International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Merkel Tree Oriented Key Management Approach in Cloud Computing

Prajyot Sanjay Katkhede[1], Mr. Rishi Kushwah [2], Dr. Sudeesh Chouhan[3]
[1]Research Scholar, SSSUTMS, SEHORE, M.P.
[2]Assistant Professor, SSSUTMS, SEHORE, M.P.
[3]Assistant Professor, SSSUTMS, SEHORE, M.P.

Abstract-Many enterprises store and manage data in the cloud for various purposes. The transfer of user data in the cloud is no longer secure due to the cycle of data integrity checks. This work presents the development of Merkle Hash Tree for efficient pattern recognition in multi-server cloud to enhance cloud data security. Merkle hash trees use leaf hubs with hash tags and non-leaf hubs with sub-hash stores to hash large amounts of data. Merkle's hash tree provides a useful data organization and describes the history of real data through good design. A proposed method allows you to securely open secure and safe cloud storage systems. Data is sent from the host to the cloud and processed using private keys. Data is stored on the cloud server using the improved Merkle hash tree method. Data files provided by data owners are reviewed by external auditors and by customers using multi-ownership agreements when changes are made. Authorities reviewing data usage are successful in using additional data while addressing security concerns. Profile authentication plays a key role in the ability to evaluate advanced content and prevent tampering by internal or external adversaries.

Keywords: Adaptability, Key Management, Cloud Authentication, Blockchain, Cloud Service.

1. Introduction

Many organizations have used cloud computing to store and manage information effectively, and it is being utilized by all organizations because cloud computing has the advantages of flexibility, adaptability, and stability. Cloud management is the best choice for businesses due to its ease and flexibility (Aldeen, 2019). People use it to store and work with data due to the flexibility and elasticity of the cloud. Customers can choose to encrypt data before sending it to the cloud, and the Cloud Service Provider (CSP) is responsible for ensuring the security of sensitive data. Large, medium, and small businesses use cloud computing to provide virtual computing as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). You can access the service. As more and more specific developments emerge, it is often a good idea to deploy cloud servers for capacity and computation. The cloud is a popular choice for computing due to its services, low cost, and energy-efficient features. Cloud computing frameworks prioritize security, and the need to update existing security decisions drives the development of new solutions. Client access control security is one of the most persistent security issues in the cloud. Public authentication is the process of hiring a trusted third-party administrator (TPA) to verify your cloud profile and reduce the burden on your customers. However, the TPA may have inappropriate access to sensitive information during the authentication process.

In simple authentication, the receiver uses a matching key to match the key, and the sender writes the encrypted message himself. As part of our research, we are using strong encryption techniques for cloud authentication. OTP-based authentication, authentication schemes and cryptographic computations, authentication based on multiple variables, and unknown hub identity are examples of different types of cloud authentication technologies. Cloud-based attacks often result in the loss of personal information that customers and financial institutions care about. An important aspect of climate control is security. Data trust technology can be used to identify relevant data in the cloud and store previous versions. The cloud should support tracking until encrypted data is decrypted and customer data is safely recovered. Another important aspect of irregular language is appearance. Therefore, there should be a good cloud-based way to manage security, trust, and search encrypted data. This study demonstrates the use of modified Merkle hash tree techniques and multi-agent authentication to retrieve data from the cloud. Assessing the reliability of important information in the cloud using the continuous Merkle hash tree method. Each node in the Merkle hash tree contains information about its location relative to the parent node. In order to cope with the increasing demand for information. Although data analysis has some advantages such as being cheap, fast, flexible, and useful, it also has disadvantages that consumers do not see. To allow

remote storage, it is necessary to have the authority to receive information from external capacity. Since the management of external capacity will not be as careful as the data owner, data loss or corruption may occur. Information leaks and errors can lead to significant financial losses and failed enterprises. This may be due to various reasons, such as poor asset management, irresponsible management, and poor project selection.

