SECURING HEALTHCARE DATA USING ATTRIBUTE BASED ENCRYPTION TECHNIQUES IN CLOUD ENVIRONMENT

C.Krishnan [1], Dr.T.Lalitha[2]
[1]Research Scholar, Computer Science, Research and Development Centre, Bharathiar University, Coimbatore.
[2]Research Supervisor, Computer Science, Research and Development Centre, Bharathiar University, Coimbatore.
Email I'd: krishnan.peaceful@gmail.com[1], lalithasrilekha31@gmail.com[2]

Abstract: In recent years, there is a tremendous demand for healthcare systems that establishes a framework to reduce the time required to complete the work and the expensive procedures used to recover a patient's medical report, along with the constant integration of various sets of medical data to furnish it to the healthcare industry. EHRs (Electronic Health Records) widely permit the insurance companies, patients, and healthcare providers to launch, manage and process the healthcare information of the patients from anywhere at any time. Therefore, healthcare providers support moving the medical data and processes to the clouds, which can perform the processes more effectively and avoid the physical distance between patients and providers. However, securing sensitive kinds of data is a severe issue in a cloud environment. This article proposes a new framework and analyzes the four kinds of encryption techniques. Among the four methods, the HIBE approach produces better results.

Keywords: Encryption, Attribute, Cloud Computing, Patient, Healthcare

I INTRODUCTION

Cloud services empower the doctors to access the healthcare records of the patients, even if they are many kilometers away. The need to make phone calls to the doctors to know the patient's health records have been dismissed and directly accessed from the cloud. Ensure the control carried by the patients on their own PHRs (Patient Health Records); cloud computing is an excellent method to conceal the PHRs before outsourcing.

Out of all the advantages of cloud computing in healthcare systems, data security and data privacy are major concerns that make the healthcare industry prosper and move ahead to adopt new technologies. The cost of cloud computing benefits neutralizes the high risk caused by emergencies due to information security addressed cautiously. According to the critical data level that needs to be stored or processed and the features of the specific cloud services designed by the cloud providers, the types of risk differ.

A novel patient-centric approach proposes this paper, along with a suite of mechanisms to obtain data access control over PHRs deposited in the semi-trusted servers. The ABE (Attribute-Based Encryption) techniques leverage to conceal each patient's PHR record to achieve scalable and fine-grained data access control for PHRs. Satisfy protects the PHR deposited in the semi-trusted server, and the ABE technique adopts it as the primary encryption primitive. With ABE, policies accessing the data are established based on the features of the data stored or the user. It enables the patient to share their PHR selectively among the wide range of users, encrypting the record beneath the set of features without establishing all the users present in the list.

II LITERATURE REVIEW

The Cloud computing technique is an effective system for accessing and storing data. The rising concept in exchanging health information for research and others is sharing of the electronic PHR. Confidentiality of the information except to the authorized users is the powerful security needs for the health record. Huda Elmogazy et al., 2016 has conducted a study to examine the requirements and proposed an algorithm to assist the healthcare cloud providers in securing storage and sharing of the patient's data that they host. The algorithm designs to permit only legitimate users to acquire the portion of the data records granted for access. The main concern will be on the unique security problems of Cloud computing used in the healthcare industry and the assistance rendered by the ABE in addressing the regulatory requirements in the healthcare area. The proposed study on ABE assures data confidentiality, authentication, integrity, and availability in the hierarchy's multi-level order. It permits healthcare providers to add or delete any order without any difficulty, which views as a chief benefit, especially in medical research [1].

With a progressive increase in the adoption of EHRs by many healthcare organizations, the case for data storage in the cloud has become captivating for locating the EHR systems as it is inexpensive and renders a pliable, broad mobile access that is needed increasingly in the developing market. Before implementing cloud-based EHR systems, the issues like data security, overall performance, and patient privacy to be addressed. A standard encryption technique includes a public key and symmetric key to perform EHR encryption/decryption results in increased control on access and achievement of performance overhead. Suhair Alshehri et al. 2012 elaborates an ABE method named CP-ABE (Ciphertext Policy ABE) to conceal EHRs concerning the healthcare providers' features or credentials and to decrypt the EHRs that possess the set of features necessary for proper access. Using CP-ABE, a cloud-based EHR system designed and utilized analyzes the scalability and flexibility of the proposed along with the preliminary tests to interpret the scalability and flexibility of the given approach. The proposed work presents a framework for a secured system based on a cloud computing EHR system implemented with CP-ABE, rendering efficient solutions to the issues based on standard encryption mechanisms. The framework also investigates the feasibility of the acquired CP-ABE on the aspect of storage overhead and performance. The results clarify that the described framework gives better performance and utilizes negligible storage, and therefore it can be used in the place of standard encryption procedures in the cloud-based EHR approach [2].

