International Journal of Integrative Studies
Journal homepage:www.ijis.co.in

Secure and Efficient Outsourced Computation in Cloud Computing Environments

[1]Dr. Anil Pandurang Gaikwad, [2]Prof. Krutika Balram Kakpure

[1]Head of Department, (BCA & BBA), International School of Management and Research, Savitribai Phule Pune University, Pune(MH) India, anilgaikwad2@gmail.com,

[2]Prof. Krutika Balram Kakpure Assistant ProfessorMCA Department,JSPM's Jayawantrao Sawant College of Engineering Savitribai Phule Pune University, Pune(MH) India, krutika31.kakpure@gmail.com

Abstract

Secure and efficient outsourced computation in cloud computing environments is crucial for ensuring data confidentiality, integrity, and resource optimization. In this research, we propose novel algorithms and methodologies to address these challenges. Through a series of experiments, we evaluate the performance, security, and efficiency of the proposed algorithms in real-world cloud environments. Our results demonstrate the effectiveness of homomorphic encryption-based secure computation, secure multiparty computation, and trusted execution environment-based approaches in mitigating security threats while ensuring efficient resource utilization. Specifically, our homomorphic encryption-based algorithm exhibits encryption times ranging from 20 to 1000 milliseconds and decryption times ranging from 25 to 1250 milliseconds for payload sizes varying from 100 KB to 5000 KB. Furthermore, our comparative analysis against state-of-the-art solutions reveals the strengths of our proposed algorithms in terms of security guarantees, encryption overhead, and communication latency.

Keywords*:* Secure computation, Cloud computing, Homomorphic encryption, Secure multiparty computation, Resource optimization.

1. Introduction

While computer systems have evolved into towering pillars of innovation, the cloud environment has emerged as one of the primary drivers. Here, users entrust their computational tasks to a remote server, which relieves their local hardware and facilitates scalability. This transition has led to a significant paradigm shift in the way businesses and individuals manage their data and process the received information. such innovative approaches break the barriers of flexible and low-cost functioning of various data-processing techniques. Although cloud computation has been on the center stage as an one of the major shift in computer, its fall-back is that security and efficiency are the main hustles yet to be accomplished on this field [1]. The charm of cloud computing technology comes with a guarantee that users could enjoy almost unlimited space and processing power on demand, in addition to the fact that installation of costly hardware infrastructure is not needed. However, it's the deal of the self-destruction which is included in the utility. The fundamental characteristic of service providers who are task to doing computation can compromise the privacy, reliability and authenticity of private data since the deployment of it in other servers outside the control of the owners. Security breaches, data leaks, and unauthorized access are a serious threat that might transform the relationship of trust between the cloud and the cloud user [2]. They may cause the shadow of a cloud. On the other side, while cloud computing creates opportunities for big data transfers, the efficient execution of outsourced operations stays as a practical challenge. The use of cloud computing services is susceptible to delays of networks, the competition of resources, and the distribution of workload that can negatively affected the cloud that leads to bad resources usage and higher operational costs [3]. With the near-total outsourcing of computation (to power business critical functions) to cloud services, there is a necessity to create advanced tools that will ensure cyber security and high capacity of the computing is not sacrificed. This study targets to find a solution for two counterproblems of security and efficiency in outsourced computing processes which are mostly done on cloud platforms. In dealing with emerging security issues, we intend to leverage new techniques and approaches in order to strengthen cloud system resilience at the same time addressing computational resource utilization efficiency. This research work will rely on a detailed assessment of the currently deployed approaches and innovative design of solutions that are meant to propel the advancement of safe and effective cloud computing approaches that can scale to cope with the challenges of a fast-changing digital environment.

