International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-11 Issue-1, September 2021

Protection Aware User Identity and Data Storage (PAUIDS) Scheme for Management of User Identification in Cloud

R. Rajan, C. Sunitha Ram

Abstract*: Cloud computing the technology which have the capability of modifying the method computing strongly, and storage resources will be accessed shortly. User Identification is an entity to detect the user who using the system or website. In information technology the protection of information consistently become a major issue to handle. The data might place in various locations in the world since it become particularly serious. The two main factors regarding cloud technology are information protection and security. The cloud operators can easily reach the sensitive information that affects the data security and protection measures. Therefore, this research protocol mainly focuses on secure data storage that always been a significant feature of quality of service. To guarantee the 'rightness of users' information in cloud storage system a Protection Aware User Identity and Data Storage (PAUIDS) algorithm is proposed that separates the document and independently stores the user information in the cloud storage servers. The proposed algorithm reduces the encryption and decryption time in a cloud storage system and providing secure and efficient data storage in cloud environments.

***Keywords*: Data sharing, User Identity, Identity and Access Management, Data Storage, Cloud computing.**

I. INTRODUCTION

Information's are provided over the internet as a service in cloud computing on request basis. Frequently used technique called cloud computing increases the tendency in changing parallel and distributed computing atmosphere. Private cloud or public cloud or hybrid are used for the largest group of interconnected computers or network servers; these are used public cloud or private cloud or hybrid (Venkatakotireddy, G., et al., 2018 & D.Divya., et al 2014). Cloud computing services mainly divided into Infrastructure as a Service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS). The new cloud service model that is recently developed is a Functions as a Service (FaaS) The cloud is nothing but the data centres that the users can avail over the internet.

Manuscript received on August 03, 2021.
Revised Manuscript received on September 26, 2021.
Manuscript published on September 30, 2021.
* Correspondence Author
R.Rajan*, Ph.D Department of Research Scholar, Information Technology, SCSVMV University, Kanchipuram, Enathur (Tamil Nadu), India. Email: rajanrajavelu@gmail.com
Dr. C. Sunitha Ram, Assistant Professor, Department of Computer Science & Engineering, SCSVMV University, Kanchipuram, Enathur (Tamil Nadu), India. Email: sunithabasha@gmail.com

Some of the key characteristics of the cloud computing are multinency (resource sharing and cost among large users), maintenance (easy to maintain since user can access data anywhere over the internet), performance (architecture is built with the strong interface using web services), independent location (users can connect it from anywhere), etc. The proposed method intends to encode all information and store the information by using different cloud storage servers without causing large overheads and high latency. The paper contributions are followed as:

To Prevent risks from internal risks: it accomplishes high-level protection information storage partitioning information into various cloud storage servers, in which inside risks can neither misuse the information nor recover the data from stored information on the cloud storage server.

- To provide high proficiency information processing: the proposed framework will also maintain a strategic distance from causing large overhead and high latency.
- To guarantee the user identity protection and data trustworthiness, the new plan helps protected and effective dynamic tasks.
- To provide better security model and to demonstrate that the proposed method is highly effective and flexible against false information adaption assault, and considerably cloud server plotting assaults.

II. RELATED WORKS

Wang et al. (2012) described a statistical measure approach that rectified issues of secure keyword ranking retrieval from encrypted cloud data. The ranked search gradually enhances the framework usability by enabling relevance ranking based on retrieval result. This method also ensures the file retrieval accuracy without losing keyword privacy. Nazir et al. (2013) describes various cloud models, technical and security attacks issues that arise in cloud computing. This model also observes technical security issues caused due to utilization of cloud services and in addition offers an outline of key security issues. Secure cloud architecture are utilized to protect security threats for large-scale networks. However, the secure cloud architecture implementation cost is very high.

Huiqi Xu et al. (2014) presented a Random Space Perturbation (RSP) model which is a data perturbation method proposed to perform safe, and queries like competent range query and KNN query services in cloud environments.

