Circumstantial Discussion on Security and Privacy Protection using Cloud Computing Technology

2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-6654-3789-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACITE53722.2022.9823875

Melanie Lourens[1]
[1]Department of Human Resources Management, Durban University of Technology, South Africa
Melaniel@dut.ac.za

Ayesha Naureen[2*]
2Assistant Professor, Department of Computer Science and Engineering, B V Raju Institute of Technology, Narsapur, Telangana 502313
nooriekhan005@gmail.com
0000-0002-0070-6762

Shouvik Kumar Guha
Assistant Professor (Law)
The West Bengal National University of Juridical Sciences
shouvikkumarguha@nujs.edu

Shahanawaj Ahamad
College of Computer Science and Engineering, University of Hail, Hail City Saudi Arabia
drshahwj@gmail.com

Dharamvir
Associate Professor
Dept of MCA , The Oxford College of Engineering, Bommanhalli, Bangalore, India - 560068
dhiruniit@gmail.com

Vikas Tripathi[6]
6Associate Professor, Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India, 248002
vikastripathi.cse@geu.ac.in
ORCID: 0000-0002-2254-3044

***Abstract*- Cloud computing is becoming a demanding technology due to its flexibility, sensibility and remote accessibility. Apart from these applications of cloud computing, privacy and security are two terms that pose a circumstantial discussion. Various authors have argued on this topic that cloud computing is more secure than other data sharing and storing methods. The conventional data storing system is a computer system or smartphone storage. The argument debate also states that cloud computing is vulnerable to enormous types of attacks which make it a more concerning technology. This current study has also tried to draw the circumstantial and controversial debate on the security and privacy system of cloud computing. Primary research has been conducted with 65 cloud computing experts to understand whether a cloud computing security technique is highly secure or not. An online survey has been conducted with them where they provided their opinions based on the security and privacy system of cloud computing.**

Findings showed that no particular technology is available which can provide maximum security. Although the respondents agreed that blockchain is a more secure cloud computing technology; however, the blockchain also has certain threats which need to be addressed. The study has found essential encryption systems that can be integrated to strengthen security; however, continuous improvement is required.

Keywords: cloud computing, encryption systems, blockchain, threats, security

I. INTRODUCTION

Cloud computing has witnessed a great visualisation in the field of business, healthcare and educational sectors. It has been found that this technology provides enormous amounts of resources to its end-users [1]. Moreover, the users stated that the cloud computing technology is remunerative in terms of *scalability, availability* and *manageability*. Apart from this, cloud computing also holds versatility in the field economy, stability, flexibility, convenience and quick service [2]. Cloud computing has three models of services that include the “Cloud privacy”, “Cloud services” and “Basic components” have been shown in figure 1. In the figure, **IaaS** determines the “*Infrastructure as a Service*”; and **PaaS** defines the “*Platform as a Service*”.

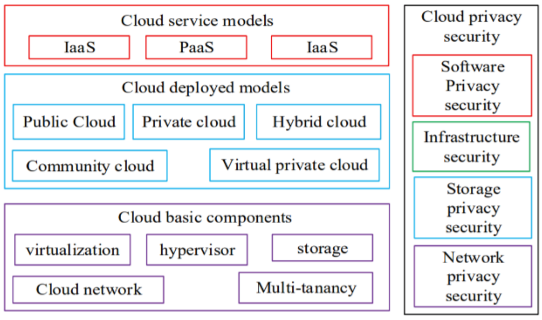

Fig. 1. Framework and models of Cloud computing

(Source: [2])

Security and privacy are two major considerations while cloud computing is being discussed. Studies suggest that the cloud services are unable to be controlled by the users effectively which result in privacy and security breach [3]. Privacy and security breaches mostly occur during the transmission and sharing of data. The “***man-in-the-middle***" is responsible for breaching the data being transferred to another end-user [4]. A thoughtful controversy is still present in the security and privacy system of cloud computing. Many journal articles have argued on this topic as well to make it clear that the cloud is more secure than smartphone storage [5]. Other studies showed that information becomes more vulnerable when transferred to a cloud environment [6]. The cloud is categorised into three types as shown in Fig. 1; the ***private cloud, public cloud*** and ***hybrid cloud***. Here, when the data is shared among the users via the public cloud, the data becomes more vulnerable as a user can attack the system anytime [7].

