ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: **Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy**

Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy

S. Marisargunam

Associate professor, Department of computer science in Artificial intelligence, International school of Technology and Sciences for women, Rajanagaram, Rajamundry, Andhra Pradesh -533294. sargunam.2010@gmail.com

ABSTRACT

Considering the possible consequences of illegal access, cloud service authentication privacy must be guaranteed. Negative actors might get access to private information without the right authentication procedures, which could result in monetary losses, harm to one's reputation, and legal repercussions. This paper proposed using the advanced encryption standard (AES) algorithm for cloud service authentication to guarantee privacy and alleviate these problems. Providing a safe and effective authentication process that ensures user data privacy is the main goal of this framework. To encrypt user credentials and other authentication-related data before sending it to the cloud service provider, the proposed framework makes use of the AES algorithm. With the use of an encryption key, the data is rendered unintelligible even in the event that it is intercepted. In order to guard against man-in-the-middle attacks and eavesdropping, the authentication system also includes secure key exchange protocols and secure communication routes. Organizations may feel secure and in control of their data stored in the cloud by implementing this cloud service authentication architecture. It provides a strong barrier against breaches of privacy, illegal access, and data breaches. A workable and efficient way to guarantee privacy and safeguard sensitive data is to employ the AES algorithm for cloud service authentication. Through the use of this framework, businesses may take use of cloud computing's advantages while retaining control over their data and lowering the danger of illegal access.

Keywords: AES, Cloud Storage, Self-generated Pseudonyms, Valid Cridentials and Eliminating Privacy Abusers.

1 Introduction

Since cloud computing provides scalable, adaptable, and affordable options for data processing and storing, it has become a crucial component of contemporary IT architecture. However, protecting the security and privacy of this data has grown increasingly important as more sensitive data is processed and kept on the cloud [1, 2] Unauthorized access to cloud services result in serious data breaches that jeopardize corporate and personal information. Strong

authentication procedures are crucial to addressing these security issues. The use of AES-based cloud service authentication to protect data privacy and security is the main topic of this article [3, 4]. Symmetric key encryption algorithms like AES are well known for their power and effectiveness. By integrating it into the authentication procedure, it adds a strong security layer that guarantees that only authorized users are able to access cloud services [5, 6]. Because AES employs key lengths of 128, 192, or 256 bits and operates on fixed block sizes, it is very resistant to cryptographic threats such as brute-force assaults [7, 8]. Cloud services that employ AES for authentication encrypt sensitive data and user credentials, guaranteeing the privacy of such information both during transmission and storage [9, 10].The chance of illegal access and data interception is greatly decreased by this encryption procedure. In cloud environments, where speed and performance are critical, AES is a perfect fit because to its efficiency in both hardware and software implementations [11, 12].

The design and application of AES-based authentication in cloud services are examined in this paper. It draws attention to the benefits of utilizing AES, including improved security, privacy, and adherence to legal requirements. Furthermore, the study addresses possible obstacles such as key management and interaction with current systems and suggests ways to overcome them [13]. By means of an extensive examination, we exhibit how AES might be successfully included into cloud authentication systems to safeguard user information and uphold confidentiality. As data breaches and cyber-attacks become more common, the findings highlight how crucial it is to implement cutting-edge encryption solutions to improve cloud service security. Cloud service providers may empower more trust and compliance in the digital era by providing a more secure and dependable environment for their consumers through the use of AES-based authentication [14, 15].

Establish an Advanced Encryption Standard (AES)-based cloud service authentication mechanism to protect privacy. An effective and safe authentication process that ensures user data privacy. The AES algorithm provides a workable and efficient way to authenticate cloud services while maintaining privacy and safeguarding sensitive data.

2 Recent Works

Srinivas Jangirala et al [2020] have provided details on a novel user authentication system that runs on the cloud and ensures the security of medical data. A secret session key is established by both the wearable sensor node and the user upon successful mutual authentication. This key is used for any future secure connections. The proposed scheme offers session-key security and protects against active attacks, as demonstrated by the widely-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool-based formal security verification and the widely-used Real-Or-Random (ROR) model-based formal security analysis. However, the information shouldn't be disclosed to an enemy because it is sensitive and confidential. In order to retain a secret session key between an

authorized user and an accessible wearable device following their successful mutual authentication with the aid of the CoTC, it is necessary to propose a cloud-based user authentication technique. Their methodology does not take authentication between a wearable device and an outside entity into account.

Bai Liu et al [2023] have unveiled a low-tech, Consortium Blockchain-based smart home data privacy protection plan. To address users' undue reliance on third-party servers and address the issue of smart home device data privacy protection, the solution consists of two modules: message authentication and data integrity audit. Message authentication, on the other hand, made use of a pairing-free certificate-less aggregate signature approach that greatly decreased device-side compute and communication cost and guaranteed data integrity using the Merkle hash tree audit scheme. Furthermore, the unforgeable smart contract uploads the audit findings automatically to the chain, and the security analysis demonstrated that the message authentication mechanism proposed in this scheme satisfies security criteria. On the other hand, smart home gadgets are less secure against malicious assaults, and wireless communications between wireless sensors and data gathering nodes are typically unstable. The gadget has a hard time maintaining its identification as a chain node. Miners must confirm the identification of the device and ensure its anonymity in order to authenticate messages.

Xiangjian Zuo et al [2022] have put out a successful sub graph matching strategy with social network authentication that protects privacy. Under the proposed scheme, users access the cloud service without disclosing their graph information to the Boneh-Goh-Nissim public key encryption technique. The cloud server assists the query user in obtaining the graph data from the data owner and performs sub graph matching operations while maintaining the confidentiality of the graph data. Meanwhile, data integrity verification and user authentication are accomplished by the proposed technique based on the message authentication code. The proposed plan satisfies the security criteria, according to the thorough security study. Moreover, the plan attains minimal processing and correspondence costs for nearby users, rendering it appropriate for several real-world uses. The graph data owner needs a lot of storage capacity to store the graph data because of its high intricacy. Therefore, the data owner's ability to do the aforementioned duties is significantly hampered by the restricted storage capacity. Furthermore, due to a lack of computational capacity, data processing and analysis may present challenges even in cases when the data owners have adequate storage space to hold the graph data.