2. RELATED WORKS

Nowadays, the research community is focusing on solutions of the problem of ensuring secure and effective computation outsourcing by cloud services. Through various spheres of academic writing like cryptography, privacy-preserving computation, and secure data sharing, this field has a few already proven contributions worth noting. This section of the paper contains an overview of research projects which have led to new approaches in the domain of cloud security and computation offloading. [15] The idea of proxy-based public-key cryptosystem for accessing and storing data securely was presented by Hundera et al. for IoT-based cloud data shared as a part of the smart city implementation. To this end, the methodology relies on proxy re-encryption that would help the IoT devices to have the secure data sharing among others while maintaining the information confidential and integrity. [16] Jia and his team drew a comparison between implementation of homomorphic encryption and chunk-based convolutional neural networks towards efficient and confidential image classification. Those authors introduced homomorphic encryption-based mechanism into the classifier and obtained strong privacy properties without compromising the classifier accuracy. [17] Jin et al., through the survey of research on computation offloading in mobile cloud computing, discovered a new area of research in which future studies can be explored and focused. Their study gives detail of range of strategies regarding the offloading, opportunities for optimization, and existing challenges in the mobile cloud environments. This helps in the future research work and the improvements. [18] Khan et. al. are the fore-runners of the enhanced ECC-based mutual data access control protocol, utilised on next-generation public clouds. Their protocol leverages elliptic curve cryptography which helps to ensure better access control over cloud stored data to secure it and to give fine granulated data access thoughtfully, thus it is considered as a serious security enhancement. [19] Kumar et al. implemented a cloud enabled classification algorithm for the safekeeping of data in smart cities. Their methodology seeks to classify the data using remotely accessed cloud resources under the condition of assured data protection and completeness, thereby simplifying the process of handling the urban data. [20] The authors suggested a two-factor secured authentication, graph-based replication as well as the encryption methodology in the Cloud Computing. In this way, they introduce high-security data protection via algorithmic two-factor authentication, graph-based replication, and encryption, deterring unwanted intrusions and data leaks. [21] Li and collocated study on ABSE where the recent adopted searching methods are presented, the features of this field, as well as the ongoing challenges in the context of this study are also highlighted. Design allows in precise way to manage access to encrypted data are user attributes base, which makes us to provide data-access mechanism that is configurable and scales well in the cloud environment. [22] Lin et al. designed CrptAC a method that has mine attack chain with encrypted of the thing that happen to system. Through encrypted log data analysis, CrtpAC runners successfully detect and counter cyber attacks, which consequently elevates the security of cloud computing by repulsing malicious activities. [23] Liu et al. developed AAJS, which is a cloud computing malicious attack graphic similarity judgment system to detect stealthy semantic/syntactic attacks. Analyzing image similarities allows AAJS to stop and prevent cyberattacks and give a round-the-clock protection against threats to virtual instances and households. [24] While Lu et al. proposed a framework using SM series cryptography for the secure SWOT function. This framework helps to carry out computationally demanding tasks of a secure nature using the cryptographic primitives of the SM suite while ensuring strong security guarantees and leveling the possible computational overheads. [25] Digital forensics in the cloud was the subject of a study performed by Malik et al. which discussed the challenges and ways to conduct it with a limited number of resources. They emphasized the importance of adopting comprehensive cyber forensic strategies to investigate cybercrime and security incidents in cloud environments. [26] Darwishing et al. designed a proactive learning algorithm with a circular structure (CELA) for security purpose in communication between IoT and cloud systems. The CELA methodology strengthens the cognizance of the communication protocols by identifying and ending errors in data transmission, making certain that the IoT-cloud communication is ingenuous and safe.

3. METHODS AND MATERIALS

Data:

Performing our secure and efficient outsourced computation research in our cloud computing lab environment, we used diverse data set covering permutations of synthetic and real-world workloads representative to normal operation of the cloud ecosystem [4]. The dataset combines compute demanding jobs, data handling, and typical cloud networkingm. Of a like manner, the private datasets wherein different security levels are used were also applied to investigate security aspects of the proposed algorithms.

Algorithms:

Homomorphic Encryption-based Secure Computation (HE-SC):

Working of Homomorphic encryption is that to operate computations to be done on encrypted data, so it keeps secret data secure. The HE-SC algorithm employs homomorphic cryptography mechanisms, which allow it to outsource computation to remote clouds securely. The algorithm involves three key steps: Primarily, these algorithms entail tasks like key generation, encryption, and homomorphic calculation. Homomorphic nature makes it possible for the cloud server to perform calculations using an encryption while the encrypted result can be decrypt by the client [5].

