Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Balancing Security And Performance In Cloudlet-Assisted Computing

Ambika S. Jaiswal[1] , Dr. V. M. Thakare[2] , Dr. Mohd. Atique[3] , Dr. S. S. Sherekar[4] , Amitesh Jaiswal[5] , Suhashini Awadhesh Chaurasia[6]

[1]Department of Computer Science, SGB Amravati University,
jaiswalambika@gmail.com
[2]Department of Computer Science, SGB Amravati University,
vil.thakre@gmail.com
[3]Department of Computer Science, SGB Amravati University,
mohd.atique@gmail.com
[4]Department of Computer Science, SGB Amravati University,
ss.sherekar@gmail.com
[5]Department of CSE-Data Science, RCOEM University,
amitesh9185@gmail.com
[6]S.S. Maniar College of Computer and Management, Nagpur
ssuhashinic@gmail.com

CAC reflects the dual importance of security and resource management because of the need to balance the intricacies of modern cloud environments in the interests of both security and proper resource management. Even though strong security mechanisms are needed to protect data and to ensure trust, efficient resource management is also crucial to maintain the performance and reliability of the cloud services. The quest for secure offloading and adaptive resource allocation increases the complexity of these environments, which requires more than simple strategies that can seamlessly integrate security with the management of resources without compromising either. This article showcases that the integration of advanced security measures, such as Sophos Security Certificates, affects resource utilization (CPU and bandwidth), offloading time, and completion of tasks. Nonetheless, the requirement for intensified security is well justified in application scenarios greatly dependent on protecting their data. The additional encryption and authentication operations generated by Sophos security guarantee a very low risk of breaches into the data, which is important to accomplish significant tasks related to sensitive matters in cloudlet-assisted computing environments.

Keywords: Security level, Sophos, SSL, Load Balancing, CAC, Cloudlet-Assisted Computing, Data Breach, Network Bandwidth.

1. Introduction

Two of the most prominent pillars that CAC needs to stand on for successful operation are security and resource management. In a world where cloud computing is being rapidly converted into the heart of modern digital infrastructure, smooth and secure access to resources is the paramount requirement. The dual importance of security and resource management in CAC cannot be emphasized enough because both components are crucial in ensuring the integrity and efficiency of cloud services. While security encompassed a wide variety of mechanisms such as encryption, authentication, and authorization aimed at protecting sensitive data and user privacy, resource management looked at the control of shared resources and assignment of appropriate rights for a seamless interaction among users and their applications in the cloud service. Resource management is about the way optimal computation resources, such as CPU, memory, and network bandwidth, need to be allocated to ensure the system operates efficiently and meets the performance requirements of both users and applications. In summary, these two aspects constitute the very backbone of CAC systems since a single type of imbalance or oversight can easily deteriorate security or result in inefficient utilization of resources.

2. Security Challenges in Resource-Constrained Environments

Data privacy and integrity are crucial in resource-constrained offloading environments because limited resources increase the likelihood of data breaches. Often, Sophos Security Certificates authenticate devices, ensuring that only the most trusted devices may securely offload tasks. Encryption protocols such as SSL/TLS, though essential for protecting data, add overhead and consume valuable CPU and bandwidth resources. Real-time security also represents a complexity because monitoring and catching threats drive pressure on systems, thereby raising the complexity of balancing robust security and efficient resource usage.

➢ Data Privacy and Integrity

Data offloading can inadvertently expose personal identifiers, financial records, and intellectual property, among other sensitive information, without appropriate security mechanisms in place. The threat is even more serious if offloading happens over insecure or public networks, as is often the case by default in resource-constrained environments. The goal, then, is to balance keeping data privacy robust with keeping resource utilization low. Such traditional mechanisms as encryption and integrity checking tend to be computationally expensive, hence they may introduce heavy overhead on already resource-constrained systems, which might degrade performance and slow down the task execution. This is why, in this kind of setting, efficient security protocols must be used to ensure data remains private throughout the offloading process even if the available computational resources are limited.

➢ Authentication and Authorization

Advanced authentication and authorization mechanisms come in through Sophos Security Certificates to reduce security risks and ensure that only accredited devices get to offload tasks. They are used for certification of devices by giving them a platform to identify trusted devices for offloading activities. Obviously, these certificates can be an effective lightweight solution for securing communications, access rights verification as well as protection of the latter from all the malicious threats in resource-constrained environments.

➢ Encryption Overhead

In resource-constrained environments, such additional CPU cycles for encryption may cause system performance degradation and increase the overall execution time for tasks. As an example, SSL/TLS encryption significantly consumes CPU resources in the process of establishing a safe connection, encrypting data before sending, and decrypting upon reception.

Another aspect is that the size of information is enlarged due to encryption protocols. This can lead to a proportionally increased consumption of network bandwidth, thus further exacerbating the resource constraints. This trade-off between security and performance thereby presents a more challenging problem in that organizations need to learn to deploy strong encryption without crippling system resources.

- **Real-Time Security**

Another major challenge provided by resource-constrained environments is ensuring real-time security. Real-time security is essential for the ability to monitor, detect, and response to security incidents in real time while still ensuring that the system continues to function with a good efficiency. Quick responses to potential threats are as vital as resource availability is limited. However, of course, the implementation of this type of real-time security, including continuous monitoring, threat detection and real-time encryption, often represents a need for additional cycles, memory allocation, and bandwidth.

3. Resource Management in Secure CAC Systems

The proper resource management in secure CAC systems dynamically allocates the available resources, such as CPU and memory, depending on security requirements, ensuring the support of high level encryption tasks. Load balancing distributes offloaded tasks amongst cloudlets while maintaining performance and security integrity by preventing resource bottlenecks. AI-based optimization further enhances resource management predict which demand comes for which type of task, giving priority to the most sensitive ones from security aspect thereby allowing efficient use of resources without compromising on the security of the system.

- **Dynamic Resource Allocation with Security Considerations**

Dynamic resource allocation in secure Cloud Access Control Systems would, therefore be crucial in finding a middle ground between security requests and system performance. Such dynamics allocations of resources like CPU, memory, and network bandwidth will be made dynamically so that the varying demands of the tasks undertaken can be sorted out with security as one of the top considerations.

