Review of Data Security and Privacy in Cloud Computing

Tarun Singh H
Student
School of Computer Science and Information Technology
Jain (Deemed-to-be University)
Bangalore, India
23mcar0171@jainuniversity.ac.in

Prerna Mahajan
professor
School of Computer Science And Information Technology
Jain (Deemed-to-be University)
Banglore, India
prerna.m@jainuniversity.ac.in

***Abstract*—Cloud computing, thus, ensure more healthy demand for cloud services, certain measures against threats in order to protect information must be taken. In essence, the current paper seeks to extend knowledge regarding the improvement of paradigms of cloud computing with particular focus on the aspect of certification of authentic users and protection of the contents that are hosted in these environments. It mentions a new approach in the context of the authentication method that was deployed for the purpose of the AAA certification is presented there along with the watermarking and this RSA algorithms to enhance the security of the cloud file-sharing. This concept is far more effective than the conventional access policies that are top down and cal beforehand for systematic risk avoidance; hence, it helps to minimize the chances of an organization being vulnerable to various risks by right management. Iturbide's data loss prevention technique eliminates the probability of losing sensitive information to the rest of the world as well as other unauthorized persons or organizations regaining access to privileged keys while Shamir's secret sharing algorithm- polynomial interpolation ensures that the generation of keys is not a time-consuming exercise. In order to address the issues of persistent security threats in cloud computing paradigm, the proposed model includes computation, encryption and access to improve the overall security of cloud environment. However, these measures have been implemented, some of them can offer the best security when it comes to the ever-evolving threat. To maintain the privacy of clients' data in the CL reinforcement learning, the paper suggests the use of homomorphic encryption for privacy-preserving RL inference. Therefore – as a result of the work – the necessity of implementing the suggested security model for the cloud computing environments as well as protecting the data and enhancing the level of trust in cloud solutions is stated.**

Keywords - QoS (Quality of Service), Energy Efficiency, Ontology, AAA (Authentication, Authorization, and Accounting), RSA Algorithm, RSA Algorithm, ReDCIM (Reconfigurable Digital Computing-In-Memory) Processor, tableopencache, LSTM (Long Short-Term Memory)

I. INTRODUCTION

This paper also contributes an improved procedure in offering discretion in cloud organizations that was also perceived to offer top protection as compared to the method under consideration. This method is directed to enhance the security control of authentication to heels of data security in cloud computing environments. Therefore, in accordance with the overall approach described above, we began the development of less deep authentication approach for AAA certification system and also provided the improved safeguard to work with cloud file-sharing through adopting a watermark and RSA algorithms. Thus, the need to systemically avoid risks makes it possible for businesses to safely implement the proposed key access management strategy rather than resort to the vertical policy model for adopting cloud computing. This is why targeted change of managing the access policies instead of the traditional top-down policy has numerous advantages. This specific scheme could help fixate and protect current important access throughout such transforms, particularly accurately those companies, which have a logically outlined hierarchy. Through the application of Shamir's secret sharing algorithm and polynomial interpolation method, our system ensures that there are fewer cases that which important data will be transferred to the public cloud and managed privileged keys. It also has the advantage of not requiring much space and being technically efficient when it comes to the creation of new keys in this system.

As mentioned above, our system is pointed at collusion attacks that might try to infringe on the Key Indistinguishability security.[1]

This paper also contributes an improved procedure in offering discretion in cloud organizations that was also perceived to offer top protection as compared to the method under consideration. This method is directed to enhance the security control of authentication to heels of data security in cloud computing environments. Therefore, in accordance with the overall approach described above, we began the development of less deep authentication approach for AAA certification system and also provided the improved safeguard to work with cloud file-sharing through adopting a watermark and RSA algorithms. Thus, the need to systemically avoid risks makes it possible for businesses to safely implement the proposed key access management strategy rather than resort to the vertical policy model for adopting cloud computing. This is why targeted change of managing the access policies instead of the traditional top-down policy has numerous advantages. This specific scheme could help fixate and protect current important access throughout such transforms, particularly accurately those companies, which have a logically outlined hierarchy. Through the application of Shamir's secret sharing algorithm and polynomial interpolation method, our system ensures that there are fewer cases that which important data will be transferred to the public cloud and managed privileged keys. It also has the advantage of not requiring much space and being technically efficient