Medical organizations face the challenge in acquiring cloud-based EHR services because of the risk associated with data breaches and leads to patient data compromise. The already existing approaches strive at patient-centric design for the EHR management in which the patients influence the power of authorizing the data access. However, it generates an essential overhead for the health victim who has to approve every medical record access. The practical issue associated with the above method is that every time the patient may not be in a situation to authorize the access. Therefore, the need to create an overall authorization delegation mechanism to have a comfortable, safe and secure cloud-based EHR framework has emerged into a new field of research. Maithilee Joshi et al., 2018 have propounded a centralized, novel, feature-based authorization mechanism that uses the ABE technique and permits entrusted procure access of the patient files. The stated mechanism converts the service management overhead obtained from the patient to the health organization and permits easy division of cloud-based EHR authority of access to the health care providers. A novel ABE approach design along with a prototype system to explain the approach [4].

Most sensitive data, such as PHRs, are placed on a third-party server like the cloud in the current situation. At present, the PHR system develops as a model centered on patients loaded with health information exchange. The PHR service providers transform the PHR application services to the cloud to minimize the operational cost associated with the specialized data centers and to utilize the cloud's elastic resources. A new algorithm of public cryptosystem named ABE uses to ensure PHRs and attempt fine-grained access control. The system proposed by Snehal Pise, 2014 addresses issues like crucial management, efficient user revocation, and scalability. The approaches focus primarily on the multi-authority and multi-owner schema. The users present in the system classified as private and public domains. In the scenario of emergency, the proposed system assures break-glass access. Besides, it assists on-demand repudiation of user or feature. The established system is healthy in terms of scalability, security, and efficiency. The PHR system illustrated assures security in the sharing of PHRs at the level of fine-grained access. Many users from the private and public domains can effectively go through the health files. The framework addresses the challenges generated by multiple users and owners, and on the other hand, it also minimizes the complexity created by key management while enriching the guarantee for privacy than any other existing method [5].

In recent years, a notable increase observes in the ABAC solicitation (Attribute-Based Access Control) in the e-health sector. An E-health system utilizes to reserve the electronic version of the patient's medical reports. The reports commonly categorize concerning their usage, i.e., PHR and EHR, where PHRs are the digital medical reports where patients are responsible for their data, while EHRs are electronic patient medical records that the healthcare providers clenched. EHRs and PHRs are considered a crucial asset to access the control mechanism to synchronize its access. The ABAC method proposed by Livinus Obiora Nweke et al., 2020 was illustrated to be an effective and efficient algorithm for rendering fine-grained access control over the expository assets. A survey conducts on the review of existing literature on the implementation of ABAC in the e-health framework area to acknowledge the suitability of the ABAC approach for e-health. The research work was classified based on the application of ABAC in EHR and PHR; then, the concept discussed to pin the future challenges. It serves as a basis for the collection and advancement of ABAC usage in e-health systems. The survey results reveal that the cloud-based repository of EHR and PHR has become very popular among healthcare professionals, and out of that, CP-ABE is one of the commonly used techniques for rendering privacy and security guarantees in the cache of PHR in the environment of the cloud. Furthermore, a comparison of various frameworks implemented in the current work and their key characteristics present for discussing its differences. The survey investigates the approach description and the future challenge faced in applying the prescribed model [6].

A state-of-art patient-centric approach and suite of operation for control of data access prescribe by Y.B. Gurav et al., 2014, to preserve the PHRs in semi-trusted servers. However, some obstacles like scalability in key management, risks associated with privacy exposure, efficient user revocation, and flexible access have endured the most salient challenge of acquiring the fine-grained and cryptographically enforced control over the data access. The proposed approach emphasizes the scenario of multiple data owners. In the PHR system, the users segregate into multiple security domains that extensively minimize the complications of key management for the users and owners. In real-time practice, some limitations observe in MA-ABE (Multi Authority ABE) concerning the property of disjunctive and issues view during revocation. As it influences the non-revoked users, the approach was transferred into ABBE (Attribute-Based Broadcast Encryption) to satisfy the disjunctive property and to handle revocation [8].