- **Load Balancing**

Load balancing strategies are of paramount importance when it comes to the efficient management of resources in CAC systems, and especially in offload tasks. Load balancing distributes workloads across multiple cloudlets or nodes so that no single resource is overwhelmed; thereby ensuring that it maintains system performance and security integrity. The load balancers ensure offloaded tasks are balanced with regard to computational load and security.

- **AI-Powered Resource Optimization**

With an integration of AI-driven resource optimization, secure CAC systems are taking on a more optimized approach to their resource management. The amount of resource that would be needed can be estimated using machine learning models based on predictions of the pattern followed by the execution of tasks and security needs.

4. Literature Review

JasobantaLaha, et al. (2024) - Because load balancing reduces response times and guarantees resource utilization that is efficient, it is a crucial part of cloud computing. The available servers are effectively distributing the workload that is being received among them. Load balancing is the technique of dividing up a task among multiple internet-connected systems or resources. Load balancing prevents any one server or computer in a cloud computing environment from being overworked, underutilised, or idle by dispersing traffic and tasks. Traffic and workloads are distributed to achieve this. To raise the overall efficiency of the cloud environment, it optimises a range of attributes, including system stability, execution speed, and reaction time. The equitable allocation of workloads, traffic, and computing resources throughout the environment is the process of load balancing. This enhances the stability and effectiveness of cloud services. Our proposed method, Enhanced Dynamic Load Balancing for Cloud Computing, may adjust load distribution and keep the system balanced by taking into consideration factors such server capacity, job distribution, and system load.

Anamika Yadav, et al. (2024) - Providing resources that are both scalable and adaptable, cloud computing has emerged as an essential component of today's information technology infrastructure. On the other hand, owing to the fact that it is NP-hard, effective resource management, and cloudlet scheduling in particular, provides a substantial difficulty. This article presents a unique cloudlet scheduling technique that is based on heuristics. The program's goal is to reduce execution time and improve load balancing in cloud computing settings.

Hesham Abusaimeh (2022) - Due to their limited resources, mobile devices' batteries, processors, storage, and bandwidth are strained as a result of having to calculate an increasing amount of data locally. That's why it's best to use an edge cloud server near the mobile device to handle compute-intensive tasks. The necessity to implement offloading strategies to overcome mobile devices' limitations gave rise to the domain of mobile cloud computing, more commonly known as MCC.

Wael Hadeed and Dhuha Basheer Abdullah (2022) - Owing to the limited resources available to edge devices, it is critical to keep an eye on how those resources are currently being used as well as the algorithms that assign them to the devices. Based on their priority, these algorithms are in charge of sending containers to cloud and edge nodes. To lessen the strain on edge devices and enable the performance of mission-critical tasks, it might be necessary to relocate edge containers to a cloud platform.

ElaheFazeldehkordi and Tor-Morten Grønli (2022) -The IoT is a relatively new concept that has quickly become an integral part of contemporary life due to its wide range of potential uses. The number of devices being connected to the Internet of Things is constantly growing. However, there are several obstacles to overcome when moving the massive volumes of data produced by these IoT devices to the cloud.

Shilpa Mehta and HetalJoshiyara (2021) - The Internet has become into a necessary tool for daily communication. In terms of its impact on the process of modernising the digital world, it is more significant. Consequently, cloud computing has become one of the most exciting technological developments of the last few years. In order to guarantee smooth functioning, it seeks to make computer services available to millions of users worldwide. The workload distributions and system behaviour in the cloud environment are especially dynamic, which leads to load imbalances across the data center's resources. The load distribution among multiple systems is a critical component of cloud computing. This keeps certain nodes from becoming overburdened while others have almost nothing to do.

Ahmad AA Alkhatib, et al. (2021) - Due to numerous network innovations, a surge in network users, and the introduction of new technologies such as cloud computing and big data, traditional network management has become increasingly challenging. Both the amount of virtual machine (VM) load and the time needed to complete activities have increased on traditional networks. This necessitates a shift away from the conventional network architecture. In an effort to improve network management compliance, a new idea known as load balancing techniques has emerged in the field of network administration. The necessity for load balancing arises from the constraints placed on network resources and the imperative to fulfil requirements. Load balancing is a technique that helps distribute traffic among several resources, which improves the efficiency and dependability of network resources.

Nosharwhan Adil, Prince Waqas Khan, Yung-Cheol Byun (2020) - As a result of the broad proliferation of smartphones and other similar devices, as well as the expanding popularity of video streaming services, there has been a considerable surge in the amount of mobile data that has been used since lately. Cloud computing refers to the architectural design that allows virtual machines, cloud servers, hosts, and traders to collaborate in order to carry out any job that is accomplished in the cloud. The virtual machine migration has been identified as the main area of concern in the context of this section. The overhead of virtual machines results in an increase in the time needed to finish the work. The emergence of smartphones has been a significant contribution to the spectacular progress that has occurred in the field of information and communication technology over the last few years. However, the new technology was not without limitations, just like its forebears. When it comes to performance (computation), storage, and energy consumption, the portable gadgets that we refer to as smartphones confront a number of critical difficulties.

5. Integration of Sophos Security Certificates for Efficient Resource Usage

The Sophos Security Certificates are integrated efficiently so as to allow proper resource usage through secure offloading without considerable performance effect. That is, these certificates optimize encryption and decryption processes so as to minimize CPU and memory stresses associated with devices. Data security is robust, but optimal resource usage is ensured. Adaptive levels of security are also provided such that the encryption strength is sufficient to accommodate fluctuating resources resulting from different circumstances, hence not to affect the resource usage but assured of security. Other benefits of Sophos certificates include giving security guarantees by authenticating the devices and cloudlets, hence offloading tasks securely and preventing unauthorized access.

➢ Efficient Encryption and Decryption

Sophos Security Certificates contributes to secure offloading by efficiently handling the necessary encryption and decryption. With these certificates, encrypted data can pass safely without taking away too much from the usual overhead of performance on encryption. Sophos certificates operate through optimized cryptographic techniques with minimal demands of computational resources on the system that cut down computations when accessing encrypted data for encryption and decryption without compromise in data security. This ensures that the transmission of sensitive data is performed securely with minimal impacts on the CPU and memory resources, thus improving the overall performance of the system in resource-constrained environments.

