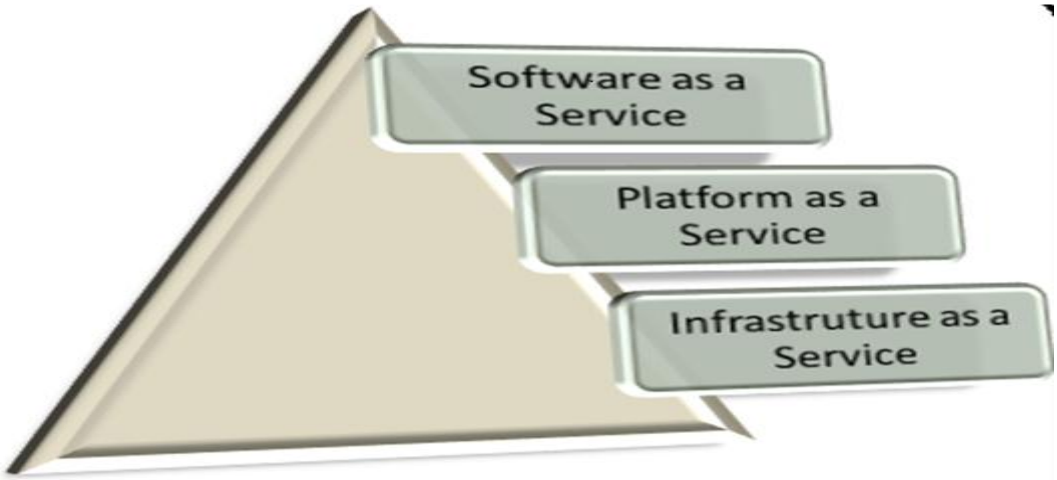

Figure-1. 3 Layer infrastructure SAAS, IAAS, PAAS.

The role of these cloud services is eminently very high. Software as a Service (SAAS) is mainly intended to be delivered to the end user via internet. Whereas, Platform as a Service (PAAS) consists set of tools and services that are intended towards coding in order to position the applications faster and accurately. Infrastructure as a Service (IAAS) is basically that controls all, whether it's networks, OS, servers etc [10, 11].

Security and privacy are one of the main concerns of a cloud computing, as it includes sensitive information [12, 13]. Cloud computing is a modern way of using web enabled devices, although it is still a unique way of networking which is both convenient as well as efficient, criticizers believe that it not sufficiently safe as the data is transferred outside the local area networks.

The International Telecommunication Union augmented the concept of IoT and suggested four technologies to realize IoT; RFID technology, intelligent embedded technology, nanotechnology, and sensor technology [14]. Cloud computing and Internet of Things (IoT) security is more important in Future Internet for their implementation, integration and usage. A Model with three security layers has been discussed in this paper along with sections as in Figure 2:

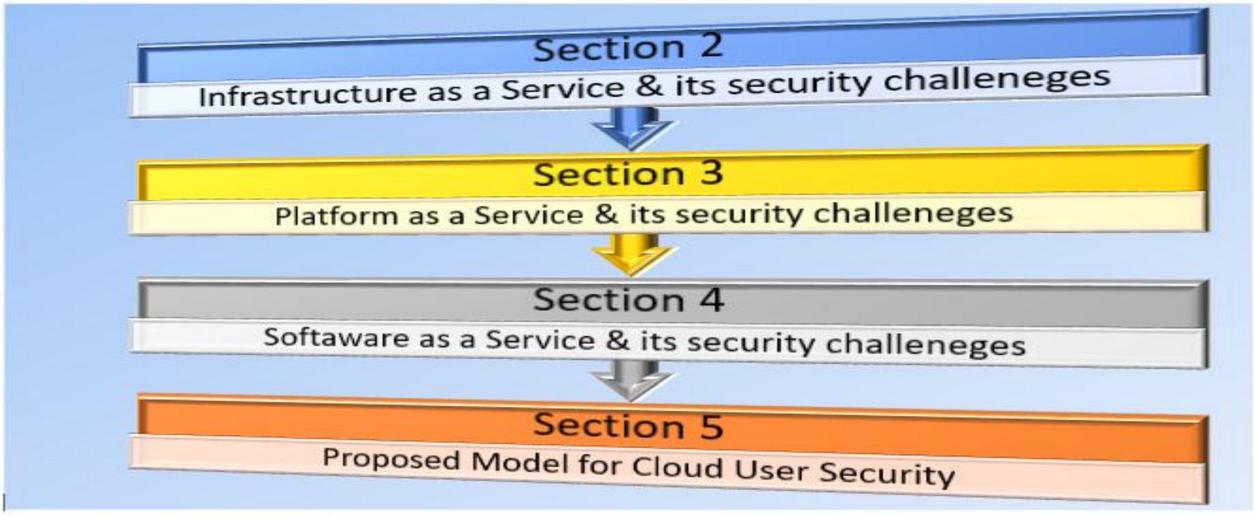
Section 2
Infrastructure as a Service & its security challeneges
Section 3
Platform as a Service & its security challeneges
Section 4
Softaware as a Service & its security challeneges
Section 5
Proposed Model for Cloud User Security

Figure-2. A model with three security layers.