Vishal Jagdale et al., 2015 have developed a model and procedure to control data access in the PHRs piled in the cloud servers. ABE encryption approach provides effective data access control over the PHRs by encrypting all the PHR files. The approach concentrates on the scheme based on multiple data owners and separates the data users into the security domains, reducing the key management complexity. The system enables modification in the file features and break-glass access during emergency conditions. The results obtained from extensive analysis present that the model provides a strong structure in securing the sharing of PHRs efficiently. It proves that ABE based technique secures the health records in a better way. An enhanced ABE technique, MAABE, permits the patients to access public users and different users from the public domain with different qualifications, roles, and responsibilities. Thus, the improved system supports the dynamic policy management model and maintains the security and privacy of the PHRs [9].

Attain the scalable and fine-grained data access control for the PHRs, Susheel R. Deshmukh, 2013 has proposed an ABE to encrypt all the patients' PHR files and improve the interoperability for good access to the data among the various departments of the healthcare industry. The proposed system supports effective and revocation of features along with emergency access in critical situations. Most of the health management systems design to satisfy the interests of the medical service providers. Keep the patients' interest away, which leads to problems oriented with interoperability and quality healthcare of the PHR among the patients and healthcare providers [10].

III PROPOSED FRAMEWORK

The recent development in the healthcare industry projects a rapid transformation towards computerization, and the need for online clinical data exchange increases between various healthcare providers [11]. Exploiting a secured path for data exchange has become the major obstacle in the healthcare industry. PHR is an online, patient-centric algorithm for the safe exchange of healthcare information. It allows the patients to coordinate and access their lifelong healthcare data with other users [12]. Cloud computing has emerged as a revolutionary concept in the area of the healthcare industry [13]. The following Fig. 1 demonstrates the proposed framework used to secure the patient's health data using the ABE technique.

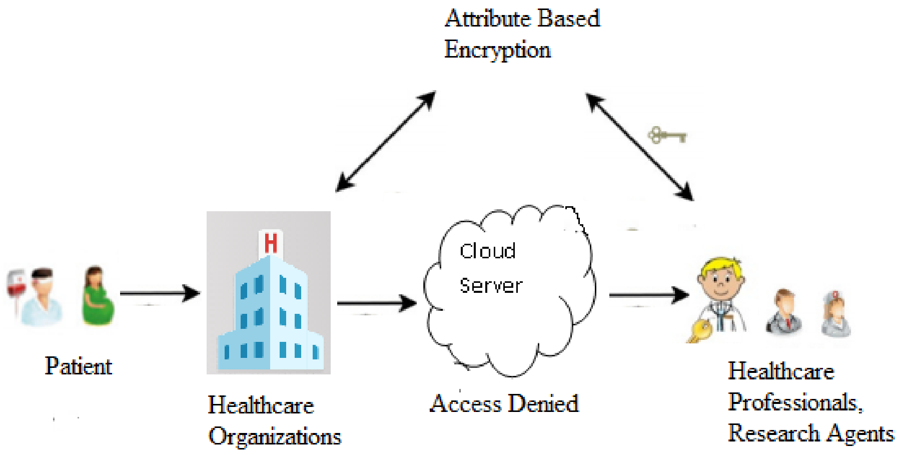

Fig 1. Proposed Framework of Secure Health Data

Due to the easy adoption of the technology, greater workflow efficiency, and significant low maintenance cost, cloud computing has gained its popularity moving ahead. The proposed framework shows an appropriate encryption model where the patients can protect their medical records and share the information between different units utilizing a cloud server [14-18]. Full control gain by the patient upon their data and the ABE. They secured its privacy. Patients hold full control of their privacy by concealing the PHR files utilizing ABE.

IV ABE TECHNIQUES

The ABE techniques leverage encrypt all the patient's PHR report to achieve scalable and fine-grained data access control of the PHRs [19]. The owner of the data updates their data into the arbitrary cloud data centers.

KP-ABE (Key Policy ABE)

Confidentiality of the information except for the authorized users and accessing are powerful security needs for the health record. In standard encryption methods, every user has their public security key

[20]. If the user needs to encrypt the given message for many recipients, it needs to measure the ciphertext for every user's key. It leads to time and space consumption.