RSP data perturbation mechanism integrated a random noise injection, encrypting the order-preserving process, expanding dimensionalities and arbitrary protuberance. It avoided malicious on the agitated data and queries. Srujana et al. (2013) implemented an efficient data retrieval scheme with the utilization of attribute-based encryption for cloud data storage with a substantial amount of data. It produced rich clarity as regards of fast retrievals with regards to general comparisons of various hunting entities. This methodology provides data security while data retrieval process takes place. Karthick et al. (2014) presented a highly decentralized information accountability framework that kept a record of the actual consumption of users' data in cloud environments. It pulled the Java Archive (JAR) programmable capabilities for both, creating a dynamic and transporting object which ensured users' accessibility. In this mechanism generated authentication and electronic logs are stored in local JARs. Manjeera Patil et al. (2013) developed a Hierarchical Attribute-Set-Based Encryption (HASBE) by improving the cipher text-policy of Attribute-Set-Based Encryption (ASBE). It implemented security scheme and constructed a prototype application that elaborated the evidence of concept for secure access control. Data Access Control for Multi-Authority Cloud Storage system with users (DAC-MACS) was proposed by Reddy G.V. et al (2017) to provide sufficient and protected knowledge curb for decoded also voiding. So personally establish a modern multi-authorization uses cipher text-policy of ASBE and modeled a sufficient feature cancellation method than manage one and the other protected along with increase low price also time measured them.

Liu et al. (2014) presented a model named Consistency as a Service (CaaS) that contained a large volume of cloud data and as well as multiple small audited data packets in clouds. Here the data cloud is managed by Cloud Service Providers (CSP's) as well as the group of users that amount to an audit cloud. It also verified the cloud data provider and maintained the promised level of consistency. Chhetri et al. (2012) implemented approaches that assisted multiple interaction models for software legal agreement establishment by providing consumers and Cloud Service Providers flexibility to select the services. It was most appropriate for given context, while simultaneously assisting in various concurrent software legal agreement interactions among various interaction models. Dastjerdi et al. (2012) developed a negotiation model for providers that considered the utilization of resources. It offered services during the negotiation and concedes of less utilized resources. Cloud provider strategy for cloud is provided when it created more on the price results. The framework displayed the ease of their profit's negotiation with multiple client requests. Rajkumar Buyya et al. (2009) designed several cloud efforts by taking the market-oriented perspective. It describes meta-negotiation transportation for the establishment of global cloud exchanges. The framework also exploits storage clouds for high performance content delivery. Indu et al. (2018) developed a model comprises of issues that is related to access management, authentication, security and services in cloud environment. The characteristics of cloud computing such as multi tenancy and the third party handled communications portraits the need of Identity and Access Management (IAM) mechanism. An Efficient Cloud Based Key Aggregate Data Sharing was proposed by Kumar, P. S., & Rao, B. T. (2016) & Karthikeyan A et.al (2020) to offer the key sharing mechanism between the user's and cloud service providers.

III. PROPOSED METHOD

Protection Aware User Identity Distributed Storage method gives the details of implementation of pre-processing steps, and how to implement the algorithm in a secured way by identifying the users and to separate the document independently. It also helps to store the information in the cloud storage servers in a safety manner. The proposed method PAUIDS algorithm and its working principle is in figure 1 along with processing details.

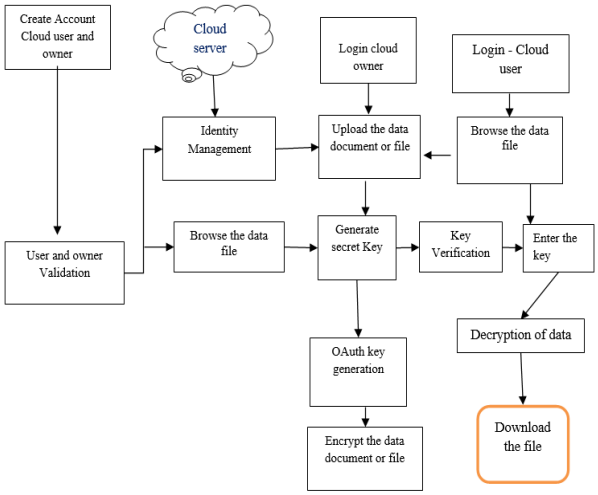

Figure 1: Block diagram of user identity and data sharing system

A. Data Owner

This module supports the data owner to register those details and also contains login details. Data owner can able to upload the encoded data document or file in cloud storage server setting even after login credentials. Here the data owner can be either an individual user or an organizational user. It ensures the data documents or files to be protected from unauthorized user.