Manuel Parra-Royon et al [2022] have offered recommendations about the cloud computing semantics of data mining services. With all the benefits of this kind of environment, customers now have access to incredibly extensive data analysis tools to the recent integration of new data mining and machine learning services within cloud computing providers. In addition to publishing definitions and descriptions in a variety of forms, cloud computing service providers

for data mining sometimes do not work well with other providers. It is essential to preserve the functionality of data mining services, particularly their portability and usability, despite variations in hardware, software, and cloud platform support. This may be seen from a functional perspective. Parts of the ML schema have been utilized for the primary portion of the service, which specifies and models the algorithm execution and experimentation. A sufficient abstraction to represent the service is also offered by MEX Core, Onto DM, DMOP, or Expose´, although their language is larger and more intricate.

Ke Huang et al [2022] have provided an explanation of a flexible, bidirectional proof-of-ownership that may be used in both static and dynamic environments to recover data duplication. Particularly, we proposed DAP to arbitrate the file's originality, M-PoW for dynamic archives, and B-PoW for static archives. Both a thorough performance review and a solid security analysis are provided. The data indicates that our B-PoW concept is effective for duplicating vast amounts of data. Our M-PoW, meanwhile, performs well enough in a dynamic environment where data is meant to be outsourced initially and updated in a dynamic data archive thereafter. An affordable way to store large volumes of data is through cloud storage. Cloud service innovations drive data generation, straining storage servers to their breaking point. The majority of modern cloud servers use the widely used deduplication technology, which finds and removes redundant data to conserve bandwidth and storage. However, developing an effective POW for dynamic archives is necessary to meet user demands for dynamic data modification and provide real-time data services. We introduce the concept of bidirectional and malleable proof-of-ownership (BM-PoW) for the aforementioned challenge, which is inspired by the malleable signature, which provides authentication even after its committed message changes.

3 Proposed Work Explanation

The advanced encryption standard (AES) technique is used in this proposed system's cloud service authentication to guarantee privacy. The first step in this procedure is user authentication, during which the user enters credentials such their login and password. Then, in order to be sure that the data cannot be read without the decryption key, these credentials are encrypted using the AES technique.

Using secure communication routes to prevent unwanted access or eavesdropping, the encrypted data is safely sent to the cloud service provider. Between the user and the cloud service provider, a key exchange protocol is used to generate a shared encryption key in order to establish a secure connection.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy

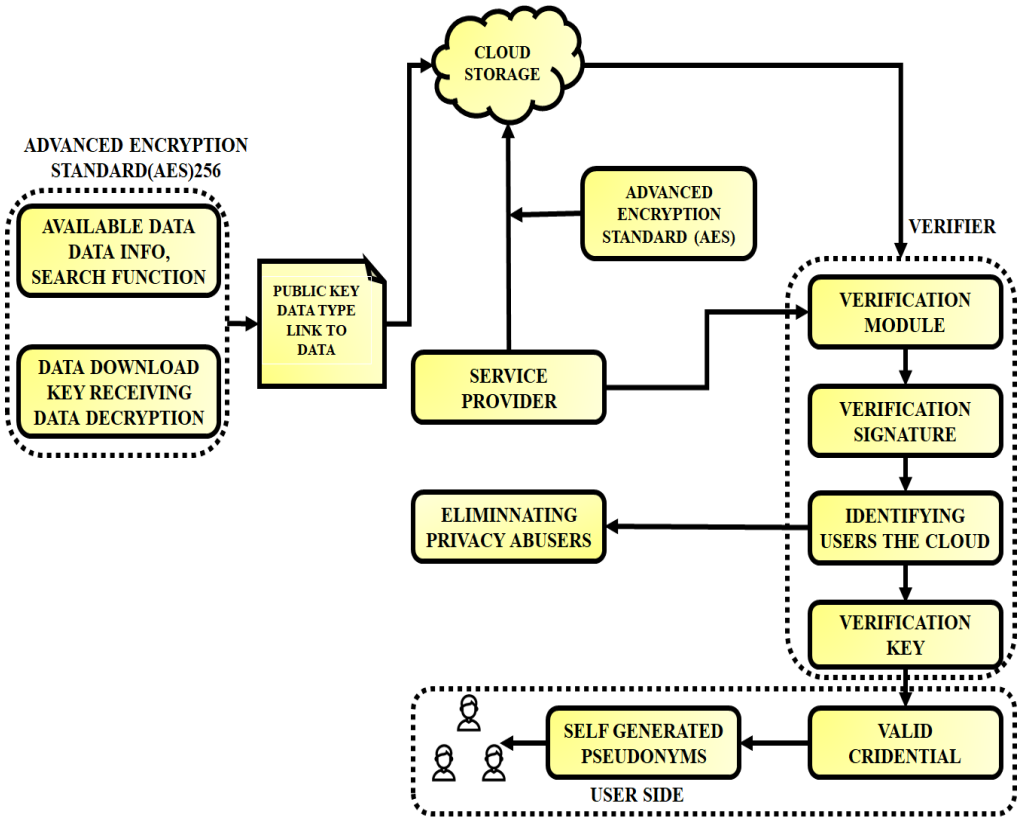


Figure 1: *Proposed block diagram*

To decode the encrypted data, you must have this key. Sensitive data is preserved securely as it enters the cloud storage system, ensuring its safety. Re-authentication is required whenever the user wants to access their data. They safely send their credentials to the cloud service provider, which is encrypted using the same AES method. The supplier then decrypts the user's credentials using the shared encryption key. It is ensured that only authorized persons may access the data by granting access to the user if the decrypted credentials match the stored credentials. Throughout the cloud service authentication system, this operational procedure guarantees the confidentiality and security of critical data.

3.1 Advanced Encryption Standard (AES) 256

The symmetric key encryption method employed by the popular Advanced Encryption Standard (AES) 256 uses a single key for both encryption and decryption. Typically, 128-bit data blocks are used by block ciphers like AES 256, which works with fixed-size data blocks. Because AES 256 employs a 256-bit key for encryption, the "256" in the algorithm stands for the key size. Brute-force assaults are just not feasible with this key size since it provides an extraordinarily vast number of potential combinations. Because it offers a strong defense

against a variety of cryptographic assaults, AES 256 is well known for its strong security characteristics. Its resilience to complex assaults, such as differential and linear cryptanalysis, which are often employed methods to crack cryptographic algorithms, is what gives it its strength.