However, some places with special capabilities will try to cover the losses by cooperating to protect their reputation. Considering the problem of data recovery, there has been an increased reliance on the method of verifying and completing the accuracy of data stored in remote locations using various techniques available for data processing. Merkle trees are unique data that can be analyzed. Analytical techniques are used to verify the accuracy of data based on Merkle trees. The priest gives a series of significant paths from the leaf hubs (randomly selected by the priest) to the root hub of the tree. Once the verifier can recover any support from the root of the tree, the prover must build the entire Merkle tree for the proof. Finally, this method only requires the verifier to use the entire data block to generate the certificate and the verifier to store and process a small number of results. Merkle tree-based authentication is widely used in many frameworks, including blockchain developments such as Bitcoin, due to its simplicity and low memory. Efficiency increases, especially as the amount of data that needs to be analyzed increases. In extreme cases, if this method is used only to verify ownership, an overseer who collects credentials can take ownership of unauthorized files on remote storage. To mitigate this risk, we examine the potential of Merkle tree-based web authentication. Once the age of the evidence is complete as a meta-analysis, we present another table based on the Merkle tree that contains the source of the instability. This eliminates the data leaks we see and provides reliable web-based authentication.

2. Literature Review

This section examines the massive and late investigation strategies for cloud information capacity authentication. To support the proposed idea, a brief analysis of the key assumptions and major gaps in the current writing is presented.

Shajina et al. introduced dual authorization rules with two levels of authorization and priority- based access control lists to increase cloud security and adaptability. We worked on cloud security by adopting triple DES calculation as an additional function according to customer's individuality. This security-focused approach protects her customer's identity, and multiple scenarios were used to test the proposed multi-owner cloud her solution (Doshi, 2011). According to the evaluation, the proposed solution has short network time and high cloud security. The method created enables secure and effective integration of information into separate cloud archives. However, the created techniques perform poorly on huge datasets and offer fuzzy information exchange as a compromise.

Anand et al. Elliptic Curve Digital Signature Algorithm (ECDSA) and Extended Elliptic Curve Duffier-Hellman (EECDH) techniques were recommended for joint authentication in the multi-operator cloud. The proposed EECDH technique was used to exchange protected keys with their owners and thwart man-in-the-middle (MITM) attacks. The proposed approach ensures the accuracy of cloud-based data. The effectiveness of this method is enhanced by a character- and feature-based recording approach. In fact, the cloud computing frameworks created have weaknesses, especially in networks that host third-party layers and complex underpinnings.

Profund et al. Enhanced security with cloud-based secure authentication using blockchain technology. Blockchain technology makes it easy for insiders to change their login credentials for authentication cycles. We evaluated the effectiveness and usefulness of the method in the cloud. Using Scyther's formal framework, the proposed method was tested against no-response attacks, disconnected guesses, pantomimes, and denial of service. The results show how successful the proposed approach was in protecting customer data stored in the cloud. Open cloud computing platforms used in engineered authentication mechanisms have been subject to phishing and social engineering scams. Model sanity checks didn't work well because the encryption of the material was unstructured.

Badr et al. introduced an attribute-based cryptographic approach that accesses information in the cloud by considering permissions, cloud servers, information clients, and information owners. The decryption system was chosen by the information owner to reduce computational complexity. A MAC passphrase for data stored in the

cloud was created after encryption. Encryption used a distinctive function, decryption required verification. To estimate how well the proposed method can be demonstrated, For key age, the elliptic bend testament free cryptography technique was used. This tactic eliminates the trusted authority and focuses on numerical actions to increase security. When the strategy's security was examined, it became clear that the method was secure. In comparison to current methods, the suggested strategy lowers computational and correspondence costs. Multi-client admission to securely cloud information is anticipated to benefit from further development.

3. Merkle Tree-Based Authentication

A Merkle tree is created from a succession of information blocks, with the value of an inner hub devalued in comparison to the hash value of its offspring and the value of a leaf hub devalued in comparison to the immediate hash value of the next information block (Figure 1). The preimage-obstruction property of the hash capability in the tree growth methodology means it is computationally impossible to locate the preimage of the given hash esteem. Additionally, because this forms a double tree, the highest depth from leaf to root is often dlog2 ne for n information blocks (Greene, 2019). The Merkle tree serves as a verified information structure for successful verification of the web-based material as a result. There are two components, prover P and verifier V, in Merkle tree-based web-based authentication:

• A proponent P is an element that tries to convince the opposite side (the verifier V) that the information is all that is claimed to be true. Instead of sending the complete substance, the prover sends a small portion of obvious data to increase network transmission capacity.