B. Cloud Client

Generally, cloud client processes the query to the cloud storage server. On basis of the query the cloud storage server processes the corresponding data document or information file to the client. Client approval step is done before this query process. In the cloud server side, it validates the cloud with the username and their corresponding password for some security purposes. If the credentials are matched then the queries can be received from the cloud user and the particular document or data files can be searched in the database. From the cloud storage the cloud user can download the necessary data that he/she required. Therefore, the cloud users are able to access the file from the cloud only after getting access permission.

Finally, the data document or file is found from the database and send to the cloud client. If the cloud storage server detects the attacker, then the alternative path is set to that attacker. Figure 2 describes about the structure of User identity and access management model.

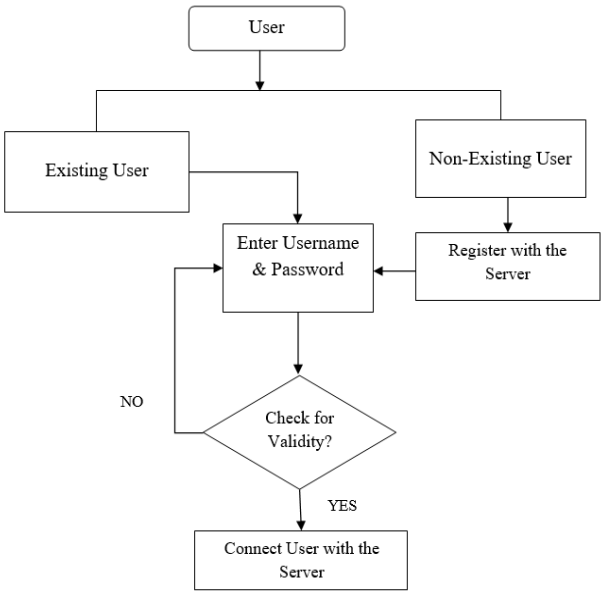

Figure 2: User Identity Access Management Structure

3.2.1 User

Users are the persons who hold some data to be stored in cloud environment and depend on the cloud for computing the stored information which comprises both individual users and organizational users.

3.2.2 Cloud Service Provider

CSP is an expertise in building and managing the distributed cloud storage servers who has significant resources. CSP offers the components of cloud computing services that own the storage spaces.

3.2.3 Third Party Auditor (TPA)

TPA, who has expertise and capabilities those users, may not have. TPA gives the unsureness to assess and expose risk of cloud storage services because of users upon request.

C. PAUIDS

Protection-Aware User Identity & Data Storage algorithm is designed to decide if the client requests for data packets are a high-level protection ensure. The algorithm is utilized to protect information from the unforeseen actions that are caused by cloud storage server-side workers. Protection of User Id protocol usually involves stage by stage transactions and user verification. Therefore validation, approval and accounting all three are considered for the protection of user identity and this process prevents the network from accessing of malicious users. Also, this proposed activity decides if the data packets will be stored in a distributed manner of various cloud storage servers. The cloud storage server will be connected to that information comprising sensitive data