KP-ABE plans to encrypt the given message a single time by the sender. It is a strategy to the user's secret key that will decide if users will be permitted to decrypt:

- Texts named with ω set of descriptive type identifiers.
- The access rule P match with the confidential key
- The works of decryption execute if $P(\omega) = 1$.

CP-ABE

CP-ABE approach is nearer to the typical access techniques. It also executes in two ways, by allocating identifier groups to the secret key, and senders can state an access control policy that recipient attribute groups should obey. Using CP-ABE, a cloud-based EHR system designed and utilized analyzes the scalability and flexibility of the proposed along with the preliminary tests to interpret the scalability and flexibility of the given approach. The framework also investigates the feasibility of the acquired CPABE on the aspect of storage overhead and performance. CP-ABE is mainly used in the PHR system to store sensitive kinds of data.

CP-ABE approach uses four primary phases: Setup Phase, Key making Phase, Encryption Phase, and the Decryption Phase.

Setup Phase: This phase obtains no input value except the implicit privacy argument. The outcome of this phase is public argument PH and the MK master key.

Key Creation Phase(S, MK): This phase obtains an input data MK master key, and the group of arguments S illustrates the key value. The outcome of this phase is the SK secret key.

Encrypt Stage(PK, M, A): This phase accepts the input values like public arguments PK, M message, and the structure of the access control A. This phase encrypts the message M and makes a CT cyphertext.

Decrypt Phase(PK, SK, CT): This phase accepts input public arguments PK, and the ciphertext CT, access value A, and the SK secret key, which is a secret key for the S group of identifiers. If the group S of identifiers convince framework A, then the phase decrypts the given message and returns the M message.

CP-ABSE A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme)

According to Hui Yin et al., 2019, CP-ABSE contains the following polynomial-time approaches.

Setup$(1^{\lambda}) \rightarrow (dk_1, SSP, dk_2)$: The data owner accesses this phase. It accepts the argument λ and produces two types of keys dk1, dk2, and SPP(System Public Parameter). The data owner uses the key dk1 to encrypt the index word with the access value and uses dk2 to make the private keys for the user based on the user's identifiers.

Keygen$(SPP, dk_2, S_u) \rightarrow K_u)$: It accesses by the owner of the data and makes the keys for the user u with the group of identifiers S_u. It accepts the identifier SSP, dk_2, and the user's identifiers group S_u and the outcome u's secret key K_u.

Encind$SPP, dk_1, w, T_w) \rightarrow I_w)$: It is executed by the owner of the data and encrypt as an index word. This phase accepts the input SSP argument, dk_1 key and the w index word, and the T_w access tree, and the result is I_w ciphertext of w's.

Trpdr$(SSP,\ K_u, q) \rightarrow T_u)$: This step is processed by u data user. It accepts the input SSP, the q query word and the $u's$ secret key K_u, and the resultant value $T_u(q)$.

Search$(SPP, I_w, T_u(q)) \rightarrow 1$: The server system executes this step. It accepts the input parameter SSP, I_w encrypted index word, and $T_u(q)$ trapdoor given by u, and the output comes the value 1 when $w = q$ and the $u's$ identifier set S_u convenience the embedded access tree in $I_w,$ concurrently; otherwise, the output is zero.

HIBE (Hierarchical Identity Based Encryption)

According to Renu Mary Daniel et al., increasing the versatile encryption technique by distributing PKG(Private Key Generator) workload between many junior-stage PKGs makes easy intermediary key and secret key allocation. Using its framework, HIBE may arrange to offer access power in the cloud, WSN (Wireless Sensor Network and MMORPGs (Massively Multiplayer Online Role-Playing Games). It uses encrypted value, totally secure communication, private encryption, partial allocation, and control of the damage. The model's performance assesses by the various matrices like receiver's anonymity, assumptions of the hardness, pairing types, reduction tightness, etc.

These approaches guarantee a high degree of privacy to the patient's health record by using multi-authority ABE. The research conducted discusses the ABE-based model to secure the PHRs.