- **Adaptive Security Levels**

Sophos Security Certificates also facilitate adaptive security levels, where encryption strength is dynamically adjusted based on resource availability. For example, when system resources like CPU or bandwidth are constrained, the system can lower encryption strength for non-sensitive tasks, prioritizing more robust encryption for critical data. This approach allows for a balance between security and resource efficiency, ensuring that security protocols remain effective without overwhelming system resources, particularly during periods of high demand or limited capacity.

- **Task Offloading with Security Guarantees**

While in offloading, Sophos certificates will enable security assurances as only authorized cloudlets receive tasks; therefore, devices and cloudlets will first be authenticated before providing their data for transmission. Thus, it is expected that unwanted access while in offloading is deterred as well as data tampering or interception. The security guarantees of integration provide Sophos certificates with an excellent strong framework in secure task offloading while at the same time maintaining resource efficiency.

6. Research Methodologies

This research assesses the effectiveness of security in the management of resources at Cloudlet-Assisted Computing. To achieve this, it follows the mode of analyzing different security levels (None, Basic, and Advanced using Sophos Security Certificates) in influencing offloading time, CPU usage, network bandwidth, and task completion times within the execution environment of a CAC setting. The study also investigates the relationship between security levels and data breach risks.

6.1. Dataset Construction

The key feature of this research is the construction of a dataset providing a basic basis for analysis in relation to how security measures impact resource management in CAC environments. Each one of these aspects of creating such a dataset is elaborated below:

I. Dataset Generation: In the experiment, a comprehensive dataset was designed with specific focuses on the offloading tasks' operations as part of its CAC framework. This dataset would comprise several dimensions in how a task was created or generated and then offloaded toward the cloudlets, which are referred to as smaller data centers or computing nodes helping in offloading tasks from the mobile devices or other endpoints.

II. Task Sizes: Tasks in this dataset differ in terms of sizes between 500 MB and up to 1000 MB. These range allow the study to consider operational scenarios under different task sizes, simulating a realistic setting where their size can differ distinctly. With the consideration of different task sizes, performance analysis could account for how security strategies, respectively, do under varying conditions of workload.

III. Security Levels: Three distinct security levels were applied to each task to evaluate their effects on performance metrics:

- **None:** These operations are performed in an insecure manner. This baseline scenario makes it possible to compare the resource consumption and performance metrics with those of other configurations that do employ security measures.

- **Basic:** In this category, basic encryption measures are applied. For example, access to tasks can be implemented using standard protocols such as SSL (Secure Socket Layer) providing a medium level of security. This will allow testing even the smallest security measure in using the resource and processing times for tasks.
- **Sophos Security Certificates:** This is for tasks that enforce strong encryption and security with the Sophos Security Certificates. This level of security is intended to maximize data protection and integrity, enabling the study to look at trade-offs between increased security and resource consumption.

IV. Key Metrics Recorded: For each of the offloading tasks, several key performance metrics were logged in detail for each, which allowed for extensive evaluations based on various security settings. The metrics are:

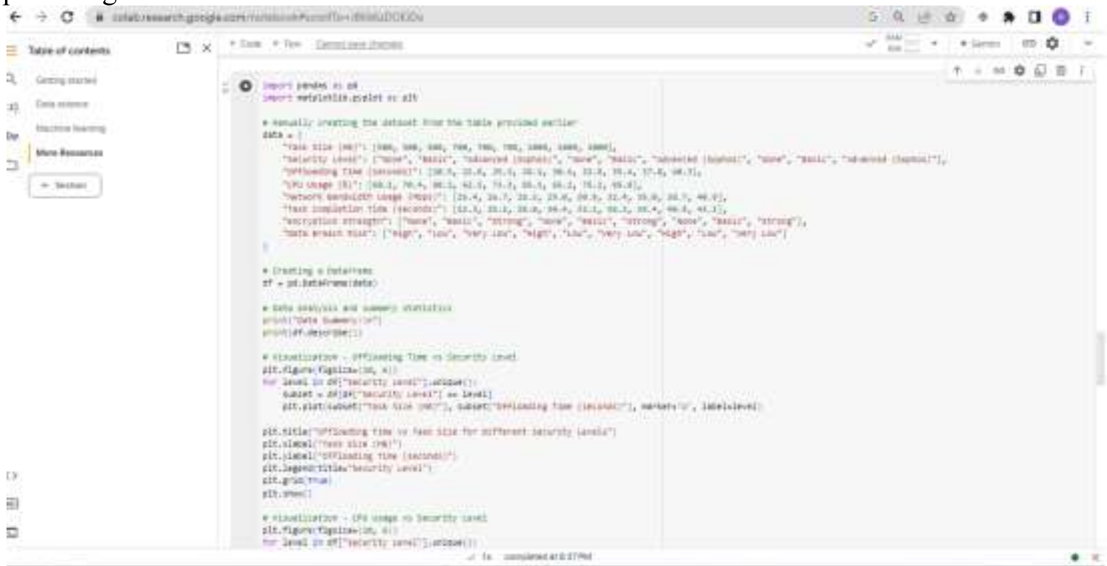
- Size of the Task (MB): Representing the size of data to be offloaded that translates to the size of processing requirements
- Security Level: Represents the security measures that have been applied to the task thus giving background to the next set of performance metrics.
- Offload Time in seconds: This measure offload time - It shows how long it takes to offload the task, and hence reveals the efficiency of the system for different levels of security configurations.
- CPU usage (%): This reflects the percent CPU resources consumed during the process of offloading the task, hence, reflecting a form of computational overhead associated with different levels of security.
- Offloading Network Bandwidth Usage (Mbps) : This records the bandwidth used when offloading, which is very important to know about the usage of network resources due to security measures.
- Total Time Task Completion in Seconds: This is actually the total time that is taken from the starting point to complete the execution of a task. It may include not only the offload time but other processing times as well.
- Encryption Strength: It is recorded as None, Basic, or Strong and captures the strength in terms of encryption applied to the tasks.
- Data breach risk: It indicates High, Low, and Very Low as the evaluation of the potential risks of data breaches to each security configuration.