when it comes to the creation of new keys in this system. As mentioned above, our system is pointed at collusion attacks that might try to infringe on the Key Indistinguishability security.[2] Technologically speaking, many companies today have adopted this method of service delivery due to the improvement of technology over the years. These are some of the advantages that come with cloud computation; It is cheap, it can self-claim, and it has access. This however comes at the following cost of the following security threats that cannot be undermined. The above challenges include the protection, control, and authentication of data, file sharing security, and security in the use of mobile clouds. To this end, some solutions and technologies that have been implemented in an attempt to address the aforementioned challenges include. But some prominent solutions are as follows: To ensure better authentication security control, impedance AAA certification mechanisms needs to be adopted; To enhance the security of files shared in the cloud, watermarking and RSA algorithms should be applied; For enhancing the security in controlling and encrypting, access control and encryption techniques must be incorporated and applied and for using trust-based technologies, they should be integrated. Thus, by utilizing such approaches, the researchers can get a clue about the way they operate, the existing strengths as well as the limitations associated with an ML model. But it is also necessary to emphasize that when speaking about cloud security, technological problems are only part of the picture, and one should also mention standardizations and legislation aspects. When controlling the safety factors of cloud and formulating the legal standards, one can create the perfect security protective system to maintain the privacy of cloud computing services, and then advance the Cloud Computing legal construction as well as the sustainable and healthy growth of the Cloud Computing industry (Sun, 2019). Similarly, in the contemporary world, with the evolving big data and restricted central processing and storage, organizations have opted for the Cloud for data storage exchange and analysis.[3]

Cloud computing can be said to be the ticket to delivering AI services since it has direct access to large computation and storage resources. However, the overall course of reinforcement business learning to be applied in cloud computing contains some problems of privacy. This is because services, which follow the implementation of RL dependency, imply the exchange of numerous privacy- associated user data between the user as well as, the cloud computing platform. Regarding the mentioned issue concerning privacy invasion; a solution has been suggested which integrates the application of homomorphic encryption scheme in cloud computing systems. The above said encryption technique enables the cloud computing platform to perform arithmetic operations on cryptic texts and this cannot expose the information of the users. It is seen that by applying homomorphic encryption, only ciphertext is transferred from the user site to the cloud computing platform for RL- based services thus making it unnecessary to transfer 'Sensitive User Data' from one party to the other. The following methodology is thus proposed with the view to creating of the method of the protection of personal data in the context of cloud computing with the help of homomorphic encryption: However, by adopting homomorphic encryption for protection of the users' data in cloud computing infrastructures for privacy-preserving reinforcement learning, the users are relieved of the challenge of privacy that comes with sharing of the private data with cloud computing platform. Furthermore, the study's approach uses learning with errors for fully homomorphic encryption for managing and securing computations in cloud computing. In this regard, homomorphic encryption can be useful when amending the problems with reinforcement learning techniques in cloud computing environments, which concerns the privacy domain. Therefore, to the users looking for RL services on the cloud computing environment, the proposed privacy-preserving reinforcement-learning framework, which entails using homomorphic encryption, as mentioned above, assists in allowing the use of such services while servicing the 'source data privacy' of users.[4]

II. LITERATURE REVIEW

Today, cloud computing has surprisingly gained acceptance over the recent past primarily due to the following reasons it has some merits over traditional computing such as Storage & Productivity & Cost. However, there is always a flip side to the cloud computing story in that; the ability of the cloud to manage data security is somewhat questionable. Cloud SaaS products are now dominant in the market currently and almost all of the cloud applications have well-established security solutions; however, the threats of security breaches are very much real. As such, to address this challenge, several measures of security have been incorporated to the system as a way of ensuring that only qualified candidates get through; this has included the use of the neural network as well as specially coded algorithms. Neural networks are also commonly being used in cloud infrastructure especially in a case of building the new architecture. CSPs apply neural networks in increasing ways of storing data and in defending the storage systems against attacks. In this case, data is compressed before dispatch to the cloud such that unauthorized clients do not access it throughout transit. Furthermore, there is the ability to solve the following computations on encrypted data while maintaining its highly secure and encrypted form: This is made achievable by the use of homomorphic encryption as the ability to perform computation on encrypted data without having to decrypt it first. This approach means that even if the provider of cloud service is violated, the data is still protected from leakage and cannot be accessed without the use of a decryption key as the transmitted data will be in an encrypted format. The combined neural networks and encryption mechanism as an enhanced security model are employed in cloud computing. It avoids the eavesdropping of messages and information held in the cloud and guarantees third parties to engage with encrypted data that can only be processed and decrypted by the data provider. The general objective of this research work is to evaluate the likelihood of applying deep learning methods and thereby incorporate the ideas of the use of neural networks and encryption to produce a safe security system for cloud computing. This research also aims to pose questions on how anonymity and encryption of data influence the application of neural networks, whether homomorphic encoding is of value not only to restore the original form of data but also to ensure that dataremains confidential as it provides insightful information from the specific data set.[5]