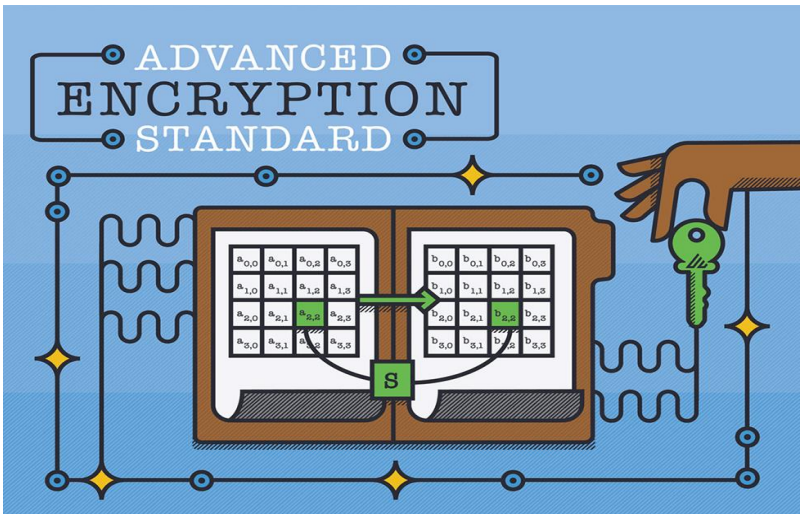


Figure 2: *Advanced Encryption Standard*

Furthermore, because of AES 256's established security and dependability, governments, financial institutions, and security-conscious businesses all around the world have embraced it. Its reliability is shown to by the fact that it is widely used and accepted in a variety of applications, including preserving stored data and safeguarding sensitive data while it is traveling over networks. Even with massive data quantities, AES 256's strong security is matched by its computational efficiency, which enables quick encryption and decryption operations. In the current era of cybersecurity, AES 256 is one of the most reliable and extensively utilized encryption methods to its robust security, effectiveness, and adaptability.

3.2 Cloud Storage

The term "cloud storage" describes the online access to distant servers that house digital data. It provides customers with an easy-to-use and expandable way to save and retrieve their files and data from any location with an internet connection. To ensure data availability and durability, cloud storage companies often keep several copies of their data spread across geographically disparate data centers. One of the main advantages of cloud storage is its scalability and flexibility, which let customers adjust their storage space according to their demands without having to deal with the headaches of maintaining physical hardware. Furthermore, cloud storage services frequently come with features like versioning, data encryption, and collaboration tools, which improve user productivity and data security.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy

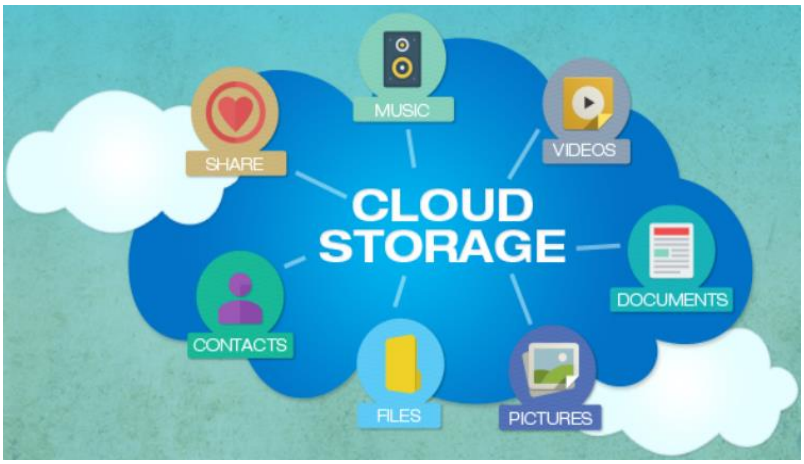


Figure 3: *Cloud Storage*

Additionally, by doing away with the requirement for local storage infrastructure, cloud storage lowers the cost of purchasing, maintaining, and upgrading hardware. Additionally, it offers smooth connection with other cloud-based services and programs, making process automation and effective data management possible. With its dependable and affordable options for managing and storing data, cloud storage has evolved into a vital resource for both consumers and enterprises.

3.3 Verifier

The manner that data is managed, accessed, and kept has been completely transformed by cloud storage. It provides people all around the world with unmatched accessibility, scalability, and ease. But with the quantity of data being kept on the cloud increasing at an exponential rate, it is crucial to guarantee the security and integrity of this data. Here come verifiers, who are essential to preserving the reliability of cloud storage systems. Verifiers serve as the cloud environment's protectors of data integrity. Their main job is to verify the accuracy of data kept in the cloud by comparing it with cryptographic hashes or pre-established checksums. This procedure aids in identifying any illegal changes or corruption that could have happened while the data being sent or stored.

Verifiers use advanced cryptographic methods and algorithms to guarantee the dependability and correctness of their evaluations. Verifiers also play a critical role in upholding adherence to industry best practices and legal requirements. Businesses may show their dedication to data protection and accountability by carrying out frequent integrity checks, which will build confidence with stakeholders, partners, and consumers. Verifiers play a critical role in ensuring the security and integrity of data stored in cloud environments. Strong verification methods will be more and more necessary as cloud computing becomes more and more prevalent in order to provide consumers piece of mind while entrusting their important data to the cloud.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy

3.4 Eliminating Privacy Abusers

By creating an open and responsible framework for cloud data management, cloud verifier technology serves as a potent defense against privacy violations. Cloud verifiers allow users to confirm the validity of their data without disclosing private information to other parties by utilizing cryptographic techniques such as homomorphic encryption and zero-knowledge proofs. This lessens the possibility of data breaches and exploitation in addition to lowering the danger of unwanted access. In addition, cloud verifiers encourage transparency and accountability from cloud service providers by enabling customers to monitor and audit data access, guaranteeing adherence to privacy laws and contractual terms. Through the integration of cloud verifier technology into their infrastructure, enterprises may cultivate trust among their stakeholders and consumers by showcasing their dedication to protecting privacy and maintaining data integrity in an increasingly connected global community.