7. Data Analysis

Data analysis indicates that stronger security in the cloudlet-assisted computing metrics significantly impacts performance while being executed. Offloading time increased approximately by 5 seconds upon the application of Sophos certificates since there is an overhead of encryption. CPU usage increased as unprotected computations were the least consumers of resources, while those under Sophos certificates needed the most. In a similar pattern, the network bandwidth usage increased with encryption and especially under Sophos certificates. The most time-consuming to complete was under the protection of Sophos; this would indicate that there is an added processing requirement. Thirdly, unprotected tasks were at the highest risk of data breaches, while with Sophos certificates in place, it dropped dramatically to "Very Low"; performance vs security trade-off.

7.1. Data Summary

Summarizing the performance metrics studied, we have the following table providing significant statistics obtained from the experimentation, highlighting a number of different performance metrics cloudlet-assisted computing. This has been processed and summarized in Python code, which allowed for easy calculation of mean, standard deviation, and percentages.



```
import pandas as pd
import matplotlib.pyplot as plt

# Manually creating the dataset from the table provided earlier
data = {
    "Task Size (MB)": [500, 500, 500, 700, 700, 700, 1000, 1000, 1000],
    "Security Level": ["None", "Basic", "Advanced (Sophos)", "None", "Basic", "Advanced (Sophos)", "None", "Basic", "Advanced (Sophos)"],
    "Offloading Time (seconds)": [20.5, 22.8, 25.3, 28.1, 30.4, 33.2, 35.4, 37.8, 40.3],
    "CPU Usage (%)": [60.1, 70.4, 80.2, 62.3, 73.3, 83.1, 65.2, 75.2, 85.8],
    "Network Bandwidth Usage (Mbps)": [25.4, 26.7, 28.3, 29.6, 30.9, 32.4, 35.0, 38.7, 40.9],
    "Task Completion Time (seconds)": [22.3, 25.2, 28.0, 30.4, 33.1, 36.2, 38.4, 40.5, 43.1],
    "Encryption Strength": ["None", "Basic", "Strong", "None", "Basic", "Strong", "None", "Basic", "Strong"],
    "Data Breach Risk": ["High", "Low", "Very Low", "High", "Low", "Very Low", "High", "Low", "Very Low"]
}

# Creating a DataFrame
df = pd.DataFrame(data)

# Data analysis and summary statistics
print("Data Summary:\n")
print(df.describe())

# Visualization - Offloading Time vs Security Level
plt.figure(figsize=(10, 6))
for level in df["Security Level"].unique():
    subset = df[df["Security Level"] == level]
    plt.plot(subset["Task Size (MB)"], subset["Offloading Time (seconds)"], marker='o', label=level)

plt.title("Offloading Time vs Task Size for Different Security Levels")
plt.xlabel("Task Size (MB)")
plt.ylabel("Offloading Time (seconds)")
plt.legend(title="Security Level")
plt.grid(True)
plt.show()

# Visualization - CPU Usage vs Security Level
plt.figure(figsize=(10, 6))
for level in df["Security Level"].unique():
```

Table7.1: Statistical Summary of Performance Metrics in Cloudlet-Assisted Computing

Metric	Task Size (MB)	Offloading Time (seconds)	CPU Usage (%)	Network Bandwidth Usage (Mbps)	Task Completion Time (seconds)
Count	9.000000	9.000000	9.000000	9.000000	9.000000
Mean	733.333333	30.377778	73.088889	31.922222	33.022222
Std	217.944947	6.806206	9.428739	5.347377	7.132457
Min	500.000000	20.500000	60.100000	25.400000	22.300000
25%	500.000000	25.300000	65.200000	28.300000	28.000000
50%	700.000000	30.400000	73.300000	30.900000	33.100000
75%	1000.000000	35.400000	80.200000	35.000000	38.400000
Max	1000.000000	40.300000	85.800000	40.900000	43.100000

Table 7.1 gives a comprehensive statistical summary of the most relevant performance metrics within a cloudlet-based computing framework obtained from nine different task runs including task size, offloading time, CPU utilization, network bandwidth usage, and task completion time. The average size of the task is around 733.33 MB. There is a standard deviation of 217.94 MB with considerable variability in the size of the tasks, where differences are really high. The mean offloading time is 30.38 seconds, which falls in the range of 20.50

to 40.30 seconds with a standard deviation of 6.81 seconds. The average CPU usage indicates 73.09%, ranging from 60.10% to a maximum of 85.80% with a moderate standard deviation of 9.43%. The average network bandwidth usage was 31.92 Mbps, ranging between 25.40 and 40.90 Mbps, and indicating stable usage patterns with a standard deviation of 5.35 Mbps. Finally, the average completion time of a task is 33.02 seconds; through this metric, the impact of security measures and task complexity are indicated on resource usages for efficiency in a cloudlet framework. Overall, data evidence indicates a close balance between the use of resources and the efficiency of tasks, information crucial in optimizing cloudlet-assisted computing systems towards superior efficiency and security.

7.2. Offloading Time Comparison

Differences in the offloading times for various security levels are seen by comparing the number of milliseconds taken to offload the task in the CAC environment. Table 7.2 Average Offloading Times for Different Security Levels.

Table 7.2: Offloading Time Comparison by Security Level in Cloudlet-Assisted Computing

Security Level	Offloading Time (Average)
None	27.97 seconds
Basic	30.33 seconds
Advanced (Sophos)	32.80 seconds