2. IAAS (INFRASTRUCTURE AS A SERVICE)

IAAS refers to Infrastructure as a Service is a computer based infrastructure which is controlled via internet. Infrastructure as a Service reduces the difficulty and expenditure of purchasing and maintaining individual physical servers. IAAS applications face challenges in CSP (Cloud Service Provider), Servers, Components of Networking, etc. Cloud Service Provider or CSP is mainly responsible for handling, maintaining and running the equipment. When using IAAS applications the user only has to pay on per use basis.

Some of the characteristics and workings of Infrastructure as a Service are given below [15]:

- Dynamic Scaling.
- Automation of administrative tasks.
- SLA (Service Level Agreement).
- Utility computing service and billing model.
- Internet connective.
- Desktop virtualization.

Following are some of the threats that affect IAAS application delivery model:

Security Issues Traced from Host:

a) Monitoring VMs from Host

The host machine in virtual environment faces inferences that let the host to screen and connect with running VM applications. This makes it important to secure host machines instead of providing safety to individual VMs [16]. VM-level protection plays a vital role in cloud network; applications can be co-located by utilizing diverse trust levels keeping it on the similar host and making possible to secure VMs in a multi-tenant shared environment. This allows enterprises to obtain maximum benefits of virtualization. Today's active data centers rely on secure VMs which stays safe with VM-level protection. The protection also safeguards the transmission of VMs from virtual servers to private cloud network, from private to public cloud network and as well as between cloud service vendors [17].

b) Communications between VMs & Host

Respective data is transferred between the host and VMs which is shared with computer generated resources, which makes the host capable of monitoring the network of the hosted VMs. It is valuable to consider that attackers use certain features such as shared clipboard which allows the data to be transferred between VMs and the host by applying cooperating malicious program in VMs [18]. Generally, it isn't measured as a bug or any limitation when initiating any change in monitoring or communication with a VM application from the host. Hence, the host environment should be more secured than the individual VMs. The host can impact the VMs in number of ways [19]. Such as:

- The host can start shutdown, pause and restart VMs.
- Monitoring and alignment of resources which are accessible on the VMs, like CPU, storage, network usage of VMs, etc.
- Adjust the amount of CPUs, storage, virtual disks and distinctive virtual network interfaces which are accessible to VM.
- Observing the applications which are running inside VM.
- View, copy and make adjustments if possible to the data stored in the VM's virtual disks.

Unfortunately, there is loop hole which allows the system admin or any lawful user to misuse it Takabi, et al. [18].

2.1. Security Threats Sourced from Other VMs

Observing VMs from other VMs can create security violation and also raise threats to privacy, but the use of any and improved architecture of CPUs which are assimilated with data protection feature that is capable of providing high level protection and also avoid privacy breach. One of the primary reasons for implementing virtualization is to separate security tools from untrusted VMs by shifting them to secure VMs [15, 17].

Communication between VMs is one of the utmost problematic threats, that create issues in the exchange of information among virtual machines and the way it is positioned. Sharing resources between VMs could result in reducing the security levels of each VM, like utilization of applications on the basis of shared clipboard could lead to the exchange of data between VMs and host assisting malicious program in VMs, this condition is capable of violating both privacy and security. Malicious VMs are also capable of approaching other VMs via shared memory [17].

c) DOS (Denial of Service)

The DOS makes resources unavailable for the user to reach a website. For example; sometimes when we try to access a particular website and due to over crowd or over traffic on server, it is not possible to access the website. This situation usually occurs when the requests to access the website surpasses the ability of the server to handle the requests. [19].

Utilization of IDS (Intrusion Detection System) is one of the most beneficial techniques of defense against such attacks [18]. Real-world solutions and methods in order to prevent such attacks or at least reduce their impacts are given below:

- Logical network segmentation.
- Firewalls implementing.
- Traffic encryption.
- Network monitoring.