Cloud computing is widely implemented within the Information Technology sector due to such features as virtualization, scalability, cost-efficiency, and sharing on- demand. However, about data storage and transmission using cloud services, constant doubts emerge as to security. These concerns stem from the openness of cloud databases and the risks of obtaining unofficial access to the data or having the key to encipher the data stolen. To these challenges, this paper presents a viable solution where the AES encryption will be dynamic and the blockchain will be used to manage keys. Dynamic AES encryption increases the data protection level and minimizes the risk of hackers' attacks and unauthorized access. At the same time, blockchain technology offers a secure keystore of encryption keys with related metadata to reach high levels of protection and data credibility. Moreover, ensuring security during transmission and storage the Elliptic Curve Cryptography public key encryption system used in modem and portable device data communication significantly enhances security and data sharing. In summary, this kind of approach contributes to the upliftment of cloud security as it offers features such as high-level encryption, distributed key control, and safeguard from unauthorized admittance. The fact that it can be scaled and easily adjusted, which is vital in modern approaches to cloud protection, guarantees users the confidentiality of data stored in the cloud. The following suggested solution reflects on the upcoming complexities in cloud computing concerning data protection. Based on the fast dynamic AES encryption and blockchain key management, this new solution for the first time provides a systematic approach to solving the unceasing issues of data security in cloud computing. Moreover, this solution also solves the main design issues that come into existence during the design of drone routing approaches for drone delivery networks. This solution proposes a new way of improving cloud data protection by using dynamic AES encryption on the fly and key storage in the blockchain. Thus, by integrating dynamic AES encryption into the highlighted key management technique, it is possible to propose an original and multifaceted approach to solve the critical issues of data security in cloud computing.[6]

The suggested services mainly aim at the rise of reasons for outsourcing the tasks of data processing and storage. This is a trend that is a considerable menace; especially when it comes to the process of showing that data privacy over encrypted data is possible to support the search. To counteract this challenge, a novel method called privacy- preserving multi-keyword ranked search over encrypted data in a hybrid cloud is proposed which is known as MRSE-HC. It uses a special technique known as bisecting k-means clustering keyword partition strategy it divides the keyword dictionary in the documents into near-equal clusters. These partitions are then used to arrive at the keyword partition-based bit vectors for both documents as well as the query, or you could perhaps say the search index. In general, the MRSE-HC scheme is intended for private cloud prechecking of candidate documents through the partition of keywords into a bit vector and applying a trapdoor for identification of the search results of candidates in the public cloud. More to this, there is an improvement method of MRSE-HC called EMRSE-HC that has been developed. This enhancement scheme builds on these points and goes into the full binary pruning tree to provide optimization of the search system. For the defined privacy-preserving multi-keyword ranked search schemes for hybrid clouds, the following terms have been used in this paper: MRSE-HC and EMRSE-HC. These schemes offer better search than the previous well-known scheme FMRS. These schemes allow the fast and secure translation of queries on the encrypted data, as implemented in hybrid cloud systems, without revealing the identity or other similar information that may be undesirable. In the privacy-preserving multi-keyword ranked search scheme on the encrypted data in hybrid clouds called MRSE-HC, a bisecting K-mean based keyword partition algorithm is used for the division of the keyword dictionary of documents into framed partitions.[7]