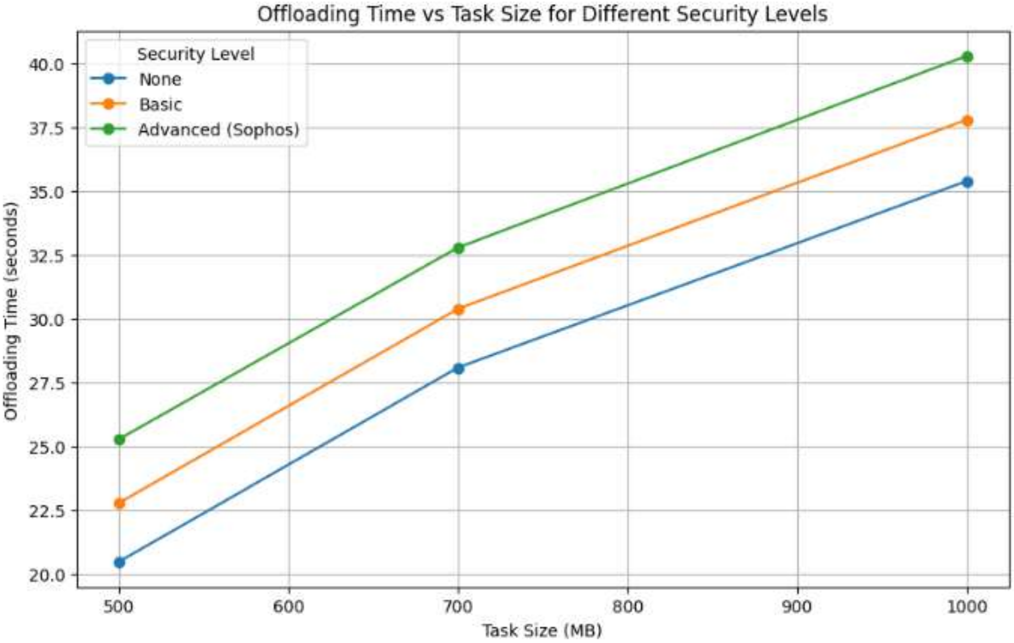


Chart 7.1: Offloading Time Performance Analysis

Data is strongly indicative of tasks offloaded without any security measures taking the least time of about 28 seconds. Introducing basic security measures raises the average time taken to offload to about 30 seconds, which implies that the minimal encryption and authentication steps do contribute to some delay. Using higher security measures, Advance with Sophos certificates, offloading time is increased up to 32.80 seconds. The reason behind its increase in offloading time is that due to additional encryption and authentication processes considered during offloading, these add more overhead and complexity in offloading.

7.3. CPU Usage Comparison

The graph for CPU utilization comparison explains how the processing power varies with the different security levels because they affected the execution of tasks in the Cloudlet-Assisted Computing environment. Table 7.3 represents an average CPU utilization for different security levels.

Table 7.3: CPU Usage Comparison by Security Level in Cloudlet-Assisted Computing

Security Level	CPU Usage (Average)
None	62.6%
Basic	73.0%
Advanced (Sophos)	83.7%

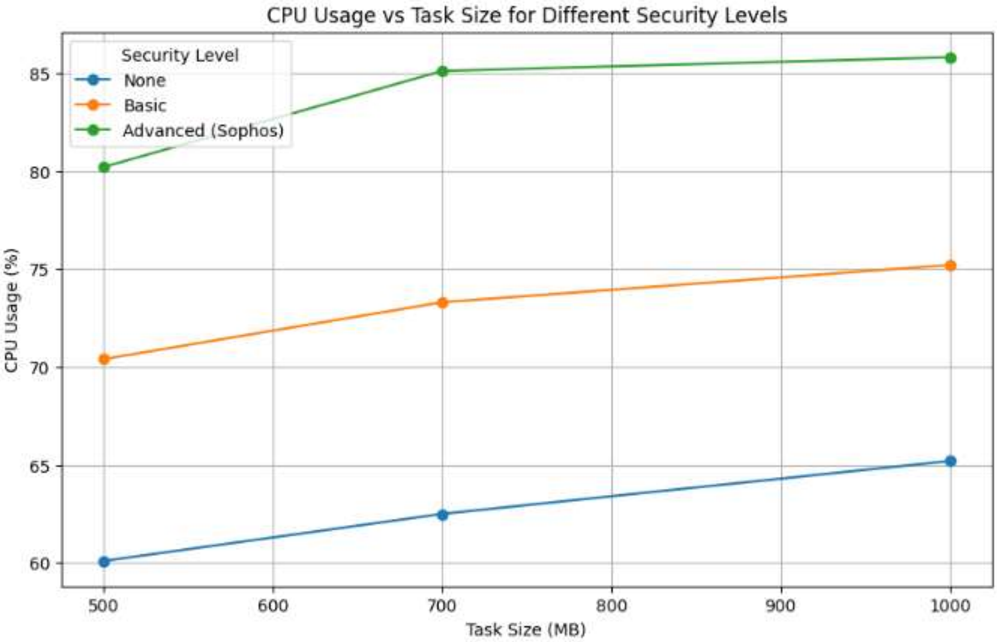


Chart 7.2: CPU Usage Performance Analysis

The statistics reveal that if no security features were in place, then the CPU usage is very low, and stands at 62.6%. When the level of basic security is in place, then the CPU usage shoots up to 73.0 percent, which reflects moderate increases across the computational requirements associated with the basic encryption and authentication processes. The maximum increase is observed at the advanced security level where both the Security Certificates by Sophos have the CPU usage to be at 83.7 percent on average. This is thus due to more complex and resource-intensive processes needed by stronger encryption and measures for enhanced security.

7.4. Network Bandwidth Usage

Figure 7.3 demonstrates how network bandwidth usage varies with various security levels for a CAC environment. Table 7.4 shows the average network bandwidth usage for varying levels of security.

Table 7.4: Network Bandwidth Usage by Security Level in Cloudlet-Assisted Computing

Security Level	Network Bandwidth Usage (Average)
None	29.80 Mbps
Basic	32.10 Mbps
Advanced (Sophos)	33.87 Mbps