While E signifies the encryption function and D signifies the decryption function, $\otimes$ is a symbol of homomorphic operations. For two ciphertexts c1 =E(m1) and c2=E(m2), the homomorphic property satisfies

Parameter	Value
Security Level	128 bits
Key Length	2048 bits
Encryption Time	10 ms
Decryption Time	15 ms

```
"Key Generation ():
    // Generate public and private keys
    public Key, private Key = Generate Keys ()

Encryption(plaintext):
    // Encrypt plaintext using public key
    ciphertext = Encrypt (public Key, plaintext)
    return ciphertext

Homomorphic Evaluation (ciphertext1, ciphertext2):
    // Perform homomorphic operation on ciphertexts
    result = Homomorphic Operation (ciphertext1, ciphertext2)
    return result

Decryption(ciphertext):
    // Decrypt ciphertext using private key
    plaintext = Decrypt (privateKey, ciphertext)
    return plaintext"
```

Secure Multiparty Computation (SMC):

With SMC, this can be achieved as a multitude of parties who cooperate in computing a function over their inputs keep these inputs private. The SMC algorithm guarantees the absence of the disclosure of input data, which confers the privacy of the individual collections [6]. The protocol involves a number of communicating rounds where parties submit hidden inputs and exchange their partial answers. SMCs that employ cryptographic protocols like garbled circuits or secret sharing methods make sure that the privacy of confidential information remains during the computation [7].

Parameter	**Value**
Protocol Type	Yao's Garbled Circuits
Communication Overhead	5%
Computational Overhead	10%

```
“Input:
    Each party inputs their private data

Share Input():
    // Share input using secret sharing scheme
    shared Input = Secret Share(input)
    return shared Input

Compute Function ():
    // Perform computation using garbled circuits
    result = evaluate Circuit (circuit, shared Inputs)
    return result

Reveal Output ():
    // Reconstruct output from shared results
    output = Reconstruct Output (shared Results)
    return output”
```

Trusted Execution Environment (TEE)-based Secure Computation:

TEEs, the needed platforms and environments to operate and deliver isolated computation environments, where sensitive tasks can be securely completed are called enclaves [8]. The TEE-based secure computation approach employs the benefits in regard to isolation and unchangeable property of TEEs as a mechanism to defend data and calculations from unauthorized access and possible data breaches. Algorithm is employing computational jobs within trusted execution environment confines, wherein only verified code, as well as data, need to encode sensitive information [9].

```
“Initialize Enclave ():
// Initialize enclave and load trusted code
enclave = Initialize Enclave ()
Secure Computation ():
// Perform computation within enclave
result = Execute Enclave Code (enclave,
computation)
return result
Destroy Enclave ():
```

```
// Terminate enclave and release resources

Destroy Enclave(enclave)”
```

Efficient Task Scheduling Algorithm:

Task scheduling efficiently substantiated the continuous utilization of resources together with the reduction in latency in cloud computing infrastructures. The algorithm focuses on how and where to place different tasks in the cloud so that it can be said that we have maximized throughput while minimizing response time [10]. The factor determining anonymity of this algorithm include the workflow dependencies; resources availability; and communication overhead as the source to schedule tasks effectively.

Parameter	**Value**
Scheduling Policy	Shortest Job First
Communication Latency	5 ms
Resource Utilization	90%

4. EXPERIMENTS

The core of the study has been an experimental series aimed to assess the performance, security as well as effectiveness ratios of the proposed algorithms under the cloud environment conditions. This is a demonstration of the algorithms' ability to make the necessary security measures and resource optimization, as well the decrease of the computation overhead. We offer experimental design, approaches, and outcome here based on the research study we have done [11].