III. FUNDAMENTALS OF CLOUD SECURITY

A. Definition and Significance of Cloud Security

The technological environment has greatly evolved over the years, and this has or has led to Cloud Security being a critical issue today. Cloud security on the other hand refers to the set of measures used to protect the resources used in cloud computing which include data, applications, information and infrastructure. They're required indispensable high-quality cloud security, because various areas, such as agriculture, tourism, transport, and energy production use cloud services to perform business functions. These attributes demonstrate that cloud security is essential of paramount importance because security in cloud computing is rather sensitive to the safety of data and availability and integrity of services. Effective security measures that are designed and put in place for the enterprise cloud architecture safeguard the data against such incidents as breaches or invasions by cyber criminals that may compromise the data stored in the cloud. For instance, data that is labeled as information concerning weather patterns or manner of cultivating the soil would be rather sensitive in the agricultural practice; had the farmers embraced secure cloud systems, they would have made the right decisions. This stability in tourism can ensure that cloud-based systems can be implemented securely for deigning bookings or other personnel information. One advantage that cloud security brings is the protection of operational details in the transportation and energy sectors to boost their performance. It must be understood that planning of activities in disaster management is as essential for cloud security too, along with the prevention and control of disasters which are common in the natural world. Therefore, owing to cloud data's dependability and the ability to return to the status of prior operations within a short period, the organizations' businesses would stay functional at their prime level even under the environmental conditions that may occur due to harsh weather or other disruptive situations. This is most relevant to industries that are exceptionally reliant on data transmission and asynchronous or synchronous communication in real-time. Cloud security plays a significant role in ensuring that the intended cloud consumers and providers can maintain and achieve the expected level of security in cloud computing systems. Ways in which it is relevant, can be described using the trend towards the need to secure the identities of numerous industries and prevent the disruption of the activities of various fields. Therefore, calling for the best cloud security measures is paramount in achieving optimum use of cloud computing innovations while minimizing threats and vulnerabilities in their services.[8]

B. Key Components and Processes Involved inCloud Security

Cloud computing is widely implemented within the Information Technology sector due to such features as virtualization, scalability, cost-efficiency, and sharing on- demand. However, about data storage and transmission using cloud services, constant doubts emerge as to security. These concerns stem from the openness of cloud databases and the risks of obtaining unofficial access to thedata or having the key to encipher the data stolen. To these challenges, this paper presents a viable solution where the AES encryption will be dynamic and the blockchain will be used to manage keys. Dynamic AES encryption increases the data protection level and minimizes the risk of hackers' attacks and unauthorized access. At the same time, blockchain technology offers a secure keystore of encryption keys with related metadata to reach high levelsof protection and data credibility. Moreover, ensuring security during transmission and storage the Elliptic Curve Cryptography public key encryption system used in modem and portable device data communication significantly enhances security and data sharing. In summary, this kind of approach contributes to the upliftment of cloud security as it offers features such as high-level encryption, distributed key control, and safeguard from unauthorized admittance. The fact that it can be scaled and easily adjusted, which is vital in modern approaches to cloud protection, guarantees users the confidentiality of data stored in the cloud. The following suggested solution reflects on the upcoming complexities in cloud computing concerning data protection. Based on the fast dynamic AES encryption and blockchain key management, this new solution for the first time provides a systematic approach to solving the unceasing issues of data security in cloud computing. Moreover, this solution also solves the main design issues that come into existenceduring the design of drone routing approaches for drone delivery networks. This solution proposes a new way of improving cloud data protection by using dynamic AES encryption on the fly and key storage in the blockchain. Thus, by integrating dynamic AES encryption into the highlighted key management technique, it is possible to propose an original and multifaceted approach to solve the critical issues of data security in cloud computing.[9].

C. Challenges and Limitations of Traditional Cloud Security Approaches

Traditional cloud automation methods have some advantages, but indeed, they come with quite a few challenges and limitations. They are, among others, managing various cloud environments, legacy systems technology compatibility problems, as well as disparities upon standardization between the tooling and practices of automation. Moreover, scalability of automation processes isdifficult across big, complex distributed environments, hence at times they might be incompetent. In addition, extensiveness and fast-changing of the cloud infostructure might make the conventional automation methods helpless in this regard. Resolving these problems is through implementing wide and comprehensive approaches to cloud automation of which novel technologies like AI and ML are availed to improve delivery standards, scalability, and adaptation.