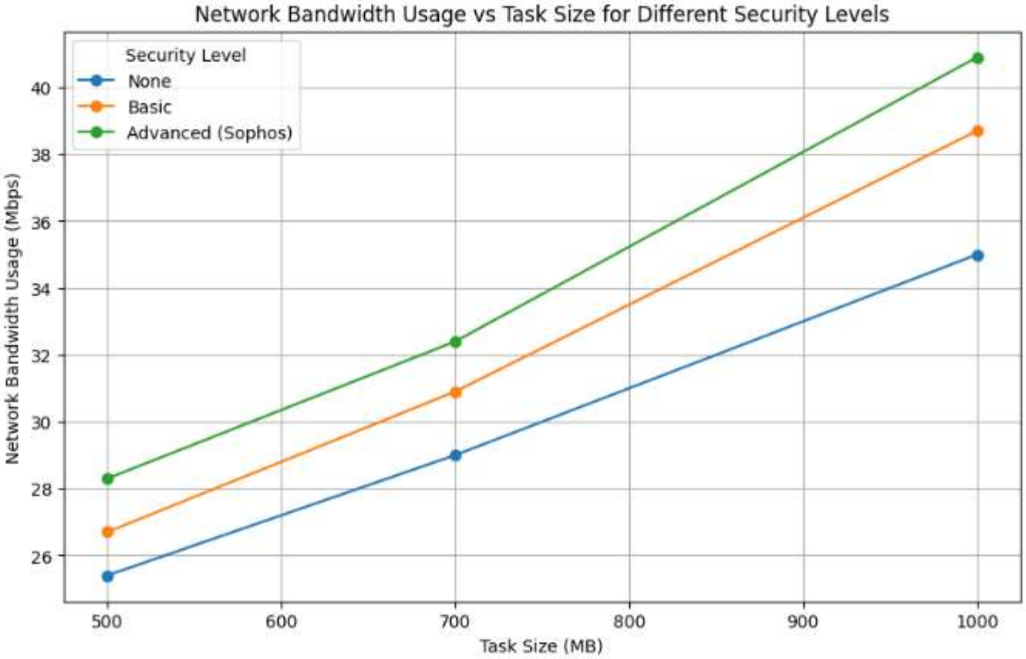


Chart 7.3: Network Bandwidth Usage Performance Analysis

As the statistics depict, with zero security, the average bandwidth utilization of the network is 29.80 Mbps. When the basic measures of security are incorporated then the bandwidth utilization is stretched to 32.10 Mbps, which indicates the overhead involved in encryption besides the integrity check of the data. The greatest increment is seen with the Advanced level of security, especially when Sophos Security Certificates are used. It brings up the average bandwidth utilization to 33.87 Mbps. This can be attributed to the implementation of more sophisticated encryption protocols that demand higher bandwidth for the extra data overhead that these encryption processes create.

7.5. Task Completion Time

The comparison of task completion time gives insight into the manner in which the various security levels affect the overall time taken to complete a task within a CAC environment. The average task completion times for various security levels are presented in table 7.5.

Table 7.5: Average Task Completion Time by Security Level in Cloudlet-Assisted Computing

Security Level	Task Completion Time (Average)
None	30.37 seconds
Basic	33.07 seconds
Advanced (Sophos)	35.80 seconds

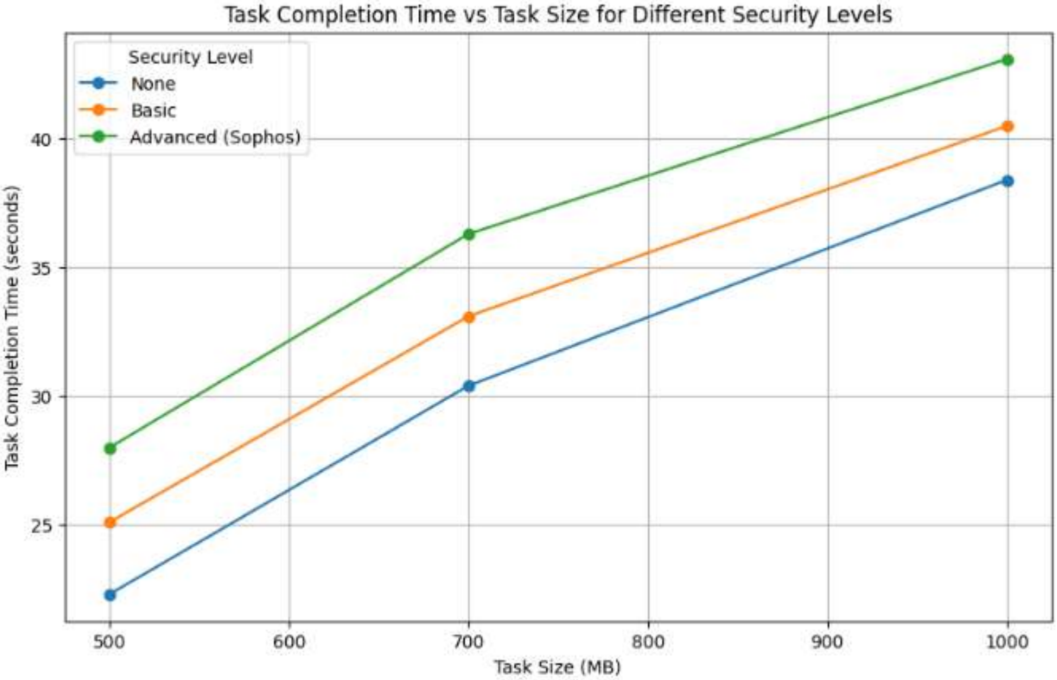


Chart 7.4: Task Completion Time Performance Analysis

The least time is for tasks accomplished without any security measures at an average of 30.37 seconds. Since more security measures are being introduced, the amount of time taken to complete the tasks goes up. Basic security measures increase the average time required to complete the task up to 33.07 seconds, therefore showing that additional checks and protocols take some processing time. The Advanced security level adds the largest amount of time interval, and especially when using Sophos Security certificates, the average finish is 35.80 seconds. The system likely still utilized a longer amount of processing and encryption to help increase security, thus providing both security and efficiency in completing the tasks.

7.6. Data Breach Risk

It can be noted that the comparison of risk due to data breach highlights the relationship in between the different security levels and the risk associated with such data breaches in a CAC environment. Table 7.6 shows the various levels of risk associated with different security configurations.

Table 7.6: Data Breach Risk Associated with Different Security Levels in Cloudlet-Assisted Computing