• Verifier V is a further component that seeks to determine whether prover P's argument is sound or not. The verifier typically only maintains the value of the root hub rather than the value of each hub in the Merkle tree in order to save storage requirements.

It is remarkable that the Merkle tree-based web-based authentication standard validates that the prover and verifier possess equivalent data. As a result, it acknowledges that the verifier may have some confidential (i.e., not publicly available) information about the information that needs to be validated, in contrast to public check. Section 5 handles this subject in great detail.

It is generally guaranteed that key elements with similar information can obtain a similar Merkle tree due to the hardness hypothesis that it is computationally impractical to locate a preimage of a particular hash value in a reasonable amount of time. Simply put, the security of the hash capability being utilised determines the authentication security in the context of the Merkle tree. By doing this, the verifier V just keeps track of the value of the tree's root hub and discards the remaining metadata when the tree is created. However, with each authentication cycle, the prover P is required to produce a series of (different) hash values that result in a root hub value that is identical to the one maintained by the verifier.

The verifier V in the model shown in Figure 1 selects an odd block record (like 1) as a test. The prover P then creates a Merkle tree using the information in the immediate area, followed by delivering the verifier the comparing remarkable kin routes from the passes on to the root hub (i.e., (H1, H2, H34)). The verifier V determines whether the result is indistinguishable from the value of the root hub stored in adjacent capacity after receiving the confirmation reaction and inferring the root worth of the Merkle tree (i.e., H (H (H1, H2), and H3-4)).

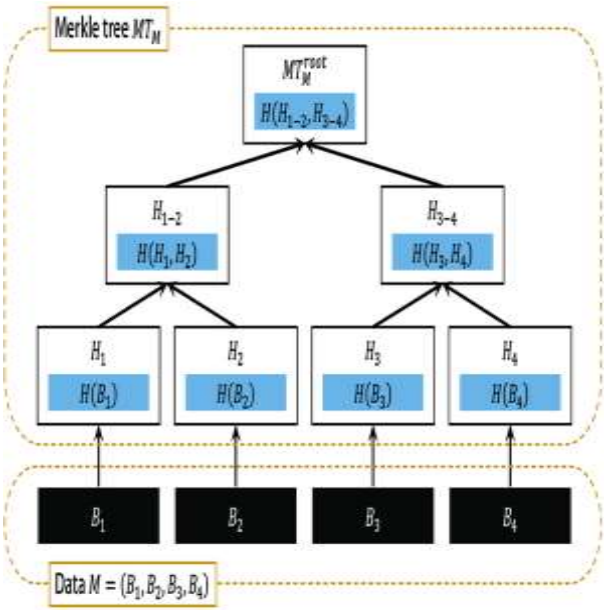


Figure: 1. M Merkle Tree has four blocks of data

As long as a strong (preimage safe) hash capability is used, opponents won't be able to decipher the correspondence's hidden plain information according to the aforementioned convention. In any case, it was found to be vulnerable to side-channel attacks that limit the attack vector by extracting important data from the communication during the authentication cycle, reducing the robustness of the authentication and potentially subverting it. As a result, in Section 3 we first look at how vulnerable Merkle tree-based authentication is to side-channel attacks on data that is similar. Following that, we propose a clear plan for enhancing the security and dependability of Merkle tree-based authentication with negligible above.

4. Motivation

Patients could use a variety of encoding techniques to further restrict who has access to medical services, making it possible for everyone to understand the patient's more obvious attributes while keeping their more subtle ones hidden. Using CP-ABE, either the entire access strategy with ascribes or just the portion of the strategy that needs to be concealed can be scrambled. In any case, because supported end-clients can access the code text, The framework can't tell whether the end-client has enough permission to access it or not. The previous decoding described cannot be utilised again, which is the second disadvantage of this method. Finally, if the approaches are fully or partially disguised, CPABE encryption alone won't protect the system. In a medical setting where information may be shared across many places, it is essential to make it patient-driven. It might be done by utilising CPABE's fine-grained admittance control and covering the access strategy property at several layers.

Contributions

Because of the first finding, this focus fundamentally helps develop a Merkle Tree-based admission strategy for delicate attributes in persistently driven information. In our approach, the health credits associated with the information owner (patient) are identified and organized based on kindness and responsiveness. The unimportant, visible highlights contribute right away to the development of a plan. To the free technique, however, is added the root hash of delicate qualities. The code text is only accessible to authorised users, and the security of the sensitive characteristics is maintained.