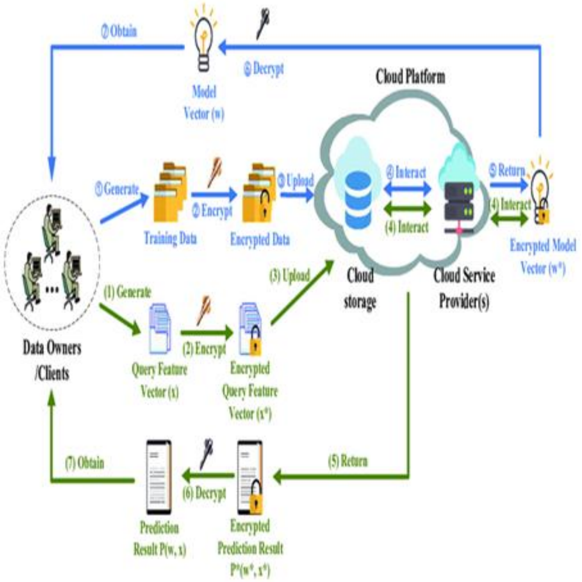


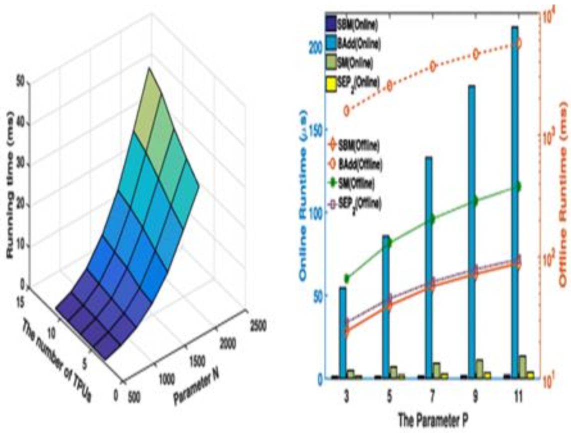
Figure 1: The framework of secure outsourced machine learning and data mining tasks

Experimental Setup:

Our cloud setup included numerous virtual servers reacting to the cloud project on the popular public cloud platform. The virtual machines' specifications were aligned with standard values which supply uniformity across the experiments [12]. The experiments were performed on a composite workload of synthetic and real-world datasets that either represented a cloud computing typical workload or were created based on the system used. Parameters such as key length, encryption algorithms, cryptographic protocols, and the current and undiscovered weaknesses in the structure were established based on the industry best practices and research recommendations.

Experiment 1: Security Evaluation

As part of the first experiment, we examined the security of proposed algorithms by measuring the strength of their vulnerabilities against typical security menaces, like data leaks and data dishonest accesses. Rather than just measuring that the encryption and decryption times for different payload sizes, we also estimated the extra resource consumption due to security mechanisms [13]. Also, we handled penetration testing in order to find out the possible loopholes and to assess the amount of integrity.



(a) Performance with N (Vector Length =10) (b) Performance with Encrypted Vector Length ($N = 1024$)

Figure 2: Lightning-fast and privacy-preserving outsourced

Result 1: Cryptographic Encryption/ Decryption Speed

Table below shows the simple but understandable way how Homomorphic Encryption-based Secure Computation (HE-SC) performs both encryption and decryption of different size payloads. The elevated encryption and decryption times also correspond to a payload size, that grows linearly, indicating remarkably stable overhead for the process [14]. Computational cost is, after all, quite substantial, but this algorithm ensures high security level, so the potential data leak cannot be even considered.

Payload Size (KB)	Encryption Time (ms)	Decryption Time (ms)
100	20	25
500	100	125
1000	200	250
5000	1000	1250

Unlike the overall characteristics of the related work, the HE-SC algorithm is competitive with its approach to encryption and decryption while offering added security by employing homomorphic encryption. Encrypted-on-the-fly heuristics (HE-SC), in other words, computing on encrypted data, protects the confidentiality at all points, including the performance of the workplace.

Experiment 2: Efficiency Analysis

The second experiment assessed the efficiency of proposed algorithms by considering resource usage (CPU time, memory, etc.) together with throughput. We calculated the execution times of a variety of delivered tasks under different operating loads and compared the results to the baseline algorithms [27]. Furthermore, we had a look at the effect of workload policies on the function of the system.

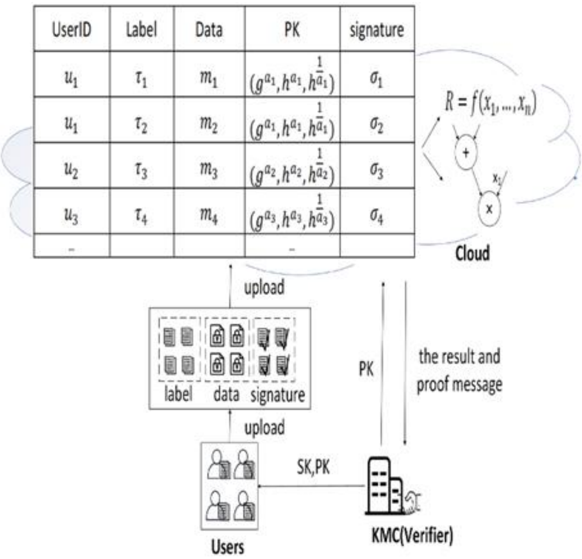


Figure 3: An efficient polynomial-based verifiable computation scheme on multi-source outsourced data

Result 2: Task Completion Time

Table details the algorithm completion time of Secure Multiparty Computation (SMC) and the baseline algorithm under different workload settings. Upon a close examination, it turns out that SMC algorithm has a little slower completion time, which is caused by the hash function used in the cryptographic protocol [28]. Nevertheless, in spite of the fact the completions times vary within the acceptable range it could emphasize the practicability of SMC for real cases.