As the controversy goes on, researchers are trying to improve the security system by integrating various other technologies. One of the technologies is *"Blockchain*" technology which has been shown to address the security issues in the cloud environment [8,9]. Other strategic planning and encryption systems are also available which make the cloud system better [10].

This research is going to execute a circumstantial discussion on the Security and Privacy of Cloud computing technology. Primary research methods have been selected to gather practical knowledge and information on the selected topic. The paper is organised into a past literature study where common and advanced practices on cloud security have been explained. After that, the current research methodology has been discussed. The subsequent section analyses the primary data and the interpretation is discussed in the later section. Finally, the study concludes its major findings in the conclusion section.

II. Literature Review

Cloud computing has gained interest due to its remote access capability and huge storage system. However, as the data are accessible by more than one end-user, security and privacy became one of the concerning threats [11]. According to Kumar and Alphonse, conventional encryption systems such as "**symmetric**" and "**asymmetric**" are not highly promising to obtain *suitability*, *flexibility* and *access control* [12]. Thus, developers have introduced "**Cryptographic techniques**" to improve the access control and privacy system. This security technique is also known as "Attribute-based encryption" which works with a policy attribute, proxy encryption and "hidden policy". Another mechanism is known as the "revocation" mechanism which also shows promising advantages in the encryption of cloud data.

Yang and colleagues have introduced a "multi-authority" encryption system which is a decentralisation-based attribute. They stated that this attribute is beneficial in sharing highly confidential information among the end-users in cloud computing. This encryption system makes every user a different and unique identity and simultaneously, the location of the users are notified [13]. The author states that this attribute holds a permission system for the user who requires key access. During the key request, the current domain authority is alerted and it ultimately enhances the privacy and security system [14].

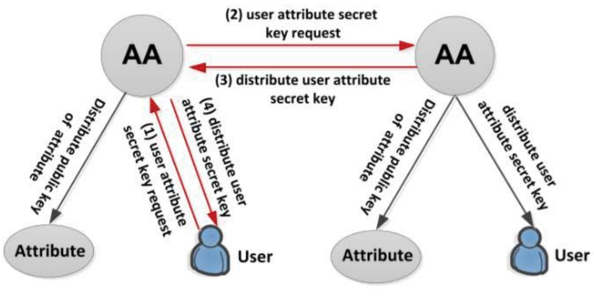
(2) user attribute secret key request
AA
AA
(3) distribute user attribute secret key
Distribute public key of attribute
(1) user attribute secret key request
(4) distribute user attribute secret key
Distribute public key of attribute
distribute user attribute secret key
Attribute
User
Attribute
User

Fig. 2. Process and scheme of "*Key distribution*"

(Source: [14])

The above figure 2 shows the attribute authority (AA); a scheme for the user when key access is requested; and secret key distribution process.

Several authors have explained the security issues and solutions in cloud computing. Basu and co-workers have also opined that privacy and security is the major concern in cloud computing and its solution is another topic of debate [15]. The authors have explained the common attacks that occur in cloud computing. These include the "Wrapping attack", "Data outsourcing", "Cross-scripting attack" and "metadata spoofing attack". Apart from this, several factors are responsible for data vulnerability. These include the Virtual Machine (VM) replication, VM rollback, VM hopping and VM escape which can pose a threat to the integrity of information [16].

Besides the types of attack, various encryption systems are also developed to protect confidential data. Hillar and co-researchers examined some encryption systems of the cloud that include the Onion encryption where "Data encryption" and "Query Execution" algorithms are used [17]. Searchable encryption also uses the data encryption algorithm, other encryption systems include "Fully Homomorphic Encryption", Attribute-based encryption" and "Fine-grained access control"[18]. These encryption schemes have shown promising advantages in data sharing, storing, decentralisation and decryption. Figure 3 shows the data encryption and decryption framework using attributes and key access.