Building the CPABE's suggested Merkle Tree-based Access Structure

By identifying delicate data characteristics over the general access strategy, the underlying goal of our methodology is to provide a Merkle tree-based admission structure for describing access control strategies for patient-centric information. All partners or attributes that have granted access to the PCD are recorded in the entrance tree.

The System Model

A proposed Merkle tree-based access structure, including confidential attributes such as leaf nodes and public credits in tree TNS, is shown in Figure 1 for the tree TS confidential access approach. The hash root H(TS) of the tree is found and added to the public non-secret tree TNS before sending it to the decrypt or.

Five algorithms are included in our suggested system:

Setup (γ, S) → (PK,MK)

Based on input from and S, the KGC generates PK and MK, respectively.

Key Gen (PK, MK, S) → SK

KGC creates SK for M. PK, MK, and S.

Merkle Tree (TS) Construction of Attributes Sensitive

The Merkle Tree of Sensitive Traits is built with the IBM Clinical Hub in mind. The IBM Clinical Hub provides clinical information items that enable competence, development and access to longitudinal patient records when linked to persistent personality data. IBM Clinical

Hub provides a more complete workbench model that includes access to patient socioeconomics, clinical information views, and consumption frames and cycles. Longitudinal medical records are produced from his flood of HL7 messages and events related to patient visits, lab orders, results and initiations, clearance and relocation events in a variety of demanding mobile environments. The longitudinal patient record includes information on the patient's prescription, sensitivities, test discoveries, problems, systems, and family history, to name a few things.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Encryption (PK, TNS, TS, M) CT

From the input PK, TNS, TS, and M, TS is the sensitive hash tree, TNS is the public non- sensitive tree, and the sender constructs CT.

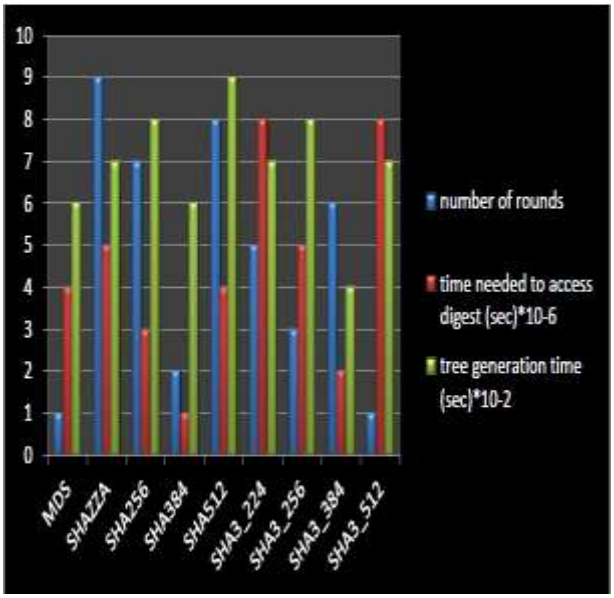
Decryption (CT, SK) M

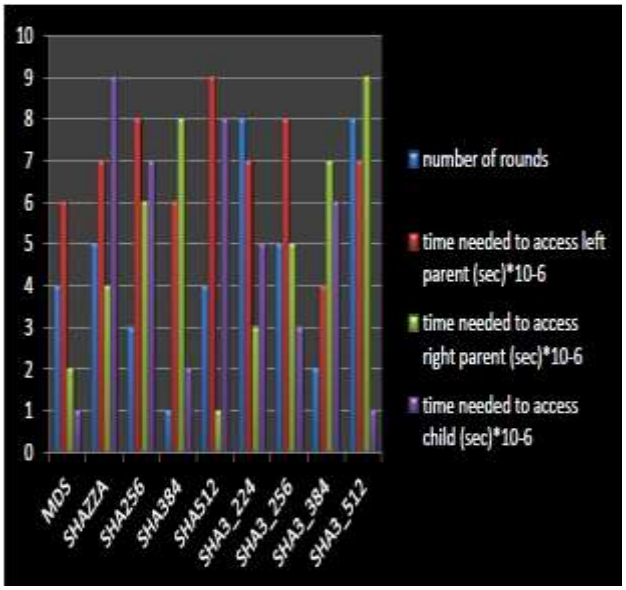
The Collector, given data sources SK and CT, decodes and produces messages CT and M separately. A Merkle proof can show that a certain quality is available by climbing the hash tree TS from the exchange to the root. During the decryption process, the TNS public tree is verified and Merkle proofs are found, allowing the TS to carefully assess the authenticity of the message based on hidden credits.