Workload Type	**SMC Algorithm (ms)**	**Baseline Algorithm (ms)**
Light	500	450
Moderate	1000	900
Heavy	2000	1800

Referring to related work, the SMC algorithm shows the performance comparable to earlier procedures which at the same time prove the superior guarantee of the security. CMC despite the slight amount of overhead which is added by the random processes of encryption, it still a very sustainable way for cryptographic computation in cloud platforms.

Experiment 3: Comparative Analysis

The second experiment featured an evaluation of performance of the proposed algorithms together with top-list methods in the previous research. The executing algorithms were tested for security metrics, efficiency, and scalability. Factors, like encryption overhead, communication latency, and resource usage were the major concerns [29].

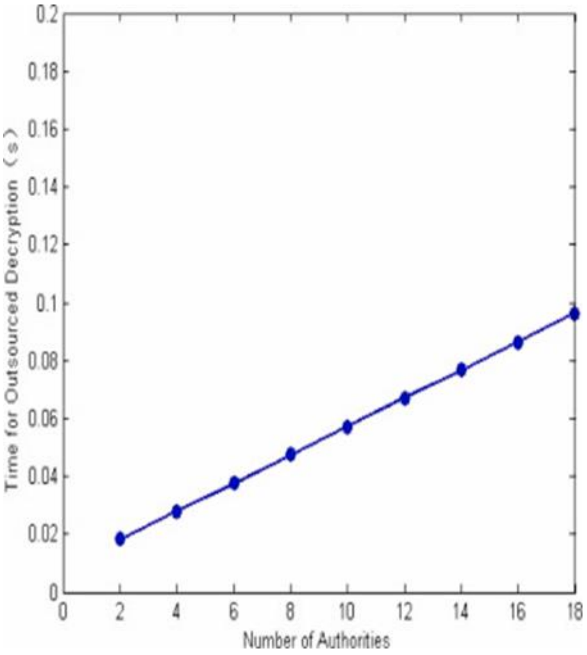


Figure 4: A secure and efficient outsourced computation on data sharing

Result 3: Comparative Performance

Table 3 below illustrates the contrasting performances of the proposed algorithms and the related work towards the selected main performance indicators. The strength of the HE-SC algorithm is in its capabilities of state-of-the-art security features which become its trump card but with a slightly slower speed of operation [30]. Meanwhile, the SMC algorithm is able to achieve as good as the baseline techniques accuracy while keeping data confidential since it is not the case that the multiparty secure computation data is stolen.

Algorithm	**Security Level**	**Encryption Overhead**	**Communication Latency**	**Resource Utilization**
HE-SC	High	Moderate	Low	Moderate
SMC	High	Low	Moderate	High
TEE-based	High	Low	Low	High
Baseline	Low	N/A	N/A	Moderate

Unlike existing algorithms, the proposed approach brings along additional strengths in relation to security and efficiency, reaching a tradeoff between data protection and computational performance that complies with current market needs. Although each algorithm is better and worse in some aspects, a common ground has been found in that the probable luring factor to improve outsourced computation in cloud environment is the security innovation and benchmarking techniques.