D. User Identity Management

IAM is a framework of business processes and policies, and it facilitates the technologies like digital identities or electronic management. This system of identity and access management can be deployed through the model of cloud-based subscription or model of hybrid provided by a third-party dealer on premises. The organization can offer an identity authentication services through the perception of user's identity and access managing data regardless of where the service resides either internally or in the cloud computing environment. The company manages the information details of employee's identity repositories and those identities will not be shared with any other entities. The organization is centralized point that provides and manages the employee's identity which includes particular information of the user including password reset/preset /changes. Here security in banking transactions is considered. The stakeholders like CSP, registry, metering, billing and users are taken and the process is worked out through these stake-holders to make the system fully secured. CSP's establishes some of the conditions to release/offer any facility. User identity and security of the service providers must be given at various stages. The business management or association should register the company with good Service Providers (SP) since it should have better Service Level Agreements (SLAs) to avoid the unnecessary interruptions. The employee can come from any of the organization should hold the sufficient individual attributes in order to trace in case if any security bridge occur. Therefore, severe security measures from start to end should be maintained. The SP will be related with the registry and hence the authorization of unit may release any of the services. Here the services may be provided on basis of registry unit. Later the details regarding services are prepared and sent to billing unit and this generates the customer bill. Through SP customer receives the billing information that includes payable details. Nowadays there is a great improvement in online banking and this makes business easier through internet SP's or any network operators. The transactions in terms of payment and fund raising (deposit) are made simple between the users. To build the network more secure the PAUIDS algorithm uses hybrid security algorithms such as RSA and AES security models. Both security models undergo process like generation of keys, encryption and decryption.

3.4.1 RSA

The key generation part of the RSA algorithm is quite central and important, and this is something that's missing in most symmetric key algorithms, where the key generation part is not really complicated in terms of mathematical computations. Generation of keys in the process of RSA algorithm includes five main steps:

Step 1: Select any two prime numbers (m & n)
Step 2: Then compute x=m * n
Step 3: Evaluate $\varphi(x) = (m - 1) * (n - 1)$
Step 4: Pick an integer 'k' to facilitate $1 < k < \varphi(x)$
Making sure the property of $\gcd(k, \varphi(x)) = 1$
Make sure the integer 'k' and $\varphi(x)$ are being co-prime
Step 5: Now compute integer 'e' so as to facilitate $e = k - 1 \bmod \varphi(x)$.

Once the process of above steps is completed then two keys (asymmetric) are generated which will be used for further cryptographic (encrypting and decrypting) process.

Here the public key comprises with the components of 'x' and 'k' while the private key is comprised with the integer component 'e'.

Using large number of prime numbers is common in the key generation process for 'm' and 'n' and it takes minimum 512 bits, consequently makes the resultant 'x' with 1024 bits (x = m * n). Therefore, this process makes the cryptanalysis process quite hard and increases the complexity.

Encryption and decryption take place while completing the process of key generation with necessary variables using the algorithm. This is of course given the fact that K public has been generated, and consists of n and e. The formula used for encryption and decryption process is given in equation 1 and 2.

Encryption → C ≡ m.e (mod n) (1)

where 'm' is the message in plaintext. Decryption → M ≡ c.d (mod n) (2)

where 'c' is the cipher text.

The recipient's public key is applied for the message encryption process for the user's who needs for encryption, also the message should only be decrypted by the right user or authorized user. The private key generated is kept secret and the public key alone shared by the recipient. Message M is sent by the sender that is transformed into smaller number of bits 'n' by using a reversible transformation protocol called padding scheme. The encrypted cipher text of message M is sent to the recipient over internet.

3.4.2AES

Advanced Encryption Starndard (AES) is a symmetric function and this operation also uses same secret key in both the sender and receiver sides of the operation.

Step 1: AES key expands to 128 bits length (10>k<128)

Step 2: Each computed key hold 128-bit length with variant cycles

Step 3: Input → Message 'M' ← keys mixed

Step 4: K0 to Kn → Apply AddRoundKey function

Step 5; K0 to Kn → Apply SubBytes

Step 6: ShiftRows is performed for the keys Kn

Step 7: Again, perform AddRoundKey function for keys K2 to Kn-1

Step 8: Apply XOR operation for encryption process of message 'M'.

Step 9: Decrypt the cipher text using inverse pattern

Matrix form of conversions makes easier for computing encryption and decryption keys and hence the advanced AES algorithm converts the plain message text and keys to 4X4 matrix representation rather than using original form.

E. User Identity hiding algorithm

Pattern Matching strings 'C' and 'D' with lengths A and B, respectively which are stored as arrays with one temperament per element. This identity hiding algorithm is applied to find the INDEX of C in D.