3. PLATFORM AS A SERVICE (PAAS) – SECURITY CHALLENGES

The key benefit that PAAS offers is the ability to manage applications without the need of installing any form of platform or tools. PAAS also provides a way to rent hardware over the internet. PAAS offers ability to manage application without the need of installing any significant platform or tools on the systems. PAAS provides platform layer resources which support operating system and software development frameworks in which it can be used to build more improved services [10]. Some of the advantages that developer can be benefitted from PAAS are:

- OS can be altered or improved as many times as needed.
- PAAS permits geographically distributed teams to share information in order to develop software based projects [15].

The use of cybernetic machines is basically to support PAAS layer in cloud computing. It is important to protect virtual machines from malicious attacks like cloud malware. Therefore, maintaining the safety and ability of applications during the transfer of data across the whole networking channel is fundamental [20]. Some of the threats of PAAS security can be summarized as:

3.1. Data Location

The core platform doesn't exist in one single host; the platform could be believed as bunch of hosts. The location of data cannot be determined to a particular specific sector over specific host, this allows more security as it is easier to handle host in a single location instead of many. Another security problem is the replication of data which creates high availability of data for users and developers, but this replicated data remains same as the main data but what diversify it from the original data is that it's location stays unknown [9].

3.2. Privileged Access

PAAS consists of many useful features; one of the utmost popular features is the utilization of debug by the advertised software developers. Debug allows developers to access to data and storage locations to modify values in order to test distinguished outcomes; it is primary tool for both developers and hackers [16].

3.3. Distributed Systems

The PAAS file system is one of the highly distributed systems. The nodes stay independent while CSP (Cloud Service Provider) handles the cluster with a standard configuration to ensure nodes stay in place. Although the client/user is responsible for their own safety, but CSP ought to be able to deliver necessary level of security [20]. Some of the real world solutions to prevent/reduce such attacks are given below:

- Condensing access control policies with objects could lead to resolve Privileged access.
- PEP (Policy Enforcement Points) is a logical entity which is present on a server that allows access control as well as it helps in managing user's request to access resources on a compute or/and network server [16].
- TCB (Trusted Computing Base is a collection of executable codes and files that can be configured to provide maximum security. TCB allows installing a layer over the OS which provides API (Application Programming Interface) for the user applications; encryption is the best possible solution [9].

4. (SAAS) SOFTWARE AS A SERVICE

Software as a Service is a method which is used in order to deliver services in the form of applications via internet. With SAAS the user doesn't need to download or install any type of software in the system as it can be easily accessed via internet without the need of any additional hardware and software management. Web-based or On-demand software are another term to describe SAAS applications. These applications are run a server hosted by SAAS provider. They control security and availability to maximize performance. SAAS was set up mainly for CRM (Customer Relationship Management) and Sales Force Automation but now it is usually used for tasks such as computerized billing, human resource management, data management, etc. [15].

Web browsers are used in order to access SAAS applications, which make it necessary to secure web browsers. Some of the available options that are applied to protect data are WS (Web Services), XML (Extended Markup Language), and SSL (Secure Socket Layer) [21]. To keep track that proper security measures are applied to proper each and every user's privacy from other users, a verification technique is used to keep high privacy level. It does get out of hand sometimes which makes it very difficult for service providers to maintain appropriate security level [22].

Software as a Service (SAAS) security threats can be summarized as:

- Verification and approval loop holes.
- Lack of Data confidentiality.
- Obtainability issues.
- Breach in Information security.
- Data admittance.
- Identity verification management.

Some practical solutions have been recommended by Navneet Singh to handle common security threats when utilizing SAAS applications [19]. Such as:

- What metrics can be used for reporting?
- What is the level of access controls?
- Is the provided data can be easily adapted in the internal monitoring tools?
- How important and critical the enterprise data is?