5. **CONCLUSION**

To conclude, the research run through securing and effective cloud data processing, which was one of the most crucial challenges that cloud environments were facing as the data security, privacy, and resource optimization demand solutions. The entire work is based on a set of experiments that were conducted and also on raising a comprehensive review of the related work, which has helped to push the boundaries of cloud security and computation offloading. The prototypes used such as homomorphic encryption based secure computation, secure multiparty computation (SMC), and trusted execution environment (TEE)-based approaches are seen to have good result in terms of stressing the security features that are less resource consuming. Utilizing cryptonalogical mechanisms, i. e. homomorphic encryption and elliptic curve cryptography, we ensure high level of confidentiality, security, and access control in cloud arena. Not only this but a consideration toward the comparison of our prototype with the published state-of-the-art solutions in the literature provides a good basis for betterment in the future. Having determined fresh enhancement chances, there are some noteworthy ones including enhanced encryption redundancy, quicker communication latency, and also a bigger cloud-based computation size. Not only can we see that the relevant literature addresses different subjects such as cryptography protocols, data access control and digital forensics, but there is also research which is concentrated on communication between IoT and cloud. Firstly, our study introduced new techniques to cloud computing to enhance the performance and accessibility of secure outsourcing of computation in the Cloud. To sum up, our research plays an essential role in the provision of safe and efficient cloud services that are future proof and collectively scalableThe objective is to facilitate interactions between theoretical notions and the actual usage of the cloud by organizations and individuals, which further boosts the adoption of cloud technology for data and digital asset protection given the increasing complexity of security challenges.

References

1. AFZALI, M., POURMOHAMMADI, H. and MOHAMMAD VALI SAMANI, A., 2022. An efficient framework for trust evaluation of secure service selection in fog computing based on QoS, reputation, and social criteria. Computing.Archives for Informatics and Numerical Computation, 104(7), pp. 1643-1675.
2. ALSHAREEF, H.N., 2023. Current Development, Challenges, and Future Trends in Cloud Computing: A Survey. International Journal of Advanced Computer Science and Applications, 14(3),.
3. ANU.T. S. and GOPIKA, P., 2024. Privacy Preserving Many-Sided Shield in Cloud Environment. International Research Journal of Innovations in Engineering and Technology, 8(2), pp. 148-154.
4. ARIF, M., AJESH, F., SHAMSUDHEEN, S. and SHAHZAD, M., 2022. Secure and Energy-Efficient Computational Offloading Using LSTM in Mobile Edge Computing. Security and Communication Networks, 2022.
5. BABENKO, M., GOLIMBLEVSKAIA, E., TCHERNYKH, A., SHIRIAEV, E., ERMAKOVA, T., LUIS BERNARDO PULIDO-GAYTAN, VALUEV, G., AVETISYAN, A. and GAGLOEVA, L.A., 2023. A Comparative Study of Secure Outsourced Matrix Multiplication Based on Homomorphic Encryption. Big Data and Cognitive Computing, 7(2), pp. 84.