3.5 Valid Cridentials

Reputable credentials are the foundation of safe access control systems, giving users a way to be verified and have their activities in different online spaces approved. Valid credentials are essential for identity verification and ensuring that only authorized parties may access sensitive data or carry out specified activities, whether they are used in government databases, corporate networks, or online accounts. These credentials usually comprise distinct identifiers, such usernames or email addresses, along with cryptographic keys, passwords, or biometric information as authentication elements. Organizations may reduce the danger of unwanted access and guard against harmful behaviours like identity theft, data breaches, and fraud by requiring users to present legitimate credentials before allowing access. Furthermore, the security and usability of legitimate credentials are being improved by developments in authentication technologies, such as federated identity management and multi-factor authentication. This allows for the easy but reliable implementation of access control methods across a variety of digital ecosystems.

3.6 Self-Generated Pseudonyms

Self-generated pseudonyms are aliases or other identities that people make up for a variety of reasons, such communicating online, protecting their privacy, or expressing themselves artistically. Because these pseudonyms are selected by the users themselves, rather than being assigned by others, they enable people to explore elements of their personalities or adopt identities that they would not feel comfortable revealing under their true names. Self-generated pseudonyms allow people to participate in online forums, social media sites, and creative projects without disclosing their real name. They provide a feeling of independence and anonymity. In online environments, they also act as a kind of defense against discrimination,

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy

unwelcome attention, and harassment. Furthermore, people experiment with multiple identities or compartmentalize different elements of their life under self-generated pseudonyms without worrying about criticism or negative consequences. Self-generated pseudonyms provide people a chance to manage the complexity of digital identification and customize their online presence in a way that feels real and powerful to them, whether they are used for social networking, blogging, or online gaming.

4 Results and Discussion

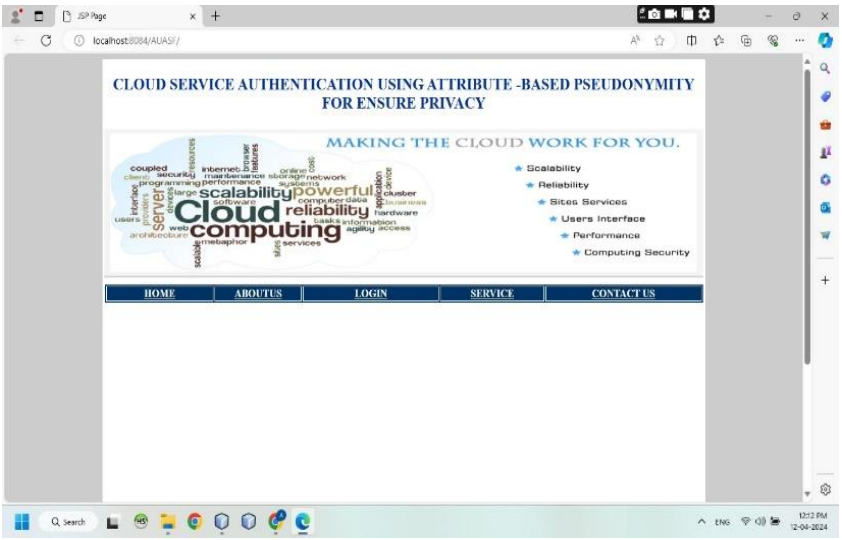


Figure 4: *Home page*

The home page is shown in Figure 4. Links to registration, login, and about are available on this home page.

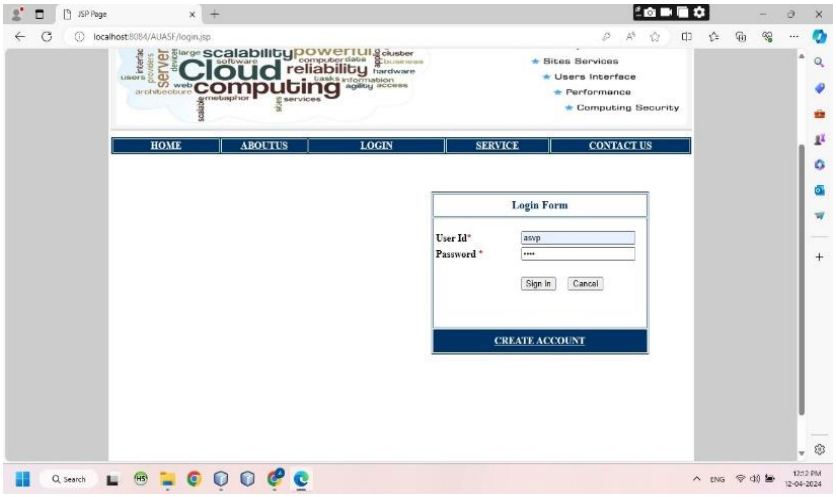


Figure 5: *Login Page*

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

This login screen for the user is shown in Figure 5. It serves as the login for the user's page. When the login page is complete, go to the login form.

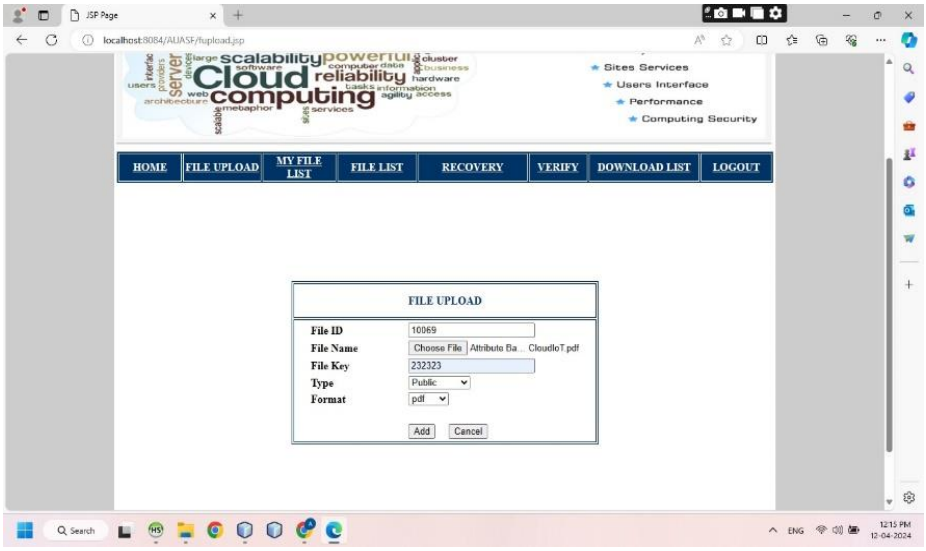


Figure 6: *Files Upload Page*

The files upload page is shown in Figure 6. Enables users to choose and upload files from their devices to a server, simplifying the sharing and storing of documents, images, and other digital information.