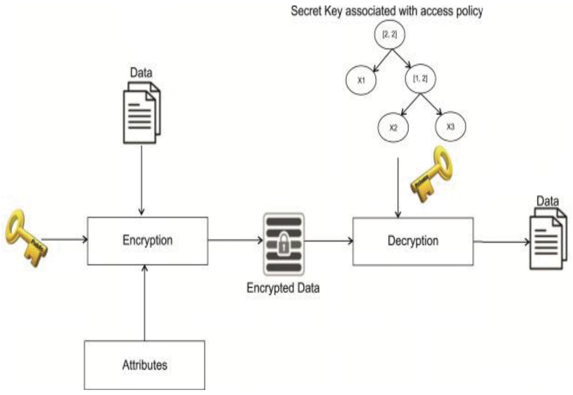

Fig. 3. Data encryption and decryption framework

(Source: [18])

According to Lee and others, the "Advanced Encryption Standard" or AES algorithm is an excellent tool for protecting data with an outstanding speed. This is a symmetric algorithm used for preserving secret keys confidentially [19]. The mechanism of this algorithm is it has 10-14 rounds with 128-256 key bits which together provide encryption several times. This algorithm is effective against most attacks; however, it is not effective against "Brute Force" and "Linear Crypt Analysis" attacks.

III. Research Methodology

The research objectives have been met by both primary and secondary research conduction. The primary research has been carried out with ***65 Cloud computing experts** of the UK*. The individuals who have been developing the security systems of cloud computing and working with it have been selected to conduct the survey. The researchers shared an online social media post concerning the survey. Around 121 individuals have shown interest in the survey. Therefore, the researchers selected *a total of 65 individuals who have been working in this field for more than 6 months*.

The survey respondents were asked to provide their email addresses and via the email addresses, a google survey form has been distributed. The survey form consisted of the demographic and essential survey questions related to the privacy and security knowledge of cloud computing. The respondents provided their opinions on the security and encryption system of cloud computing. The data was collected and converted to numerals in ***Microsoft Excel***. After that, the data was analysed and interpreted in the following section.

Secondary journal articles have been analysed to collect relevant supportive data for the primary data discussion. The secondary data will allow the researchers to bring common issues regarding this topic.

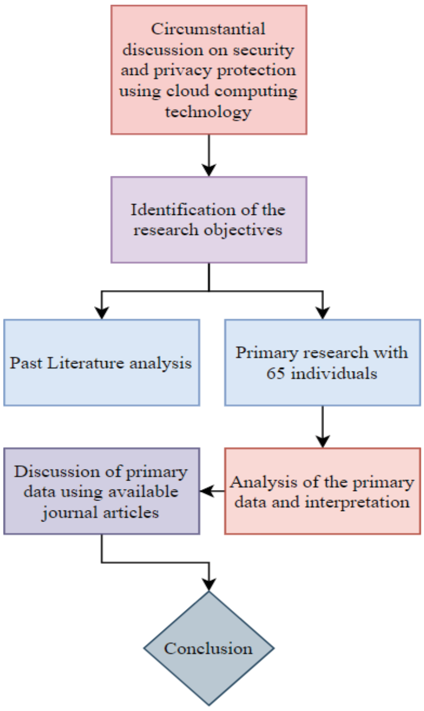
Circumstantial discussion on security and privacy protection using cloud computing technology
Identification of the research objectives
Past Literature analysis
Primary research with 65 individuals
Discussion of primary data using available journal articles
Analysis of the primary data and interpretation
Conclusion

Fig. 4. Flowchart of the research

(Source: Created by the researchers)

IV. Analysis and Interpretation

This section excludes the analysis of demographic data and focuses on the privacy and security related primary data. As the individuals have at least 6 months of experience in cloud computing; thus, their opinions have been analysed only. The survey questions and their respective responses are shown below.

Q1. Do you think the privacy and security system of cloud computing is advantageous in terms of securing confidential information?

TABLE I. SURVEY RESPONSES OF QUESTION 1

(SOURCE: CREATED BY THE RESEARCHERS)

Google form options	Total participants	Collected responses	Percentile calculation
Strongly agree	65	21	32%
Agree	65	13	20%
Neutral	65	16	25%
Disagree	65	9	14%
Highly disagree	65	6	9%