1. Begin.
2. Set X=1 & fix Max = A-B+1.
3. Replicate steps 4 to 6 whereas X ≤ Max
4. Go over for E = 1 to R → Testifies all 'C' temperaments.
5. If C[E] ≠ T[X + E - 1], subsequently proceed with Step 9.
6. Inner loop ends();
7. Temperament → identified Successfully
8. Outer loop ends
9. Now Set X = X + 1.
10. Repeat steps 3 to 8
11. if process fails then set INDEX as '0'.
12. End

F. User Id Management Actions

Through internet service providers the users sent request to cloud service providers. The user verification is carried out with their identity or attributes and then the request is forwarded to the service provider if verified. By using pattern checking the CSP authenticates the users and the request is forwarded to cloud registry for confirmation. To predict cost implications the request is being sent to cloud metering by the registry. The registry receives the cost details back from the metering unit and forwarded to the service provider. Service provider checks with the billing section to determine the total cost to be payable. Once the amount details are checked by SP then invoice or bill amount is forwarded to the verified user. The authorised user returns the payment details to SP and SP in turn sends to the bank. Bank send acknowledgement to the service provider and payment confirmation to registry. Finally, the registry authorises the transaction and service is offered to the verified user

IV. RESULTS AND DISCUSSION

This section represents the result analysis for the proposed method for estimating the data document of file transformation effectiveness and protection. The PAUIDS works on data owner and as well as cloud user side. The design does not have any loyalty with cloud storage server and its work separately for protecting user identity during data contribution and retrieval in cloud storage server environment. It performs following estimation attributes like encryption time and decryption time. Here the proposed scheme PAUIDS is analyzed by taking the traditional data integrity algorithms such as Merkle Patricia Tree (MPT) and Merkle Hellman Algorithm (MHA).

A. Encryption Time (ET)

The proposed method derives a mathematical calculation for encryption time which is given in equation 1. The proposed method access data document or file M, the public key PK, with set of features I as input. It performs the encoded document or file CC with the following manner.

$$CC = \left(I, CC\{\mathrm{CC_i}\}i\varepsilon\mathrm{I}\right) \quad (3)$$

Where ˜CC = MYs, CCi = Asi , and s is selected randomly from the feature.

B. Decryption Time (DT)

The proposed methodology exhibits the decryption time in mathematical representation which is shown in equation 4. The methodology receives a cipher input document or file CC encoded under the feature set I.

The cloud client's secret key SK for access tree A, and the public key PK. It expresses the decryption process in following way.

$$CC(\mathrm{CCi}, \mathrm{ski}) = CC(g, g)^{\mathrm{pi}(0)\mathrm{s}} \quad (4)$$

Where CC = Cipher Content and SKi = cloud client secret key element of feature I for leaf hubs. After that the pair outcome is integrated in sequential order. Lastly, it improves the sightless feature Y s = CC (g, g)ys and gives the data document or file content C if and only if I satisfy A.

Table 1 gives the encryption and decryption time of proposed PAUIDS method along with their traditional MPT and MHA methods. The PAUIDS method is investigated in terms of time of encryption and decryption (in sec) and displays their respective feature with the average values along with data files types such as document, text and PDF.

Table.1 Encryption Time (ET), Decryption Time for Text, Document and PDF data types

Learning Algorithm	Text		Document		PDF	
	ET	DT	ET	DT	ET	DT
MPT	0.23	0.36	0.27	0.37	0.65	0.68
MHA	0.18	0.31	0.22	0.32	0.52	0.51
PAUIDS	0.12	0.17	0.13	0.18	0.27	0.29

Based on Table 1, the time taken for encryption and decryption process for both proposed PAUIDS and existing MPT and MHA schemes are considered, from the result the proposed PAUIDS consumes less timing and it proves to be best approach for overall data file types along with respective features. Behalf of Encryption Time (ET) and Decryption Time (DT), it noticed proposed PAUIDS method nearest challenger was MHA. However, outcome of MHA is little far comparing to the proposed PAUIDS. Proposed scheme decreases encryption time of 0.14 seconds and decryption time of 0.17 seconds. Therefore, the proposed PAUIDS proves as best methodology on overall data files and features respectively.