Figure 7: *Service Authentication Page*

Figure 7. The Service Authentication Page. A webpage with an account creation form for cloud computing services, techniques for recovering lost passwords, and a login form containing fields for a username and password.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: **Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy**

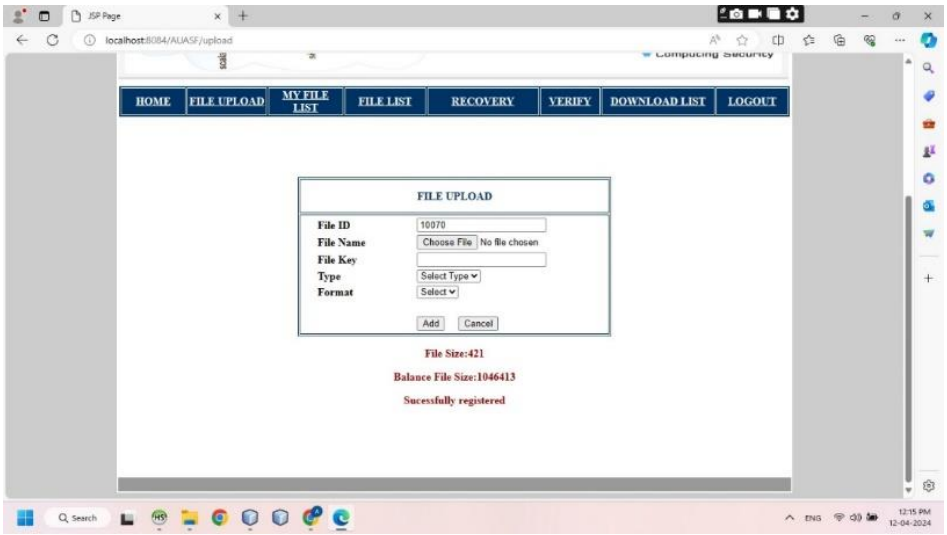


Figure 8: *Registration Page*

The registration page is shown in Figure 8. Officially enrolling someone in a service, event, or organization; usually involves consenting to terms and conditions and supplying personal information. It accomplishes the purpose of recording involvement or membership.

Figure 9: *File List Page*

Figure 9 evaluates my file list page. A list of files and folders is displayed on an interface known as the "My File List Page" for efficient management and organization. This website makes it easy for users to view, modify, and delete files, increasing productivity and giving them greater control over their digital assets.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: **Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy**