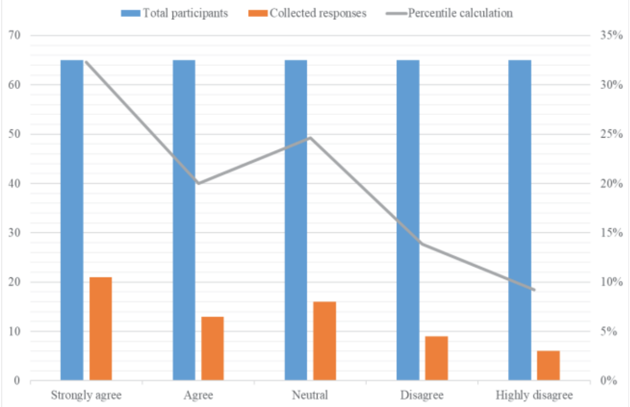

Fig. 5. Graphical representation of survey responses (Question 1)

(Source: Created by the researchers)

The first survey question (Table I, Fig. 5) has been asked to understand whether Cloud computing has any contribution to the privacy and security of data or not. The responses suggest that a total of 52% of respondents agreed that cloud computing strengthens the security of storage and sharing systems. 25% of them were neutral as there are several threats to this technology. A total of 23% disagreed on this and stated that cloud systems are becoming easier for people to access from remote places. Moreover, as the security systems are improving, new types of threats are also arising.

Q2. What do you think is the most common attack in cloud computing?

TABLE II. SURVEY RESPONSES OF QUESTION 2

(SOURCE: CREATED BY THE RESEARCHERS)

Google form options	Total participants	Collected responses	Percentile calculation
Attacks on the services platforms (PaaS and IaaS)	65	14	22%
Brute force attack	65	15	23%
Data outsourcing	65	14	22%
Wrapping attack	65	11	17%
Spoofing attack	65	11	17%

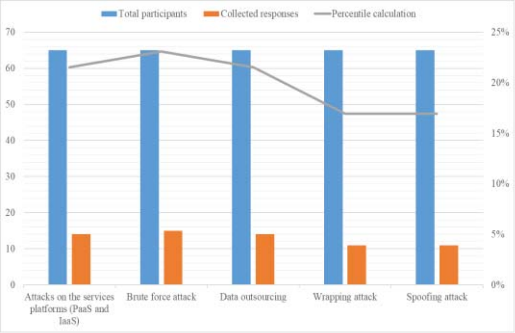

Fig. 6. Graphical representation of survey responses (Question 2)

(Source: Created by the researchers)

The second survey response (Table II, Fig. 6) show that various types of attacks occur in cloud computing. The responses do not show any prevalent attack. However, 22% agreed that Data outsourcing, 23% agreed with brute force attacks and 22% agreed that PaaS and IaaS attacks are common in cloud computing. Other attacks include Spoofing (17%) and Wrapping attack (17%).

Q3. What do you think is the most encryption system in cloud computing?

TABLE III. SURVEY RESPONSES OF QUESTION 3

(SOURCE: CREATED BY THE RESEARCHERS)

Google form options	Total participants	Collected responses	Percentile calculation
Blockchain technology	65	19	29%
Virtual Private Network	65	4	6%
Encryption schemes such as searchable, homomorphic, onion and fine-grained encryptions	65	13	20%
Biometric identification	65	11	17%
Identity-based encryption	65	8	12%
Attribute-based encryption	65	10	15%

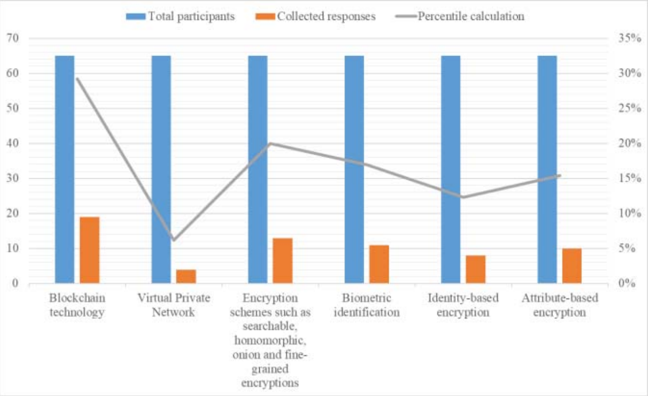

Fig. 7. Graphical representation of survey responses (Question 3)

(Source: Created by the researchers)

The third question has been asked to understand the most secure technology or encryption system in cloud computing (Table III, Fig. 7). 29% of the respondents agreed that blockchain is a more secure technology than other encryption systems of cloud computing. 20% of the respondents also agreed that encryption schemes such as searchable encryption and onion encryptions are beneficial to protect security keys. The onion encryption contains more than one security layer. 15% and 12% of respondents agreed that "Attribute-based encryption" and Identity-based encryptions are two other useful encryption systems. Few of them (6%) agreed that Virtual Private Network (VPN) is advantageous.