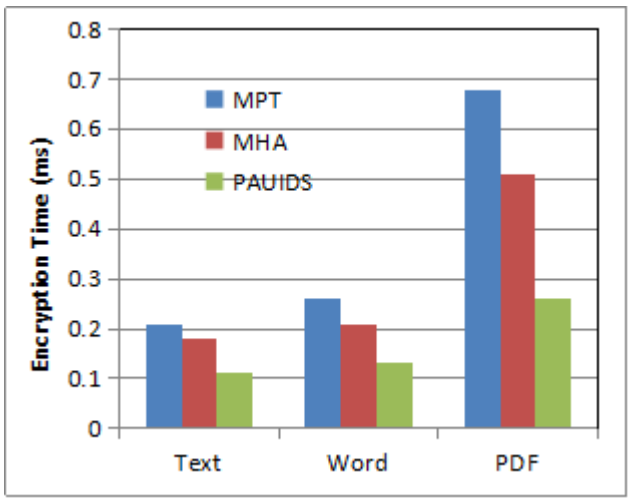

Figure 3: Encryption Time for MPT, MHA & PAUIDS Schemes

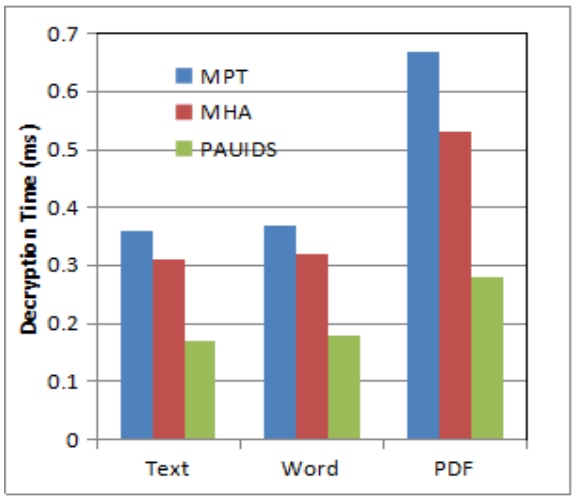

Figure 4: Decryption time for MPT, MHA & PAUIDS Schemes

- **AES Prediction**

Compared to AES the RSA security model gives better results in terms of protecting user identities. The number of users and the number of generations of OTP's gets matched eventually while downloading the files using RSA pattern. However, the number of users and the matching OTP's while using AES seems to be not much efficient for our proposed protocol. Figure 4 shows the AES process for downloading file prediction.

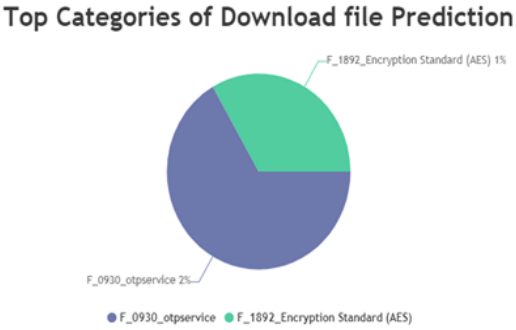

Figure 5: AES for Download file prediction

V. CONCLUSION

User Identification is an entity to detect the user who using the system or website. To prevent the data and to preserve the user from the malignant cloud operators who have chances to reach the sensitive data, here the PAUIDS scheme is proposed. This work mainly focuses on client identity and secure data storage which is always been a significant feature of quality of service. To guarantee the 'rightness of users' information in the cloud storage system PAUIDS algorithm is proposed that separates the document and independently stores the user information in the cloud storage servers. The results are shown and proved that the proposed algorithm reduces the encryption and decryption time in a cloud storage system and also provides secure and efficient data storage in cloud environments.