IV. EXCEPTION METHODOLOGY

NCS is an ingenious technique created to improve on the current strategies used in cryptosystems through the inclusion of a number of complex classes. In this study, it builds upon the foundation of a good prime, LCG, SWA, and XOR gate logic as a sound means of effecting good encryption and decryption processes. Using a good prime number is highly relevant for NCS because of the properties of such type of number that create a principal difficulty for factorization, which is the main point for strengthening the cryptographic system. It is worthy of note that Linear Congruential Generator (LCG) is used due to its efficiency in generating pseudo-random numbers whereby this series is imperative in forming cryptographically random keys. The role of the Fixed Sliding Window Algorithm (SWA) is very crucial in the optimization of the encryption functions since the process is divided into manageable windows. This approach does not only increase the capabilities of the software/program but also the security by making it more difficult for the attacker to guess the next encryption pattern. XOR logic gate is another widely used gate in the cryptographic applications due to its ability to concatenate the generated pseudo-random numbers to the plaintext in NCS. This operation acts at the bit level to ensure that the outcome is inherently as unpredictable as possible so that the attacker will not be able to decode the original message without the key. Combining these components, NCS offers a very reliable and effective cryptographic solution, which utilizes the features of each of the mentioned techniques to prevent unauthorized access and attacks to the confidential information.[10]

Convergent encryption and the role of re-encryption algorithms to be put into operation together with the Dynamic Count Filters (DCF) as advanced and noble solutions in the field of data security and ownership rights identification. Convergent encryption applied on plaintext data allows for reducing redundancy by encrypting two and more identical plaintexts into one and the same ciphertext on the one hand, and combining the advantages of both symmetric encryption and decryption on the other hand; this is useful in cloud computing. A block of securing; role re-encryption algorithms helps the data to beshared and collaborated, while ensuring the confidentiality of the information even when the data has to be decrypted from one key and encrypted to the key of the recipient without the latter having to see the information in plain form. DCF as specific components of filters increase the speed and flexibility of data updating and ownership confirmation through mechanisms associated with the utilization of probabilistic data structures for counting tasks that are necessary in situations when updating and confirming data is required frequently, for example, in decentralized databases or blockchains. Collectively, these technologies provide integrated cloud-based protection for data ownership and data guarantee processes in contemporary distributed frameworks while boosting general security and agility in numerous applications such as cloud services, blockchain, and distributed data storage.[11]

The Improvement of the RDIC (Remote Data Integrity Checking) protocol increasing the privacy of the protocol gives a remarkable advancement by enhancing the feature of “zero-knowledge privacy” to enhance data privacy in communication. RDIC protocols are useful in so far as guaranteeing the security of data that is stored off-site, widely used in cloud computing paradigms where data outsourcing is rife. Incorporating ZKP into RDIC allows for data validation without any knowledge of the data, its content, or its attributes. Indeed, in a zero-knowledge proof, the unspoken part guarantees that the integrity of the data is ensured while the identity of the owner of the data remains protected. Zero-knowledge proofs are basically where a prover can convince a verifier of some statement without the latter getting any further information beyond if the statement is true or not. In the context of RDIC, this implies that a CSP can convincingly demonstrate data authenticity to the data owner without knowing the contents of the data being outsourced. This bring a lot of improvement to the current protection of data from unauthorized access or leakage. Through the adoption of zero-knowledge privacy in the RDIC protocol, there will be an improvement in the security of data to organizations that are in the cloud and improve trust so that more and more organizations become comfortable with cloud technologies. This advancement is pertinent to the current postmodern world where personal information becomes even more valuable, and protection thereof is paramount to the success of virtually every organization. [12]

Cryptography and its tools are very central in the protection of privacy in the current world given that data, no matter how secure, can always be breached. These techniques define a broad scope of the methods that should be applied to protect the authenticity, integrity, and confidentiality of the data. When it comes to the tools for employing the much-needed cryptographic techniques, the Differential Privacy Data Publishing protocol is among the most efficient means in the spheres of data publishing and continuous data updating while ensuring enhanced privacy. The DPDP protocol operates through three key operations: Prepare Update is where you read the update commonly in the form of disk images to be written on the CompactFlash card, Perform Update is where the contents of the update file are copied and scripted to the end user/s and Verify Update which is like a final check to ensure that the Update/Change was successfully completed. During this step, the data owner creates a differential privacy parameter and orients the update operation on the dataset. Later, in the Perform Update phase, the actual update operation on the dataset takes place; again, while updating, the privacy of an individual is maintained. Last of all in the Verify Update step, the data owner confirms the correctness and completeness of the updated dataset, as he also marks the effective utilization of privacy-preserving techniques. By incorporating encryption, hashing, and zero-knowledge techniques in the DPDP framework, the privacy of data is well maintained while the update of data is efficiently achieved. These techniques allow data owners to update datasets with less leakage of individuals’ information to improve the responsible sharing of data in several sectors such as healthcare, finance, and government. [13]