Q4. What do you think are the common attacks on blockchain technology?

TABLE IV. SURVEY RESPONSES OF QUESTION 4

(SOURCE: CREATED BY THE RESEARCHERS)

Google form options	Total participants	Collected responses	Percentile calculation
Smart contract	65	11	17%
Wallet theft	65	17	26%
Ingestion into blockchain	65	19	29%
Replay attacks	65	10	15%
Double spending	65	8	12%

As the blockchain is an interesting technology to maintain confidentiality in cloud computing, it is important to know the security threats as well. Table IV shows that Blockchain network ingestion is the most common attack on the blockchain (29%). 26% of the respondents agreed that Wallet theft is also a common security issue in the blockchain. The least prevalent attacks on blockchain include the smart contract (17%); replay attacks (15%) and Double spending (12%).

V. Discussion and Findings

The survey responses have upheld the issues and opportunities of security in cloud computing. Most of them agreed that cloud computing is more secure than conventional storage and data sharing systems. Concerning this, e Rubab and colleagues stated that cloud computing is secure; however, certain encryption and attribution systems are required to eliminate the existing security challenges [20]. The current study has also shown that many cloud computing experts disagreed which suggested the major concerns of security.

The research has isolated the common types of attacks on the cloud computing system which include spoofing, wrapping, brute force, service platform and data outsourcing attacks [21]. Data outsourcing is prevalent here which is deletion or manipulation of essential data [22]. According to other studies, wrapping attacks are more prevalent than the other attacks where the signatures and messages are duplicated for verification [23]. As the more prevalent attack has not been found from the primary research, all of the attacks can be considered and need to be addressed [24]. Spoofing and data outsourcing are two similar types of attacks that *steal, delete or manipulate* original data.

The study has found that blockchain is a more secure technology to store and share confidential data. Evidence suggests that blockchain is a decentralised technology that provides an excellent defence system. The decentralisation system provides the monitoring capability by more than one authority. Usually, the other technologies and their security systems are monitored by one authority or organisation; whereas, the blockchain is a distributed network and more than one authority monitors the suspicious activity [25].

Although various security systems are available, cloud computing is still vulnerable to some of the attacks that have been shown in the interpretation (wallet theft, ingestion and so on). Therefore, the security system of cloud computing needs continuous improvement instead of relying on a single encryption system [26].

VI. Conclusion

The study has executed the circumstantial discussion of privacy and security using cloud computing technology. Various security and privacy threats have been obtained for which researchers are integrating new attributes to strengthen the security system. It is a highly controversial and circumstantial debate where it cannot be said that one particular encryption or security system is enough to eliminate all the threats. The cloud computing experts considered blockchain to be more secure; however, still, certain vulnerabilities need to be addressed. Other studies were also unable to determine the particular technology which is most secure. Therefore, it can be said that, as the threats and attacks are increasing, the security system requires continuous improvement.

References

[1] Chenthara S, Ahmed K, Wang H, Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access. 2019 May 30;7:74361-82.

[2] Sun P. Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications. 2020 Jun 15;160:102642.

[3] Gupta BB, Yamaguchi S, Agrawal DP. Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimedia Tools and Applications. 2018 Apr;77(7):9203-8.

[4] Lee J, Yu S, Kim M, Park Y, Lee S, Chung B. Secure key agreement and authentication protocol for message confirmation in vehicular cloud computing. Applied Sciences. 2020 Jan;10(18):6268.

[5] Tsaregorodtsev AV, Kravets OJ, Choporov ON, Zelenina AN. INFORMATION SECURITY RISK ESTIMATION FOR CLOUD INFRASTRUCTURE. International Journal on Information Technologies & Security. 2018 Oct 1;10(4).

[6] leadingedgetech.co.uk. (2022). How secure is cloud computing?. Available at: https://www.leadingedgetech.co.uk/it-services/it-MRHconsultancy-services/cloud-computing/how-secure-is-cloud-computing/ [accessed 1 March 2022]

[7] Torkura KA, Sukmana MI, Cheng F, Meinel C. Cloudstrike: Chaos engineering for security and resiliency in cloud infrastructure. IEEE Access. 2020 Jul 6;8:123044-60.