V RESULT AND DISCUSSION

Centralized servers use to maintain the PHRs that consist of patient's personal health information and diagnosis reports. One of the patient-centric approaches in health information exchange frequently outsourced to store at a third-party server, namely cloud providers. There is a concern about privacy as the approach deals with the patients' personal health information that get exposed to arbitrary servers and unauthorized parties. The schemes to enrich the security are used to preserve the health sufferer's personal data to accessed in public. To ensure patients' control over their own PHRs generates a promising approach to encrypt the personal medical report before outsourcing. In this research work, four kinds of ABE techniques such as KP-ABE, CP-ABE, CP-ABSE, and HIBE uses to secure the patient's health-related data. The performances of the ABE techniques are analyzed based on their execution time. The execution time can be calculated based on the number of attributes. Among the four techniques, HIBE uses less for encrypting the attributes. Table 1 shows encryption time taken by the encryption methods depends on the number of attributes.

Table 1 Encryption Time of ABE techniques

	5 Attributes	9 Attributes	11 Attributes
KP-ABE	4.75	5.15	7.1
CP-ABE	6	6.15	7.5
CP-ABSE	6.14	6.25	7.75
HIBE	3	5.05	6.23

The following Fig. 3 illustrates the performance of the ABE techniques.

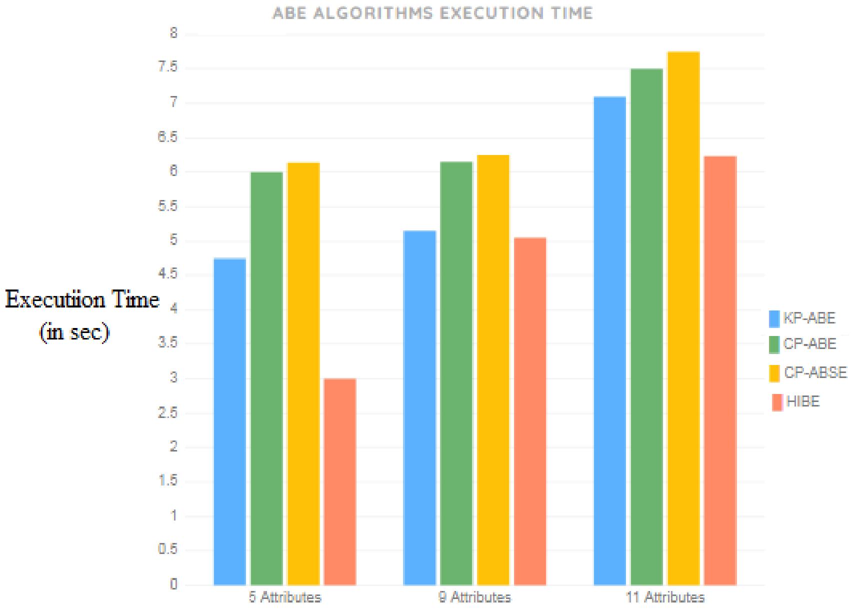

Fig 3 Performace of ABE Techniques

VI CONCLUSION

The most emerging framework in the health information exchange sector is PHR, which store at cloud servers. Despite its wide usage, various privacy issues identify due to the interference of unauthorized people. Assure the patients control their PHRs; it is a model to encrypt the patient's medical reports before the cloud storage. Still, issues like efficiency in key administration, risk of privacy, efficient user administration, and flexible access remain to be solved to achieve cryptographically imposed control on the data access. Enhance the interoperability; often, PHR hosted by arbitrary cloud service providers. However, in recent years many cloud data rupture incidents are observed due to privacy concerns related to outsourcing patients' PHR to the cloud server. During encryption, the chief challenge is to attain fine-grained access control on the PHR data in a secure and scalable way. This research work uses four types of ABE methods uses to encrypt the patient's sensitive data. The performance of the ABE approaches was assessed based on their encryption time. Among the four ABE techniques, HIBE has been taken less time for encryption.

REFERENCES

[1] Huda Elmogazy & Omaimah Bamasag(2016), “Securing Healthcare Records in the Cloud Using Attribute-Based Encryption” , *Computer and Information Science*, Published by Canadian Center of Science and Education Vol. 9, No. 4, ISSN 1913-8989 E-ISSN 1913-8997.

[2] Suhair Alshehri, Stanisław P. Radziszowski, & Rajendra K. Raj(2012), “Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption”, *IEEE 28th International Conference on Data Engineering Workshops*, pp.. 143-146.