V. RELATED WORKS

Cloud computing solution has revealed a trend of adoptingthe solution within the current past; there has been the awareness and adoption of cloud services. However, cloudcomputing has also opened a few opportunities and threats with regard to its security. These security issues arise from the nature of cloud resources that are shared and the ease ofassembly, and extension of the cloud environment along with the facility of manipulation by the third party or an unauthorized person to gain access to the system or even corrupt the data. In this regard, the researchers and practitioners have directed the attention towards the ML techniques to address these concerns. From the research conducted in the existing literature, it can be inferred that the inclusion of ML approach in the cloud computing environment has revealed efficiency for the security issues like the detection of the attacks, the prevention of the attacks, the identification of the vulnerabilities, and the protection of the user’s data’s privacy. These techniques analyse vast volumes of information and, moreover, identify the patterns of the unusual occurrence that can imply possible security threats. Hence, it can be concluded that cloud security systems enhance their stance with the help of machine learning and updated knowledge regularly.

. It also allows for the ideal incorporation of the present machine learning models such as aid Vector Machines andalso outline differences in the model’s performance. Thus,this systematic review focuses on the right direction of applying machine learning in cloud computing for enhancing the cloud security and for the subsequent researches on the similar topic. The implementation of machine learning in the protection and prevention of cloudsystems will assist organizations in enhancing on the area of security from the attacks, identifying vulnerability, and guarantee the safety of personal information. This demonstrates how machine learning encounters the novel and didactic for resolving the security of cloud computing.[14]

The capability of self-driving car is innovative because of its employment of AI, machine learning featured with integrated robotics to eliminate the necessity of a human driver. This, in turn, should lead to a marked enhancement in the efficiency of transport, the rationally organization of fuel consumption, and passengers’ safety; not to mention the aesthetic enjoyment to be derived from traveling. On the same note, with a shift to more automated vehicles which are equipped with artificial intelligence for decision making, there is a creation of new problems like security and privacy. These are new generation vehicles with computers within the automobiles and they integrated themto communication networks and this makes them vulnerable to various attacks. Moreover, with the increase in storage and deposit of huge volumes of data that containpasscode information on self-driving cars a lots of privacy risks are realized. This paper aims at analyzing the root causes of the mentioned security issues and privacy concerns in self-driving cars. This paper will distinguish between the contents of the different forms of attacks on the autonomous vehicles with regards to the layers, elucidate the architecture of the different layers of autonomous vehicles through the use of a four layered model, and review on the security and privacy attack towards them; the paper will in addition discuss on the various means of handling these threats. Hence, this paper attempts to discuss the open issues in the context of AVs and provide guide for the future researchers so that the future AVs that are integrated into our transport systems are safe and secure. This paper is a survey on security as well as privacy threats in relation to ASVs; the authors have adopted a layering structure. They have also analysedthe modellings of these self-driving cars in four-layer model and have described several security and privacy issues of these cars. Besides, the authors have provided various counter measures to enumerate the said security and privacy threats.[15]

VI. CONCLUSION

The growth of cloud computing means that it is an environment of potential and adversities, including security and Issues of running queries. In this extensive research work, several mechanisms and processes have been carefully discussed to enhance the security of the cloud paradigm, ranging from GPG encryption techniques up to the recent inventions of NCS and RDIC along with Zero- Knowledge Privacy. These strategic approaches are discovered στιγμές used for dealing with the dynamic nature of the cloud systems and the ever-increasing threat intelligence of cybercriminals. Similarly, the integration of artificial intelligence (AI) with cloud management comes as the primary key factor that can help address the issues that revolve around resources and improve performance. Strategies like the LSTM algorithms and the DRL platforms provide flexibility in resource management and reduction in energy use, they allow the system optimum overall performance with minimal expenditures. In addition, advances in computational acceleration including integration of ReDCIM processors and the novel in-memory Booth multiplication using BIT proceed to provide noteworthy impacts in enhancing the efficiency and resource consumption in cloud platforms. The presented advancements enable cloud platforms to solve highly computational problems more flexibly and efficiently, thus contributing to the growth of the field to new levels of organizational brilliance. Therefore, AI technologies and methodologies in collaboration with innovative research can support the goal of enhancing technological advancements and their future that governs cloud computing services delivery systematically, aggressively deal with security challenges and the efficient utilization of resources in the digital world, making it the pinnacle of technology.