[8] Bodkhe U, Tanwar S, Parekh K, Khanpara P, Tyagi S, Kumar N, Alazab M. Blockchain for industry 4.0: A comprehensive review. IEEE Access. 2020 Apr 17;8:79764-800.

[9] Namasudra S, Chakraborty R, Majumder A, Moparthi NR. Securing multimedia by using DNA-based encryption in the cloud computing environment. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2020 Dec 16;16(3s):1-9.

[10] Li J, Wang S, Li Y, Wang H, Wang H, Wang H, Chen J, You Z. An efficient attribute-based encryption scheme with policy update and file update in cloud computing. IEEE Transactions on Industrial Informatics. 2019 Jul 25;15(12):6500-9.

[11] Kumar P, Alphonse PJ. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. Journal of Network and Computer Applications. 2018 Apr 15;108:37-52.

[12] Yang Y, Chen X, Chen H, Du X. Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing. IEEE Access. 2018 Mar 28;6:18009-21.

[13] Li J, Chen X, Chow SS, Huang Q, Wong DS, Liu Z. Multi-authority fine-grained access control with accountability and its application in cloud. Journal of Network and Computer Applications. 2018 Jun 15;112:89-96.

[14] Basu S, Bardhan A, Gupta K, Saha P, Pal M, Bose M, Basu K, Chaudhury S, Sarkar P. Cloud computing security challenges & solutions-A survey. In2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) 2018 Jan 8 (pp. 347-356). IEEE.

[15] Saravanakumar C, Geetha M, Manoj Kumar S, Manikandan S, Arun C, Srivatsan K. An efficient technique for virtual machine clustering and communications using task-based scheduling in cloud computing. Scientific Programming. 2021 Jul 19;2021.

[16] Hiller J, Pennekamp J, Dahlmanns M, Henze M, Panchenko A, Wehrle K. Tailoring onion routing to the internet of things: Security and privacy in untrusted environments. In2019 IEEE 27th International Conference on Network Protocols (ICNP) 2019 Oct 8 (pp. 1-12). IEEE.

[17] Yousuf H, Lahzi M, Salloum SA, Shaalan K. Systematic review on fully homomorphic encryption scheme and its application. Recent Advances in Intelligent Systems and Smart Applications. 2021:537-51.

[18] Lee BH, Dewi EK, Wajdi MF. Data security in cloud computing using AES under HEROKU cloud. In2018 27th wireless and optical communication conference (WOCC) 2018 Apr 30 (pp. 1-5). IEEE.

[19] e Rubab K, Azhar T, Anwar M, Majeed S. Security threats in cloud computing: Trend and challenges. International Journal of Computing and Communication Networks. 2020 Sep 12;2(1):29-35.

[20] A. Jain, A.K.Yadav & Y. Shrivastava (2019), "Modelling and Optimization of Different Quality Characteristics In Electric Discharge Drilling of Titanium Alloy Sheet" Material Today Proceedings, 21, 1680-1684

[21] Jain, A. K. Pandey, (2019), "Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191

[22] A. Jain, A. K. Pandey, (2019), "Multiple Quality Optimizations In Electrical Discharge Drilling Of Mild Steel Sheet" Material Today Proceedings, 8, 7252-7261

[23] Panwar, D.K. Sharma, K.V.P.Kumar, A. Jain & C. Thakar, (2021), "Experimental Investigations And Optimization Of Surface Roughness In Turning Of EN 36 Alloy Steel Using Response Surface Methodology And Genetic Algorithm" Materials Today: Proceedings. Https://Doi.Org/10.1016/J.Matpr.2021.03.642

[24] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Metal Matrix Composite Using Electric Discharge Machining: A Short Review" Evergreen, 8 (4), pp.740-749.

[25] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Fiber Matrix Composite through Electric Discharge Machining: A short review" Material Today Proceedings. https://doi.org/10.1016/j.matpr.2021.07.288

[26] Gao YL, Chen XB, Chen YL, Sun Y, Niu XX, Yang YX. A secure cryptocurrency scheme based on post-quantum blockchain. IEEE Access. 2018 Apr 18;6:27205-13.