WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Offloading Methodology Based on Optimization for Mobile Cloud Computing

[1]Yaduvendra Singh, [2]Prof. Unmukh Datta

[1,2]Computer Science, Maharana Pratap College of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya

ABSTRACT -

Cloud Computing is widely utilized in today's internet age. It is evident that Cloud Computing serves as an effective solution to meet the computational, memory, and energy requirements of smartphones. The significance of Cloud Computing in mobile devices has led to the emergence of a new field known as Mobile Cloud Computing (MCC). Recently, Mobile Cloud Computing has received significant attention from both academic and industrial fields. In mobile Cloud Computing applications, the primary concerns are security and privacy, which still face significant challenges. Mobile computing is a technology through which we can transfer data such as voice, text, video etc. from one mobile to another mobile without any physical connection i.e. without any wire. We can understand this with our example like I live in Delhi and my friend lives in Mumbai, if I want to send a video or a photo or a text message to my friend, then I can send it easily. But it is worth thinking that when data is being sent from one mobile to another, during that time there is no physical connection between the two mobiles, both the mobiles are not connected in any wire. So it means that because of mobile computing we can send data from one mobile to another mobile, be it of any type, whether it is text, audio, video or any photo. All this work is possible only because of mobile computing technology, because of which data transmission is possible, without any physical connection. MCC enhances mobile devices' energy efficiency and resourcefulness by enabling applications to offload resource-heavy computational tasks to cloud computing resources. By delivering optimal services to mobile users, MCC integrates the components of mobile networks and cloud computing. In mobile cloud computing, all data and complex computing modules can be processed in the cloud, which alleviates the necessity for mobile devices to have powerful configurations such as CPU speed and memory capacity. MCC marks a new phase in the integration of mobile devices with Cloud Computing to form a new foundation. Nonetheless, mobile devices face numerous challenges concerning their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., privacy, mobility, and security). It is a fusion of mobile computing, Cloud Computing, and wireless networks that provides outstanding computational resources to network administrators, mobile users, and Cloud Computing providers.

I. INTRODUCTION

The Cloud Computing environment offers significant flexibility and availability of computing resources. This recent technological advancement marks the beginning of a new era of e-services across various fields. Cloud Computing refers to the provision of computing services, which encompass servers, storage, databases, networking, software, analytics, and intelligence, delivered over the Internet (referred to as 'the cloud') to facilitate quicker innovation, adaptable resources, and economies of scale. Cloud Computing [1][2] is widely utilized in numerous sectors. The integration of Cloud Computing with Mobile Devices has given rise to a new field known as Mobile Cloud Computing (MCC) [3][4], which provides advantages for mobile users, network providers, and Cloud providers alike. Mobile devices encounter several challenges regarding their resources (such as battery life, storage, bandwidth, etc.) and communications (including privacy, mobility, and security). MCC offers mobile users data storage and processing services in the cloud, eliminating the necessity for a high-performance device configuration, such as CPU speed and memory capacity, since all resource-intensive computing tasks can be executed in the cloud. Recently, MCC has garnered considerable interest in both academic and industrial circles [5][6].

The swift expansion of mobile devices and wireless networking has compelled many services to be accessible via these devices. Cloud Computing is revolutionizing the infrastructure of Internet computing. Given that the majority of services will be accessed from the cloud through the Internet, Mobile Cloud Computing has been introduced. In recent years, advancements in information technology have propelled the world towards network-based computing. An increasing number of users are seeking applications and services from the Internet. This remarkable growth and demand for applications have led to the emergence of the concept of Cloud Computing [1]. Cloud Computing heralds a new era in Internet development, encompassing the provision of application services, software services, and hardware services over the Internet. Technically speaking, it consists of a cluster of servers or personal computers organized to deliver the aforementioned services on the Internet. Since 2007, Cloud Computing has emerged as a significant research topic within both scientific and industrial communities. Mobile Cloud Computing is a branch of Cloud Computing and it is generated from Cloud Computing itself. In this we will learn about the privacy of data and its security. Information about computation offloading in mobile cloud computing will also be obtained and in this research work, a type of model will be created in which the privacy and security of the donor can be assured so that it is known that the data we store is highly confidential. Mobile cloud computing is also known as MCC. It comes under this that the processing of data and