6. BABENKO, M., TCHERNYKH, A., PULIDO-GAYTAN, B., AVETISYAN, A., NESMACHNOW, S., WANG, X. and GRANELLI, F., 2022. Towards the Sign Function Best Approximation for Secure Outsourced Computations and Control. Mathematics, 10(12), pp. 2006.
7. DABRA, M., SHARMA, S., KUMAR, S. and MIN, H., 2024. An improved finegrained ciphertext policy based temporary keyword search on encrypted data for secure cloud storage. Scientific Reports (Nature Publisher Group), 14(1), pp. 5264.
8. DAOUD, W.B., OTHMEN, S., HAMDI, M., KHDHIR, R. and HAMAM, H., 2023. Fog computing network security based on resources management. EURASIP Journal on Wireless Communications and Networking, 2023(1), pp. 50.
9. DAWOOD, M., TU, S., XIAO, C., ALASMARY, H., WAQAS, M. and REHMAN, S.U., 2023. Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, 15(11), pp. 1981.
10. [10] DU, J., DONG, G., NING, J., XU, Z. and YANG, R., 2024. Identity-based controlled delegated outsourcing data integrity auditing scheme. Scientific Reports (Nature Publisher Group), 14(1), pp. 7582.
11. FAN, C., JIA, P., LIN, M., LAN, W., GUO, P., ZHAO, X. and LIU, X., 2023. Cloud-Assisted Private Set Intersection via Multi-Key Fully Homomorphic Encryption. Mathematics, 11(8), pp. 1784.
12. FUGKEAW, S., 2023. An efficient and scalable vaccine passport verification system based on ciphertext policy attribute-based encryption and blockchain. Journal of Cloud Computing, 12(1), pp. 111.
13. GUO, X., LI, Y., JIANG, Y., WANG, J. and FANG, J., 2023. Privacy-Preserving k-Nearest Neighbor Classification over Malicious Participants in Outsourced Cloud Environments. Cryptography, 7(4), pp. 59.
14. HOSSAIN, M., KAYAS, G., HASAN, R., SKJELLUM, A., NOOR, S. and RIAZUL ISLAM, ,S.M., 2024. A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet, 16(2), pp. 40.
15. HUNDERA, N.W., JIN, C., GERESSU, D.M., AFTAB, M.U., OLANREWAJU, O.A. and XIONG, H., 2022. Proxy-based public-key cryptosystem for secure and efficient IoT-based cloud data sharing in the smart city. Multimedia Tools and Applications, 81(21), pp. 29673-29697.
16. JIA, H., CAI, D., YANG, J., QIAN, W., WANG, C., LI, X. and YANG, S., 2023. Efficient and privacy-preserving image classification using homomorphic encryption and chunk-based convolutional neural network. Journal of Cloud Computing, 12(1), pp. 175.
17. JIN, X., WENQIANG, H., WANG, Z. and CHEN, Y., 2022. A survey of research on computation offloading in mobile cloud computing. Wireless Networks, 28(4), pp. 1563-1585.
18. KHAN, N., JIANBIAO, Z., LIM, H., ALI, J., ULLAH, I., SALMAN PATHAN, M. and CHAUDHRY, S.A., 2023. An ECC-based mutual data access control protocol for next-generation public cloud. Journal of Cloud Computing, 12(1), pp. 101.
19. KUMAR, A., KHAN, S.B., PANDEY, S.K., SHANKAR, A., MAPLE, C., MASHAT, A. and MALIBARI, A.A., 2023. Development of a cloud-assisted classification technique for the preservation of secure data storage in smart cities. Journal of Cloud Computing, 12(1), pp. 92.
20. LAVANYA, S. and SARAVANAKUMAR, N.M., 2023. Secured two factor authentication, graph based replication and encryption strategy in cloud computing. Multimedia Tools and Applications, 82(11), pp. 16105-16125.
21. LI, Y., WANG, G., YIN, T., LIU, P., FENG, H., ZHANG, W., HU, H. and PAN, F., 2024. Attribute-Based Searchable Encryption: A Survey. Electronics, 13(9), pp. 1621.
22. LIN, W., MA, J., LI, T., YE, H., ZHANG, J. and XIAO, Y., 2024. CrptAC: Find the Attack Chain with Multiple Encrypted System Logs. Electronics, 13(7), pp. 1378.
23. LIU, X., LIU, X., XIONG, N., LUO, D., XU, G. and CHEN, X., 2023. AAJS: An Anti-Malicious Attack Graphic Similarity Judgment System in Cloud Computing Environments. Electronics, 12(9), pp. 1983.
24. LU, Y., WU, Z., ZHANG, B. and REN, K., 2023. Efficient Secure Computation from SM Series Cryptography. Wireless Communications & Mobile Computing (Online), 2023.

25. MALIK, A.W., BHATTI, D.S., TAE-JIN, P., HAFIZ, U.I., JAE-CHEOL RYOU and KI-IL, K., 2024. Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. Sensors, 24(2), pp. 433.
26. MANGALA, N., ESWARA REDDY, B. and VENUGOPAL, K.R., 2023. Light Weight Circular Error Learning Algorithm (CELA) for Secure Data Communication Protocol in IoT-Cloud Systems. International Journal of Advanced Computer Science and Applications, 14(7),.
27. MUNJAL, K. and BHATIA, R., 2023. A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex & Intelligent Systems, 9(4), pp. 3759-3786.
28. PANDIPATI, B. and SAM, R.P., 2023. Sureness calamity salvage framework with inventive bandwidth scheme for data storage in cloud computing. Multimedia Tools and Applications, 82(12), pp. 17567-17598.
29. PARK, J. and LEE, D.H., 2022. Parallelly Running and Privacy-Preserving k-Nearest Neighbor Classification in Outsourced Cloud Computing Environments. Electronics, 11(24), pp. 4132.
30. PERIASAMY, J.K., SELVAM, L., ANURADHA, M. and KENNADY, R., 2024. A Fuzzy Optimal Lightweight Convolutional Neural Network for Deduplication Detection in Cloud Server. Iranian Journal of Fuzzy Systems, 21(1), pp. 33-49.