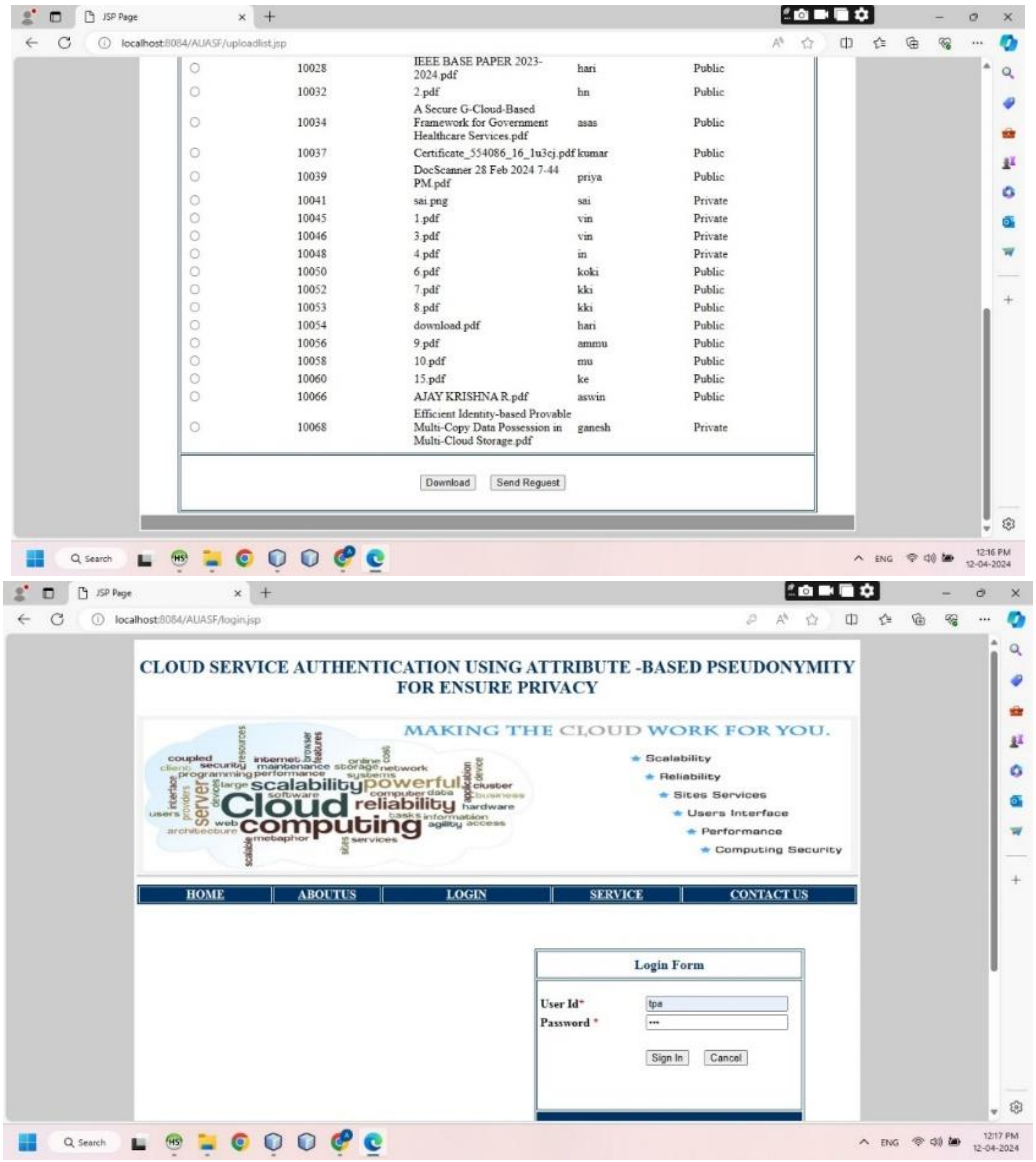


Figure 10: *Login Form Page*

Figure 10 depicts the page where users log in. A login form page is an online interface that users use to access a website's restricted area or service by entering their login credentials, such as their username and password. Authentication fields are often included, and it may additionally have functionality like links for password recovery or account registration.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: **Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy**

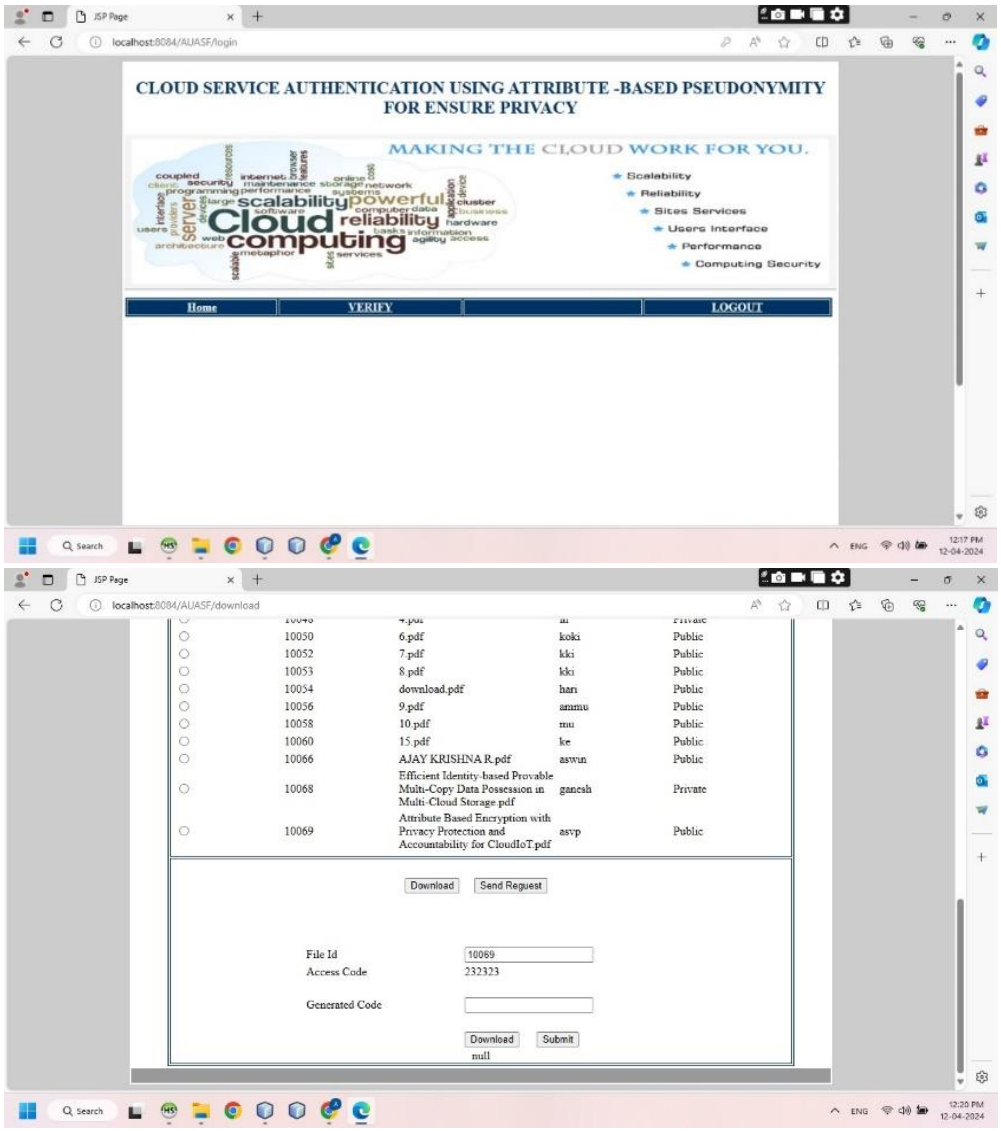


Figure 11: *Service Login Page*

The features and information presented on a website where users must submit their login credentials to safely access a particular online service or platform are described in detail in figure 11. It often has spaces for the password, username, and email in addition to options to create an account or recover forgotten passwords. Through the login page, users may authenticate themselves and gain access to the service's features and capabilities.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: **Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy**