5. PROPOSED MODEL

The AES algorithm with the combination of RSA has been proposed in this paper to ensure high level cloud security. For data upload on cloud mandatory keys are AES secret key and RSA public key. Private key of RSA and AES secret key are essential to download data from cloud. Whenever anyone makes an effort to upload data on cloud first that file stored onto directory for short time. In encryption process first AES algorithm is applied on file after that RSA algorithm is applied on encrypted data. Reverse process is followed for decryption. All the three layers are designed considering AES algorithm. AES or Advanced Encryption Standard is a balanced cipher which is in the form of blocks. AES practices blocks of data which are 128 bits in size. Its key length is 128, 192, or 256 bits. The data is formulated in a four row manner by the use of Advanced Encryption Standard. The first layer is there to verify identification details of each and every user. Whereas the second layer relies on data identification and encryption from where the data is moved to the third layer, which ensures data is properly secure and ready to be transferred by using cryptography technique. AES encryption action takes place in a ten round form of process. The AES encryption is going to be identical in the first two layers but not in the third layer for better security. The process of analyzing the user is going to begin right after first four words are entered as the key schedule consists of matrix order in a 4X4 manner, derived from 128 bit input block known as the state array. All three services i.e. IAAS, PAAS and SAAS are going to use this encryption technique. For instance, the input is going to be read by XORed then the data is going to move to the three layers for processing. In the first layer a nonlinear switch is going to replace each byte with another as per the given information, this step is known as SubBytes. In the next step which is called ShiftRows the data is transported to rows, where each and every row is removed regularly at periodic intervals. In the third and final layer, data is going to be operated in columns as per its requirement, which will be transmitted after getting merged with four bytes in every column then the merged data is going to be united with round key. Each and every round key obtained from the AES encryption key at periodic key intervals. This step is called as MixColumn and AddRoundKey. The RSA involves distribution of public and private key to sender and receiver to encrypt and decrypt the message respectively as it is hard to find the factors of large integers in it. The key generation, message encryption and message decryption are the three phases in RSA [23].

The architecture for the proposed model is shown in Figure 3:

Architecture of the Proposed Model

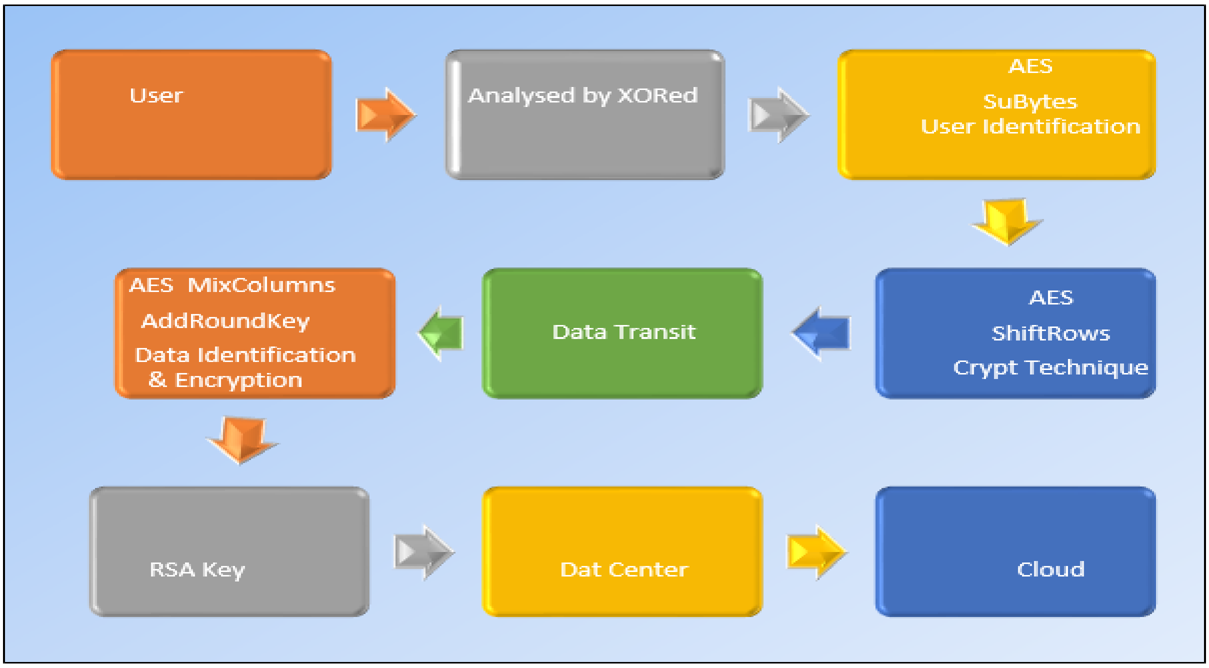

Figure-3. Architecture of the proposed model.

6. CONCLUSION

Cloud computing is capable of sharing large data in different forms. This makes it very unsafe. The security problems are common in the cloud computing network. The paper proposes solution to handle cloud security threats in order to ensure a highly safe and private user experience without any unwanted data breach in the cloud network. Authors have projected solutions for day to day challenges in cloud computing environment by using security layer models. The various cloud computing services and its security concerns has been reviewed. The main reflection of this paper revolves around intelligent way of utilizing a compact algorithm AES and RSA. The AES is one of the most compact encryption which consumes less storage space and its calculation time is short as well. Although every user has a different choice in choosing security method for cloud computing, but the prosed security model assures safe, flexible and privacy based cloud user experience. The various cloud computing services and its security concerns have been discussed.