Security Level	Data Breach Risk
None	High
Basic	Low
Advanced (Sophos)	Very Low

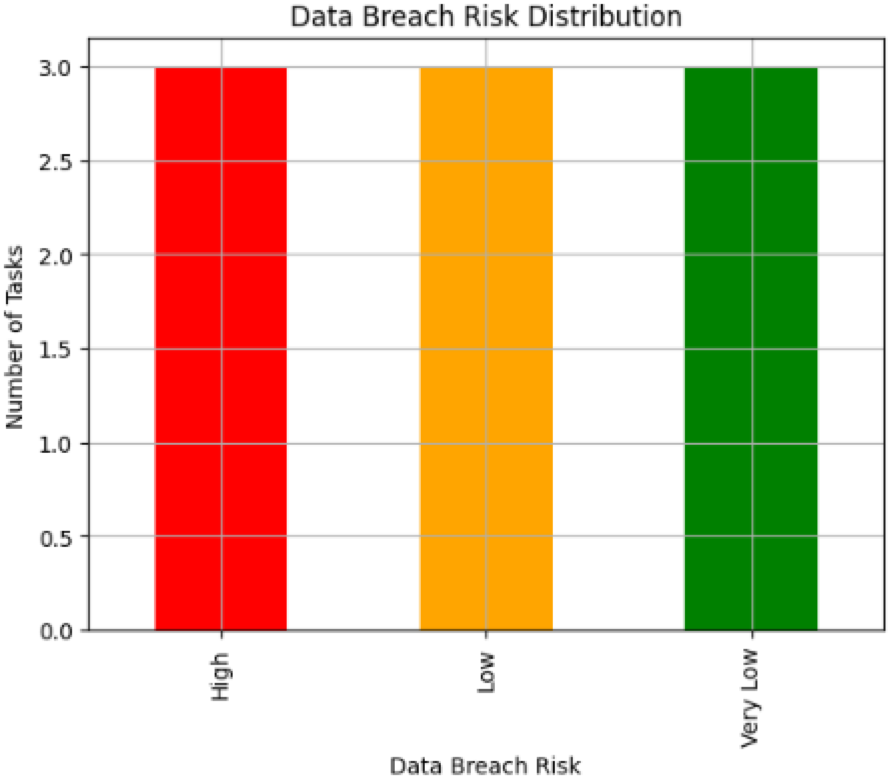


Chart 7.5: Distribution of Data Breach Risks

From this information, it can be noted that tasks processed without security controls are labeled as "None," which thereby is exposed to a high possibility of data breaches. That is, though it performs quite good as far as processing speed and resources usage are concerned, sensitive data would remain open to attack or unauthorized access. The Basic Security measures applied result in low risk of data breach, meaning that some risk is offered, though never foolproof. An advanced security measure applies the greatest risk reduction; especially when the Sophos Security Certificate are used, resulting in very low risk. This would increase the security level of breaches but would result in increased resource usage and more prolonged processing time. In any case, it does make an important point about how there is an intricately fine balance between performance at the top level and having security provisions in place to safeguard sensitive data inside a CAC system.

7.7. Results and Discussion

The final results will be summarized based on the analysis as well as on the visualizations provided by the Python code in the following key areas: Offloading Time, CPU Usage, Network Bandwidth Usage, Task Completion Time, and Data Breach Risk. The examples emphasize trade-offs between performance and security in CAC environments.

7.7.1. Offloading Time vs. Security Level

While performing the analysis of specific task scenarios, the fastest offloading times were realized in the tasks that did not apply security measures. For example, in a 500 MB task where no security measure was applied on it recorded nearly about 20.5 seconds to offload it, while when processed with the Sophos security certificates, the offloading time took nearly 25.3 seconds. Such an increase highlights the role that security measures have in affecting task performance, especially the delay by encryption algorithms and necessary verification steps for ensuring integrity and confidentiality of data.

7.7.2. CPU Usage vs. Security Level

For instance, in processing a 500 MB job, without any security measures being deployed, the CPU utilization stood at around 60.1%. Then after deployment of the job with Sophos security certificates, the CPU utilization shoots up to a staggering 80.2%. It can therefore be drawn that advanced security measures indeed possess a resource-consuming nature since they consume much more computational power to perform encryption and decryption processes, and in the process of authenticating.

7.7.3. Network Bandwidth Usage vs. Security Level

Even at such a low level of task size, as noted from the previous sections, an example is witnessed while working with a 700 MB task with nearly 29.0 Mbps used bandwidth without using any security certificates. In return, the same task requires around 32.4 Mbps with the help of security certificates from Sophos. This equilibrium shows not just the original data but rather related metadata and overhead that would be sent through encryption to maintain it at the set security level.

7.7.4. Task Completion Time vs. Security Level

For instance, the same 1000 MB job that had no security measures at all took about 38.4 seconds. The same job secured with Sophos certificates took 43.1 seconds to complete. This is a difference of 4.7 seconds, thus easily figuring out extra processing time that needs to encrypt and decrypt data and the probable extra overhead on overall throughput and performance.

7.7.5. Data Breach Risk

In particular, those activities which are not secured are rated as "High", while those that utilize Basic security are rated as "Low". The difference is indeed striking when comparing those with tasks secured by means of Sophos certificate, which is rated as "Very Low" - with the super effectiveness that more advanced security will bring in the terms of mending potential threats and vulnerabilities.

8. Conclusion

The trade-off in security and resource management in Cloudlet-Assisted Computing is, after all, quite inevitable. Though more stringent security measures, such as Sophos Security Certificates are advisable for avoiding security breaches, offloading time overheads are particularly on the higher side in the form of CPU usage, network bandwidth consumptions, and the time taken to complete a given task. However, the strength of security against data breach is incredibly enhanced.

Key takeaways in the analysis are:

- Security or Performance: This raises an issue of explicit trade-off between security and performance. The organizations are required to balance needs for high-strong data protection against the performance demands of real-time or latency-sensitive applications.
- Resource Management: Resource-constrained environments require careful resource allocation and management, especially in terms of secured task management. Systems should have priorities on tasks developed according to their sensitivity and needs.
- Security Deployment: More critical data needs stronger security certificates such as Sophos Security Certificates, but there should be an optimization so that there is minimal system performance degradation.

The importance of this analysis is in its contribution to the understanding of how security affects the related resource management and offloading performances in CAC environments. The outcomes could guide future deployment decisions on whether securing resources within a cloudlet environment or consuming resources with maximum protection to data.

This data analysis showcases that the integration of advanced security measures, such as Sophos Security Certificates, affects resource utilization (CPU and bandwidth), offloading time, and completion of tasks. Nonetheless, the requirement for intensified security is well justified in application scenarios greatly dependent on protecting their data. The additional encryption and authentication operations generated by Sophos security guarantee a very low risk of breaches into the data, which is important to accomplish significant tasks related to sensitive matters in cloudlet-assisted computing environments.

From the analysis, organizations that employ CAC need to maintain an excellent balance between security and performance by adopting complex security mechanisms such as Sophos for sensitive data jobs while employing less resource-consuming measures for other tasks.