VII. REFERENCES

1. Celiktas, B., Çelikbilek, İ., & Ozdemır, E. (2021,January 1). A Higher-Level Security Scheme forKey Access on Cloud Computing. Institute ofElectrical and Electronics Engineers, 9, 107347-107359. https://doi.org/https://doi.org/10.1109/access.2021.3101048

2. Gupta, I., Singh, A K., Lee, C., & Buyya, R. (2022,January 1). Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions. Institute of Electrical and Electronics Engineers, 10, 71247-71277. https://doi.org/https://doi.org/10.1109/access.2022.3188110

3. BENIAMINO, DI, MARTINO., ANTONIO, ESPOSITO., ERNESTO, DAMIANI. (2019). TOWARDS AI- POWERED MULTIPLE CLOUDMANAGEMENT. IEEE INTERNETCOMPUTING, https://doi:10.1109/MIC.2018.2883839

4. Park, J., Kim, D., & Lim, H. (2020, January 1). Privacy-Preserving Reinforcement Learning Using Homomorphic Encryption in Cloud Computing Infrastructures. Institute of Electrical and Electronics Engineers, 8, 203564-203579. https://doi.org/https://doi.org/10.1109/access.2020.3036899

5. Sana, M U., Li, Z., Javaid, F., Liaqat, H B., & Ali, M U. (2021, January 1). Enhanced Security in Cloud Computing Using Neural Network and Encryption. Institute of Electrical and Electronics Engineers, 9, 145785-145799. https://doi.org/https://doi.org/10.1109/access.2021.3122938

6. Shakor, M Y., Khaleel, M I., Safran, M., Alfarhood, S., & Zhu, M. (2024, January 1). Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. Institute of Electrical and Electronics Engineers, 1-1. https://doi.org/https://doi.org/10.1109/access.2024.3351119

7. Dai, H., Ji, Y., Yang, G., Huang, H., & Yi, X. (2020, January 1). A Privacy-Preserving Multi- Keyword Ranked Search Over Encrypted Data in Hybrid Clouds. Institute of Electrical and Electronics Engineers, 8, 4895-4907. https://doi.org/https://doi.org/10.1109/access.2019.2963096

8. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019, January 1). Security and Privacy- Preserving Challenges of e-Health Solutions inCloud Computing. Institute of Electrical and Electronics Engineers, 7, 74361-74382. https://doi.org/https://doi.org/10.1109/access.2019.2919982

9. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5. https://doi.org/10.1186/1869-0238-4-5

10. Srinivasan, S., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2012). State-of-the-art cloud computing security taxonomies: A classification of security challenges in the present cloud computing environment. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (pp. 470-476). https://doi.org/10.1145/2345396.2345467

11. Pike, T. W., Gagnon, K. B., Worthen, N. J., &Blumstein, D. T. (2022). No evidence of auditoryhabituation to noise in the wild. PLOS ONE, 17(4),e0274628. https://doi.org/10.1371/journal.pone.0274628

12. Doe, J. (2019). Advances in data securitytechniques. IEEE Access, 7, 2920998. https://doi.org/10.1109/ACCESS.2019.2920998

13. Shahriar, H., & Kamali, S. (2014). Remote data integrity checking with data privacy preservation in cloud storage. International Journal of Information Security, 13(5), 469-478. https://doi.org/10.1007/S10207-014-0263-8

14. Nassif, A B., Talib, M A., Nasir, Q., Albadani, H.,& Dakalbab, F. (2021, January 1). Machine Learning for Cloud Security: A Systematic Review. Institute of Electrical and Electronics Engineers, 9, 20717-20735. https://doi.org/10.1109/access.2021.3054129

15. Hataba, M., Sherif, A., Mahmoud, M., Abdallah, M., & Alasmary, W. (2022, January 1). Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey. IEEE Communications Society, 3, 811-829. https://doi.org/https://doi.org/10.1109/ojcoms.2022.3169500