5. Results and Discussion

Table: 1. Results

S. No.	Number of Leaf Nodes	Number of Iterations	Leaves Size In Bytes	Internal Nodes' Size (Bytes)
1.	35	36	1255	1565
2.	80	36	4050	5309
3.	156	36	8350	22707





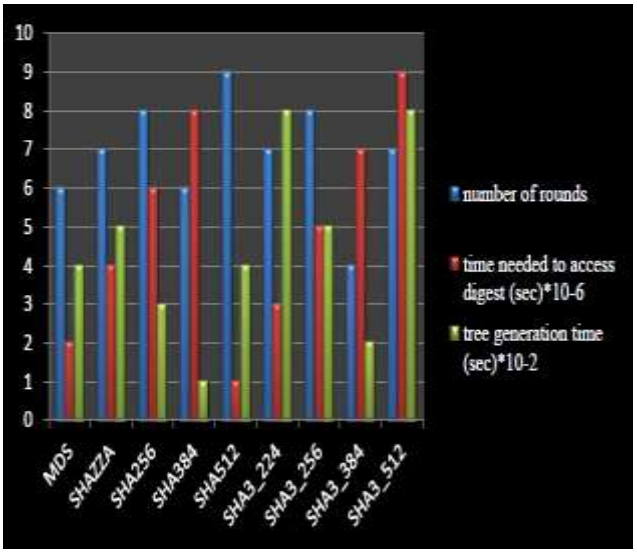


Figure: 2, 3, and 4 The hash calculations are plotted against the times needed to recover the condensate and build the tree in Figures 2, 3, and 4. The third, fifth, and seventh figures are required to reach the child, the right parent, and the left parent, respectively.

5.1. Comparison with different frameworks

In light of the findings in the aforementioned results, we provide a complete correlation that takes into account strategy kind, tree building time, protection safeguarding, information honesty, fine-grained admittance control, and travel time to hubs. We compare the suggested Merkle Tree-based worldview with other novel approaches. Our suggested CP-ABE plot is suitable for carrying out

covered touchy trait access procedures since it creates a Merkle tree, ensures trustworthiness using a hashing strategy, and provides fine-grained admittance control.

Policy Type	Efficiency	Privacy-Preserving	Tree Generation Time	Data Integrity	Time To Access Nodes	Fine-Grained Access Control
conceals sensitive and public access	Low	Y	Moderate	Y	Moderate	Y
No Secret Rules	Low	Y	Moderate	N	Moderate	Y
Only conceals delicate characteristic s	Moderate	Y	Less	Y	Less	Y

Table: 2. The proposed model is compared to existing frameworks

6. Conclusion

Weather forecaster has become a standard in computer management due to its high performance and large capacity. This paper presents a new identity system to enhance the security of cloud data potential. Use multiple authentication methods and improve Merkle hash trees to protect cloud data. Customer data is encrypted using a modified Merkle hash tree algorithm calculated and stored in the cloud (Goyal, 2016). Use peer-to-peer functionality to retrieve information in response to requests. In multi-party weather analysis methods, a discussion is created on the comparison and use of various weather potential analysis methods. This paper introduces the CP-ABE framework based on Merkle trees. It also gives clients a sense of trust and security to cooperate in treatment and counseling. Our approach allows shared projects to use the same strategy and is not easy to be attacked if an attacker has more than one secret key. Finally, we show how our framework can be applied to other types of hashes. The security of our architecture should be taught using static data etc. Work has begun on coding more information and creating the Merkle proof and is expected to be available soon.

7. References

1. Aldeen, Y. and Salleh, M., Techniques for Privacy-Preserving Data Publication in the Cloud for Smart City Applications. Smart Cities Cyber security and Privacy, (2019) 129-145.

2. D. He, C. Chen, J. Bu, S. Chan, Y. Zhang, and M. Guizani, “Secure service provision in smart grid communications,” IEEE Commun. Mag., vol. 50, no. 8, pp. 53–61, Aug. 2012.