[3] Nirmala Sugirtha Rajini, S(2015)," Access Control in Healthcare Information Management Systems Using Biometric Authentication", *International Journal of applied environment sciences(IJAES),* vol. 10 no.1, pp.143-148, ISSN: 0973-6077.

[4] Maithilee Joshi, Karuna P. Joshi & Tim Finin(2018), Attribute Based Encryption for Secure Access to Cloud Based EHR Systems, *IEEE 11th International Conference on Cloud Computing*, pp. 932-935.

[5] Snehal Pise(2014) Security of Personal Health Records through Attribute Based Encryption in Cloud Computing, *International Journal Of Engineering Research & Technology*, Vol. 03, No. 01, pp. 1952-1954.

[6] Livinus Obiora Nweke, Prosper Yeng, Stephen D. Wolthusen & Bian Yang(2020), “Understanding Attribute-based Access Control for Modelling and Analysing Healthcare Professionals’ Security Practices”, *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 2, 2020, pp. 683-690.

[7] S. Nirmala Sugirtha Rajini & E. Mercy Beulah(2016), “Cloud Based Architecture For Healthcare System”, *Asian Journal of Microbiology, Biotechnology & Environmental Sciences*, Vol. 18, No. 4, pp. 1017-1018.

[8] Y.B.Gurav & Manjiri Deshmukh(2014), “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption*”, International Journal of Computer Science and Mobile Computing*, IJCSMC, Vol. 3, No. 2, pp. .617 – 625.

[9] Vishal Jagdale, Dinesh Kekan & Ishwar Baride(2015), "Secure Sharing of Personal Health Records in Cloud using Attribute-based Encryption*", International Journal of Computer Science and Mobile Computing*, Vol.4, No. 4, pp. 309-312.

[10] Susheel R. Deshmukh(2013), ” Attribute-Based Encryption And Interoperability Of Personal Health Records In Cloud Computing*”, International Journal of Recent Advances in Engineering & Technology (IJRAET),* ISSN: 2347 - 2812, Vol. 1, No. 2.

[11] Benoit Libert(2014), "Key Policy Attribute Based Encryption And Public Key Encryption with Keyword Search."

[12] Hui Yin, Jixin Zhang, Yinqiao Xiong, Lu Ou, Fangmin Li, Shaolin Liao & Keqin Li (2019), “CP-ABSE: A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme, IEEE vol. 7, pp.5682-5694.

[13] Renu Mary Daniel, Elijah Blessing, Rajsingh & SalajaSilas(2017), “Analysis of hierarchical identity based encryption schemes and its applicability to computing environments “,*Journal of Information Security and Applications*”, Vol. 36, pp. 20-31.

[14] Natrayan L, and M. Senthil Kumar. "An integrated artificial neural network and Taguchi approach to optimize the squeeze cast process parameters of AA6061/Al2O3/SiC/Gr hybrid composites prepared by novel encapsulation feeding technique." Materials Today Communications 25 (2020): 101586.

[15] Magesh, S., et al. (2020) "Pervasive computing in the context of COVID-19 prediction with AI-based algorithms. "International Journal of Pervasive Computing and Communications, 15(5); 477-487.

[16] Sundaram, P. S. S., Basker, N. H., & Natrayan, L. (2019). Smart Clothes with Bio-sensors for ECG Monitoring. International Journal of Innovative Technology and Exploring Engineering, 8(4), 298-301

[17] Magesh, S., et al. (2020) "Concepts and Contributions of Edge Computing in Internet of Things (IoT): A Survey." 146 –156. DOI: 10.22247/ijcna/2020/203914

[18] Paranthaman V, K. Shanmuga Sundaram, and L. Natrayan. Influence of SiC Particles on Mechanical and Microstructural Properties of Modified Interlock Friction Stir Weld Lap Joint for Automotive Grade Aluminium Alloy. Silicon (2021): 1-11.

[19] Rammohan, S. R., Jayashri, N., Bivi, M. A., Nayak, C. K., & Niveditha, V. R. (2020). High performance hardware design of compressor adder in DA based FIR filters for hearing aids. International Journal of Speech Technology, 1-8

[20] Niveditha, V. R., and T. V. Ananthan. "Improving Acknowledgement in Android Application." Journal of Computational and Theoretical Nanoscience 16.5-6 (2019): 2104-2107.