Funding: This study received no specific financial support.
Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.

REFERENCES

[1] Cloud Vulnerabilities Working Group, "Cloud vulnerabilities research program." Retrieved: https://www.vulnerability-lab.com/. [Accessed Dec 2019], 2016.

[2] G. Calvary, *Computer science and ambient intelligence*, 1st ed. London: Iste, 2013.

[3] Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: Multi-keyword ranked search over encrypted cloud data supporting synonym query," *IEEE Transactions on Consumer Electronics*, vol. 60, pp. 164-172, 2014.Available at: https://doi.org/10.1109/tce.2014.6780939.

[4] S. O. Kuyoro, F. Ibikunle, and O. Awodele, "Cloud computing security issues and challenges," *International Journal of Computer Networks*, vol. 3, pp. 247-255, 2011.

[5] L. Allen, T. Heriyanto, and S. Ali, *Kali linux - assuring security by penetration testing*, 1st ed. Birmingham, UK: Packt Publication, 2014.

[6] A. K. Shouket, "Secured architecture strategy for fighting against bots," *Computer Science & Telecommunications*, vol. 40, pp. 16-23, 2013.

[7] B. M. Salih and H. A. Edreis, "Comparison between virtualization and cloud computing," *International Journal of Science and Research*, vol. 5, pp. 195-199, 2016.Available at: https://doi.org/10.21275/v5i6.nov164128.

[8] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200-222, 2016.

[9] K. Kumar and P. Kaur, "Road traffic control system in cloud computing: A review," *International Journal of Grid and Distributed Computing*, vol. 8, pp. 201-206, 2015.Available at: https://doi.org/10.14257/ijgdc.2015.8.3.20.

[10] T. Erl, R. Puttini, and Z. Mahmood, *Cloud computing: Concepts, technology & architecture*: Pearson Education, 2013.

[11] M. Loudini, S. Rezig, and Y. Salhi, "Incorporate intelligence into the differentiated services strategies of a Web server: An advanced feedback control approach," *Journal of Internet Services and Applications*, vol. 1, pp. 1-16, 2013.

[12] S. Rajasekhar, E. Murali, and G. Nagalakshm, "Efficient architecture cloud computing confidentiality," *International Journal of Research Studies in Computer Science and Engineering*, vol. 3, pp. 12-16, 2016.

[13] C. Esposito, A. Castiglione, B. Martini, and K. Choo, "Cloud manufacturing: Security, privacy, and forensic concerns," *IEEE Cloud Computing*, vol. 3, pp. 16-22, 2016.Available at: https://doi.org/10.1109/mcc.2016.79.

[14] N. Huansheng, *Unit and ubiquitous internet of things*: CRC Press, 2016.

[15] S. Pearson and G. Yee, *Privacy and security for cloud computing*, 1st ed. London: Springer, 2013.

[16] L. Zhang, "Software architecture evaluation," *Journal of Software*, vol. 19, pp. 1328-1339, 2008.Available at: https://doi.org/10.3724/sp.j.1001.2008.01328.

[17] R. Samani, B. Honan, J. Reavis, and V. Jirasek, *CSA guide to cloud computing*, 1st ed. Waltham, MA: Syngress, 2015.

[18] H. Takabi, J. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy Magazine*, vol. 8, pp. 24-31, 2010.Available at: https://doi.org/10.1109/msp.2010.186.

[19] S. Sherin, S., "Security and privacy issues of cloud computing; Solutions and secure framework," *IOSR Journal of Computer Engineering*, vol. 10, pp. 33-37, 2013.Available at: https://doi.org/10.9790/0661-01043337.

[20] A. Gouri, K. Karthik, G. Arpita, and G. Priya, "Review on security management in cloud computing," *International Journal of Engineering and Computer Science*, vol. 5, pp. 18897-18906, 2016.

[21] Z. Tari, "Security and privacy in cloud computing," *IEEE Cloud Computing*, vol. 1, pp. 54-57, 2014.

[22] M. ZekriyapanahGashti, "Scrutiny new framework in integrated distributed reliable systems," *International Journal of Distributed and Parallel Systems*, vol. 3, pp. 13-20, 2012.Available at: https://doi.org/10.5121/ijdps.2012.3502.

[23] R. Minni, K. Sultania, S. Mishra, and D. R. Vincent, "An algorithm to enhance security in RSA," presented at the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.

Views and opinions expressed in this article are the views and opinions of the author(s), Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.