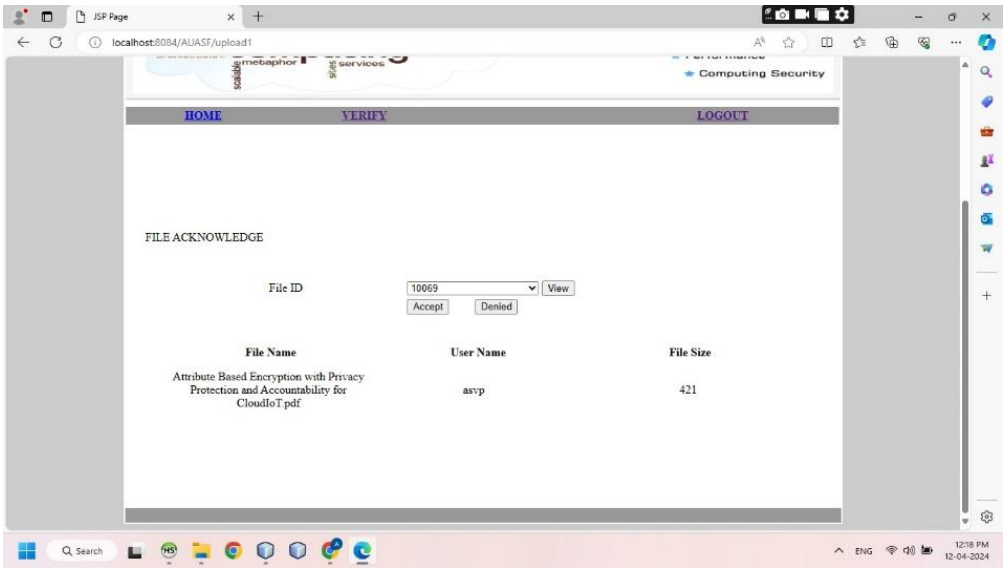
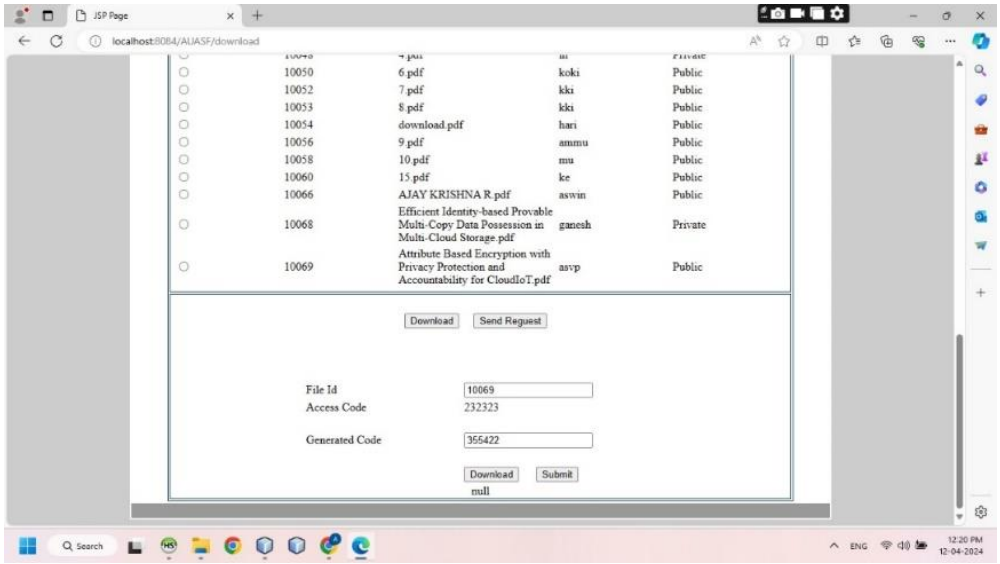


Figure 12: *File Acknowledge Page*

Figure 12 displays the file acknowledgement page. A digital confirmation screen that shows up when an action, such uploading or submitting a file, is successfully completed. The file name, upload time, and a receipt confirmation message are often included. By confirming that their material has been received and processed, this page helps consumers feel confident and clear throughout the engagement.



ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 03(04), APRIL 2024, pp. 14-30

Article Title: **Cloud Service Authentication Based On Advanced Encryption Standard (AES) For Ensure Privacy**