REFERENCES

1. Abusaimeh, H. (2022). Computation Offloading for Mobile Cloud Computing Frameworks and Techniques. TEM Journal, 11(3), 1042-1046.
2. Adil, N. O. S. H. A. R. W. H. A. N., Khan, P. W., & Byun, Y. C. (2020). Performance Enhancement through Communication Offloading for Energy Efficiency on Mobile Cloud Computation. Int. J. Sci. Technol. Res, 9, 186-194.
3. Al-Saleh, Y., Sabico, S., Al-Furqani, A., Jayyousi, A., Alromaihi, D., Ba-Essa, E., ... & Al-Daghri, N. M. (2021). Sulfonylureas in the current practice of type 2 diabetes management: are they all the same? Consensus from the Gulf Cooperation Council (GCC) countries advisory board on sulfonylureas. Diabetes Therapy, 12(8), 2115-2132.
4. Babar, M., Khan, M. S., Ali, F., Imran, M., & Shoaib, M. (2021). Cloudlet computing: recent advances, taxonomy, and challenges. IEEE access, 9, 29609-29622.
5. Baraki, H., Jahl, A., Jakob, S., Schwarzbach, C., Fax, M., &Geihs, K. (2019). Optimizing applications for mobile cloud computing through MOCCAA. Journal of Grid Computing, 17(4), 651-676.
6. Boukerche, A., Wu, Q., & Sun, P. (2019). Efficient green protocols for sustainable wireless sensor networks. IEEE Transactions on Sustainable Computing, 5(1), 61-80.
7. Chen, M., Guo, S., Liu, K., Liao, X. and Xiao, B. (2020), 'Robust computation offloading and resource scheduling in cloudlet-based mobile cloud computing', IEEE Transactions on Mobile Computing 20(5), 2025–2040.
8. Fazeldehkordi, E., & Grønli, T. M. (2022). A survey of security architectures for edge computing-based IoT. IoT, 3(3), 332-365.
9. Gayathri, S., & Aarthy, D. K. (2022). Computer-Aided Detection of Malignant Mass in Mammogram Using U-Net Architecture. In Artificial Intelligence and Evolutionary Computations in Engineering Systems: Computational Algorithm for AI Technology, Proceedings of ICAIECES 2020 (pp. 179-185). Springer Singapore.
10. Guan, S., Boukerche, A. and Loureiro, A. (2020), 'Novel sustainable and heterogeneous offloading management techniques in proactive cloudlets', IEEE Transactions on Sustainable Computing . in press.
11. Hadeed, W., & Abdullah, D. B. (2022). Load Balancing Mechanism for Edge-CloudBased Priorities Containers. Int. J. Wirel. Microw. Technol, 12, 1-9.
12. Haibeh, L. A., Yagoub, M. C., &Jarray, A. (2022). A survey on mobile edge computing infrastructure: Design, resource management, and optimization approaches. IEEE Access, 10, 27591-27610.
13. Haq, N. A., &Sarvagya, M. (2020, February). Analysis on Channel Parameters and Signal Processing methods at mm-wave for 5G networks. In 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC) (pp. 1-6). IEEE.
14. Husnain, M., Khalid, A., & Shafi, N. (2021, April). A novel preprocessing technique for toxic comment classification. In 2021 International Conference on Artificial Intelligence (ICAI) (pp. 22-27). IEEE.
15. Inupakutika, D., Akopian, D., Chalela, P., & Ramirez, A. G. (2020). Performance analysis of mobile cloud computing architectures for mHealth app. Electronic Imaging, 32, 1-7.

16. Islam, A., Kumar, A., Mohiuddin, K., Yasmin, S., Khaleel, M. A., & Hussain, M. R. (2020). Efficient resourceful mobile cloud architecture (mRARSA) for resource demanding applications. Journal of Cloud Computing, 9, 1-21.
17. Mehta, H. S., &Joshiyara, H. (2021). Load Balancing in Cloud Computing: A Comprehensive Survey on Recent Techniques. Int. J. Adv. Trends Comput. Sci. Eng, 10.
18. Shafiq, D. A., Jhanjhi, N. Z., Abdullah, A., & Alzain, M. A. (2022). A load balancing algorithm for the data centres to optimize cloud computing applications. IEEE Access, 9, 41731-41744.
19. Shaik, S. P. (2020). Enhancing Cloud Computing Security Through Deep Learning: An Artificial Neural Network Approach.
20. Somu, N. L., & Peddi, P. (2021). An Analysis Of Edge-Cloud Computing Networks For Computation Offloading. Webology (ISSN: 1735-188X), 18(6), 7983-7994.
21. SomulaRamasubbareddy., and Sasikala, R. (2019). A honey bee inspired cloudlet selection for resource allocation. In Smart Intelligent Computing and Applications (pp. 335-343). Springer, Singapore.
22. SomulaRamasubbareddy., and Sasikala, R. (2019). A load and distance aware cloudlet selection strategy in multi-cloudlet environment. International Journal of Grid and High Performance Computing (IJGHPC), 11(2), 85-102.
23. SomulaRamasubbareddy., and Sasikala, R. (2019). A research review on energy consumption of different frameworks in mobile cloud computing. In Innovations in Computer Science and Engineering (pp. 129-142). Springer, Singapore.
24. SomulaRamasubbareddy., and Sasikala, R. (2019). RTTSMCE: a response time aware task scheduling in multi-cloudlet environment. International Journal of Computers and Applications, 1-6.
25. SomulaRamasubbareddy., and Sasikala, R. (2021). CAVMS: Application Aware Cloudlet Adaption and VM Selection Framework for Multi-Cloudlet Environment. IEEE Systems Journal, 15 (4), 5098-5106.
26. Sophos Group Plc. (2021). Sophos Security White Paper: Encryption and Data Protection. Sophos.
27. Uma, D., Udhayakumar, S., Tamilselvan, L., & Silviya, J. (2020). Client aware scalable cloudlet to augment edge computing with mobile cloud migration service.
28. Xu, X., Chen, Y., Yuan, Y., Huang, T., Zhang, X., & Qi, L. (2020). Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing. Multimedia Tools and Applications, 79, 9819-9844.
29. Yadav, Anamika & Varshney, Hridesh & Kumar, Sarvesh. (2023). Intelligent Cloudlet Scheduling for Optimized Execution Time in Cloud Computing Environments. Journal of Computers, Mechanical and Management. 2. 14-21. 10.57159/gadl.jcmm.2.5.23074.