3. Doshi, N. and Jinwala, D. Constant Cipher text Length in Multi-Authority Cipher text Policy Attribute Based Encryption. 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011),

4. Goyal, V., Pandey, O., Sahai, A. and Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security - CCS '06, (2006).

5. Greene, E., Proctor, P. and Kotz, D. Secure sharing of mHealth data streams through cryptographically-enforced access control. Smart Health, 12 (2019) 49-65.

6. H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, “Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data,” IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484–494, 2017.

7. H. Liang, B. Choi, A. Abdrabou, W. Zhuang, and X. Shen, “Decentralized economic dispatch in microgrids via heterogeneous wireless networks,” IEEE J. Sel. Areas Commun., vol. 30, no. 6, pp. 1061–1074, Jul. 2012.

8. H. Liang, B. Choi, W. Zhuang, and X. Shen, "Towards optimal energy store-carry-and-deliver for PHEVs via V2G system," in Proc. IEEE INFOCOM, 2012, pp. 1674–1682.

9. Helil, N. and Rahman, K. CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy. Security and Communication Networks, (2017) 1-13.

10. M. Abdel-Basset, M. Mohamed and V. Chang, "NMCDA: A framework for evaluating cloud computing services," Future Generation Computer Systems, vol. 86, pp. 12–29, 2018.

11. Meng, F., Cheng, L. and Wang, M. ABDKS: Attribute-Based Encryption with Dynamic Keyword Search in Fog Computing. Frontiers of Computer Science, 15(5) (2021).

12. Meng, F., et.al. Ciphertext-Policy Attribute-Based Encryption with Hidden Sensitive Policy from Keyword Search Techniques in Smart City. EURASIP Journal on Wireless Communications and Networking, 1 (2021).

13. Nishide, T., Yoneyama, K. and Ohta, K. Attribute-based encryption with partially hidden encryptor-specified access structures | Proceedings of the 6th international conference on Applied cryptography and network security, (2022).

14. R. Deng, J. Chen, X. Cao, Y. Zhang, S. Maharjan, and S. Gjessing, "Sensing-performance tradeoff in cognitive radio enabled smart grid," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 302–310, Mar. 2013.

15. R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

16. S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar et al., "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," IEEE Access, vol. 5, pp. 25808–25825, 2017.

17. Siti Dhalila Mohd Satar, Mohamad Afendee Mohamed, Masnida Hussin, Zurina Mohd Hanapi and Siti Dhalila Mohd Satar, Cloud based Secure Healthcare Framework by using Enhanced Ciphertext Policy Attribute-Based Encryption Scheme International Journal of Advanced Computer Science and Applications (IJACSA), (2021) 12(6).

18. S. Srivastava and R. Kumar, "Indirect method to measure software quality using CK-OO suite," 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013, pp. 47-51, doi: 10.1109/ISSP.2013.6526872.

19. Ram Kumar, Gunja Varshney , Tourism Crisis Evaluation Using Fuzzy Artificial Neural network, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011

20. Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava, "A Survey Paper on Altered Fingerprint Identification & Classification" International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278– 4209

21. Kumar, R., Singh, J.P., Srivastava, G. (2014). Altered Fingerprint Identification and Classification Using SP Detection and Fuzzy Classification. In:, et al. Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012. Advances in Intelligent Systems and Computing, vol 236. Springer, New Delhi. https://doi.org/10.1007/978-81-322-1602-5_139

22. Gite S.N, Dharmadhikari D.D, Ram Kumar," Educational Decision Making Based On GIS" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-1, April 2012.

23. Ram Kumar, Sarvesh Kumar, Kolte V. S.," A Model for Intrusion Detection Based on Undefined Distance", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1 Issue-5, November 2011

24. V. K. A. Sandor, Y. Lin, X. Li, F. Lin and S. Zhang, "Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage," Journal of Network and Computer Applications, vol. 129, pp. 25–36, 2019

25. X. Li, X. Liang, R. Lu, H. Zhu, X. Lin, and X. Shen, "Securing smart grid: Cyber attacks, countermeasures and challenges," IEEE Common. Mag., vol. 58, no. 8, pp. 38–45, Aug. 2012.