REFERENCES

1. Wang, C., Cao, N., Ren, K., & Lou, W., 2012, 'Enabling secure and efficient ranked keyword search over outsourced cloud data', IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467-1479.
2. Nazir M., & Rashid M.S., 2013, 'Security Threats with Associated Mitigation Techniques in Cloud Computing', International Journal of Applied Information Systems, vol.5, no.7, pp. 16-28.
3. Huiqi Xu, Shumin Guo, Keke Chen, 2014, 'Building Confidential and Efficient Query Services in The Cloud with Rasp Data Perturbation', IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 2, pp.1-18.
4. Srujana, M., Narayana, S. S., Divya, Y., & Girvani, M., 2013, 'Reliable Proxy Re-encryption in Unreliable Clouds', International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, pp. 746-750.
5. Karthick, K., Jennifer, P., & Muthukumaravel, A., 2014, 'Ensuring Distributed Accountability for Data Sharing in Cloud', Middle-East Journal of Scientific Research, vol. 20, no.6, pp. 702-704.
6. Manjeera Patil,A. Suresh Babu, 2013, 'HABSE: A Hierarchical Attribute-Based Solution For Flexible And Scalable Access Control in Cloud Computing', International Journal of Electrical, Electronics and Computer Systems (IJEECS), vol. 1, no. 3, pp. 2347-2812.
7. Liu Y., Wu H.L., & Chang, C.C., 2014, 'A Fast and Secure Scheme for Data Outsourcing in the Cloud', TIIS, vol.8, no.8, pp. 2708-2722.
8. D. Divya, A. Karthikeyan, G. Panneerselvam and D. Priya, "A maximum powerpoint tracking using perturb and observation algorithm by LABVIEW and arduino," 2014 International Conference on Science Engineering and Management Research (ICSEMR), 2014, pp. 1-4, doi: 10.1109/ICSEMR.2014.7043623.
9. Chhetri, M. B., Vo, Q. B., & Kowalczyk, R., 2012, 'Policy-based automation of SLA establishment for cloud computing services', 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 164-171.
10. Dastjerdi, A. V., & Buyya, R., 2012, 'An autonomous reliability-aware negotiation strategy for cloud computing environments', 12th IEEE/ACM International Symposium on Cloud and Grid Computing (CCGrid), pp. 284-291.
11. D. Divya, A. Karthikeyan and G. Panneerselvam, "Fault indulgent in embedded memory using WCET real-time embedded system," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-6, doi: 10.1109/ICICES.2014.703415.
12. Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, & Ivona Brandic, 2009, 'Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Comuting as the 5th Utility', Future Generation Computer Systems, vol. 25, pp. 599-616.
13. Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.
14. Venkatakotireddy, G., Rao, B. T., & Vurukonda, N. (2018). A Review on Security Issue in Security Model of Cloud Computing Environment. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 207-212). Springer, Singapore.
15. Kumar, P. S., & Rao, B. T. (2016). AN EFFICIENT CLOUD BASED KEY AGGREGATE DATA SHARING. Journal of Theoretical & Applied Information Technology, 83(3).
16. Karthikeyan A, Kuppusamy PG, Amiri IS (2020) Secured identity-based cryptosystem approach for intelligent routing protocol in VANET. Scalable Comput Practice Exp 21(1):41–46.

AUTHORS PROFILE

Mr. R. Rajan, who has been Pursuing PHD in the department of Information Technology at Sankara University (Enathur) during 2014. Basically, his foundation is to complete Diploma in Electronics and Communication Engg from Bhakthavatchalam Polytechnic, Directorate of Technical Education, 2003 with first class and then had been completed B-Tech Information Technology from Karpaga Vinayaga College of Engg and Technology, Anna University, 2007 with first class. He had been completed MTech Information Technology from Sathyabama University, 2012 with first class. He had been working various engineering colleges in Kanchipuram district. He has been around more than 10 years' experience in teaching profession. He is more interests in research and technological field. His interest is in the formation of networking, network security, cryptography, big data analytics, cloud computing and etc. He has been attended international conference and done publications.

Dr. C. Sunitha Ram, has been completed PHD for the Department of computer science and engineering in the year of 2017. she has more than 10 years' experience in teaching profession. She is an Assistant professor of SCSVMV university in the department of Computer science and engineering. She has more theoretical and practical experience in teaching profession. She has more than 10 years' experience in teaching profession. Her teaching interest in Principles of compiler design, Computer architecture, System software, Database Management Systems (DBMSs), and Neural Networks. Her area of interest lies in pattern recognition, Compiler design, Signal processing domain. Her area of specialization lies in Computer intelligence domain. She has been attended various international conferences and done publications.