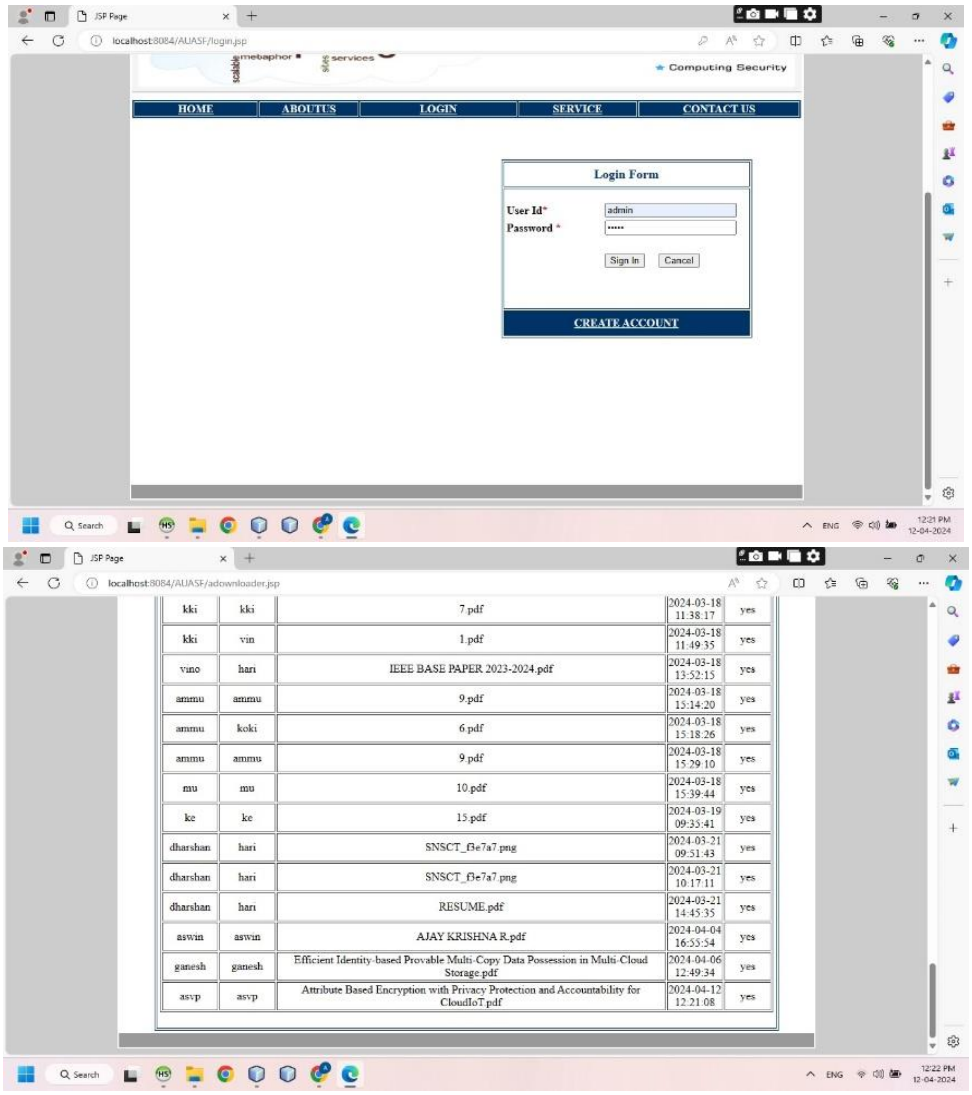


Figure 13: *Document Displaying a List page*

The page where a document displays a list is shown in Figure 13. A description, either written or visual, of several objects organized in a logical or classification order. It facilitates comprehension and readability by effectively arranging and presenting information. To effectively communicate the material, lists formatted using bullet points, numbered items, or other forms.

5 Conclusion

A solution for cloud service authentication that protects privacy using attribute-based pseudonymity has been successfully established in this project. Enabling attribute verification safely, the Java-developed solution combines an AES-256 encryption algorithm with a secret

sharing technique. The Verifier (Authentication Server) is in charge of confirming signatures using an access tree structure, and users who supply legitimate credentials with embedded characteristics and self-generated pseudonyms are its principal constituents. AES-256 is used to produce keys and public values. Because of the way the system is built, users may access and maintain more security and privacy without having to register their credentials with the service provider. To provide effective and dependable authentication for users storing data in the cloud, it also provides fine-grained access control and allows verified attribute delegation. All things considered, this research shows a strong methodology for cloud service authentication, emphasizing security and privacy while utilizing cutting-edge encryption methods.

References

1. Ling Xiong; Fagen Li; Mingxing He; Zhicai Liu; Tu Peng, Year: 2022, "An Efficient Privacy-Aware Authentication Scheme With Hierarchical Access Control for Mobile Cloud Computing Services", in IEEE Transactions on Cloud Computing, Vol: 10, no: 4, pp. 2309-2323.

2. Xu Yang; Xun Yi; Surya Nepal; Ibrahim Khalil; Xinyi Huang; Jian Shen, Year: 2022, "Efficient and Anonymous Authentication for Healthcare Service With Cloud Based WBANs", in IEEE Transactions on Services Computing, Vol: 15, no: 5, pp. 2728-2741.

3. Jangirala Srinivas; Ashok Kumar Das; Neeraj Kumar; Joel JPC Rodrigues, Year: 2020, Rodrigues, "Cloud Centric Authentication for Wearable Healthcare Monitoring System", in IEEE Transactions on Dependable and Secure Computing, Vol: 17, no: 5, pp. 942-956.

4. Jie Cui; Xiaoyu Zhang; Hong Zhong; Jing Zhang; Lu Liu, Year: 2020, "Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment", in IEEE Transactions on Information Forensics and Security, Vol: 15, pp. 1654-1667.

5. Zahid Ghaffar; Shafiq Ahmed; Khalid Mahmood; Sk Hafizul Islam; Mohammad Mehedi Hassan; Giancarlo Fortino, Year: 2020, "An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-Social-Systems", in IEEE Access, Vol: 8, pp. 47144-47160.

6. Gaurang Panchal; Debasis Samanta; Ashok Kumar Das; Neeraj Kumar; Kim-Kwang Raymond Choo, Year: 2022. "Designing Secure and Efficient Biometric-Based Access Mechanism for Cloud Services", in IEEE Transactions on Cloud Computing, Vol: 10, no: 2, pp. 749-761.

7. Azeem AIrshad; Shehzad Ashraf Chaudhry; Osama Ahmad Alomari; Khalid Yahya; Neeraj Kumar, Year: 2021, "A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework", in IEEE Systems Journal, Vol: 15, no: 3, pp. 3664-3672.

8. Adesh Kumari; Vinod Kumar M. Yahya Abbasi; Saru Kumari; Pradeep Chaudhary; Chien-Ming Chen, Year: 2020, "CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC", in IEEE Access, Vol: 8, pp. 107838-107852.

9. Seunghwan Son; Joonyoung Lee; Myeonghyun Kim; Sungjin Yu; Ashok Kumar Das; Youngho Park, Year: 2020, "Design of Secure Authentication Protocol for Cloud-Assisted Tele care Medical Information System Using Blockchain", in IEEE Access, Vol: 8, pp. 192177-192191.

10. Mahender Kumar; Satish Chand, Year: 2021, "A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network", in IEEE Systems Journal, Vol: 15, no: 2, pp. 2779-2786.

11. Bakkiam David Deebak; Fadi Al-Turjman, Year: 2021, "Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things", in IEEE Journal on Selected Areas in Communications, Vol: 39, no: 2, pp. 346-360.

12. Bai Liu; Xueyan Yao; Kuikui Guo; Pengda Zhu, Year: 2023, "Consortium Blockchain Based Lightweight Message Authentication and Auditing in Smart Home", in IEEE Access, Vol: 11, pp. 68473-68485.

13. Xiangjian Zuo; Lixiang Li; Haipeng Peng; Shoushan Luo; Yixian Yang, Year: 2022, "Privacy-Preserving Sub graph Matching Scheme With Authentication in Social Networks", in IEEE Transactions on Cloud Computing, Vol: 10, no: 3, pp. 2038-2049.

14. Xinyu Meng; Lei Zhang; Burong Kang, Year: 2022, "Fast Secure and Anonymous Key Agreement Against Bad Randomness for Cloud Computing", in IEEE Transactions on Cloud Computing, Vol: 10, no: 3, pp. 1819-1830.

15. Jianye Huang; Willy Susilo; Fuchun Guo; Ge Wu; Zhen Zhao; Qiong Huang, Year: 2022,"An Anonymous Authentication System for Pay-As-You-Go Cloud Computing", in IEEE Transactions on Dependable and Secure Computing, Vol: 19, no: 2, pp. 1280-1291.