the storage of data all happen on cloud servers. And here the mobile works like an intermediate device and this means that it displays or shows your data on its screen. This data is processed from the cloud server itself and is loaded from there and displayed on the mobile screen, so it is the provider of the cloud itself which fetches and shows the mobile on its screen. There can be some different types of different cloud resources in cloud computing, out of which some selected cloud resources will be described here and information related to them will be given. Mobile cloud computing consists of mobile devices, so imagine that we have two devices, one of which is the mobile device at the top and the other mobile device is at the bottom of the network. So here are two different mobile devices with their own different mobile network services. Let's say there are two different mobile networks which are associated with different companies, let's say there is a company A whose mobile network is above and there is a company B whose mobile network is below. There are two mobile networks. This is a mobile network and also a mobile network. Each mobile network will have its own mobile devices. At least 4 to 6 mobile devices will be near each mobile network. The user accesses these mobile devices only and uses them within his own mobile network. Like there are 6 devices in mobile network A and there are 6 mobile devices in mobile network B too. With the help of these mobile networks, the user tries to access the data stored on the cloud and also accesses his applications located on the cloud and displays the data and after fetching it, shows it on the mobile screen.

II. LITERATURE REVIEW

Research Papers :

- Huber Flores et al. [21] examined the difficulties and possibilities presented by a new form of mobile architecture, referred to as evidence-aware mobile cloud architecture, which depends on crowd sensing to identify the best configuration for migrating mobile functionality to the cloud. The essential insight is that by utilizing the vast parallel infrastructure of the cloud to process large datasets, it is achievable to collect offloading evidence from numerous devices, which is later analyzed to infer an effective configuration for running a smartphone application on a specific device.
- Yiran Shen et al. [22] proposed an innovative cloud-enabled and Privacy-preserving sparse representation classification (P2-SRC) system aimed at ensuring the privacy of both the "data contributors" and "application users" when the cloud server is untrustworthy. In contrast to leading-edge approaches that only address threats to data values, the P2-SRC system confronts multiple forms of privacy threats, including Content Privacy Attacks, Source Privacy Attacks, and Label Privacy Attacks.
- Dazhi Li et al. [23] developed a model to represent the interactions between virtual authentication coordinators, the authentication broker, and mobile users as a three-stage game. In this model, each participant strives to maximize their own utility, with trust allocation being facilitated through G value learning. Numerical findings indicate that the proposed certificate-aware framework is effective, allowing all participants to enhance their utilities and increase the trust level within Mobile Computing systems.
- Yi Liu et al. [24] introduced a fine-grained E-Healthcare Record (EHR) access control scheme that has been demonstrated to be secure within the standard model, based on the decisional parallel bilinear Diffie-Hellman exponent assumption. In this scheme, an EHR owner is capable of generating offline ciphertexts prior to acquiring knowledge of the EHR data and access policies, thereby executing the majority of computational tasks. Additionally, the online phase can swiftly compile the final ciphertexts once the EHR data and access policies are available.
- Durbadal et al. [25] sought to develop an authentication protocol that addresses the security vulnerabilities present in current protocols. The proposed protocol introduces a dynamic password-based two-server authentication and key exchange mechanism utilizing both public and private key cryptography. Additionally, to ensure a robust user anonymity feature, a novel multi-factor authentication scheme that preserves identity has also been implemented. The security evaluation, which includes both formal security analysis using the widely-accepted Real-Or-Random (ROR) model and informal security assessments, indicates that the proposed protocol effectively defends against several recognized attacks.
- Yinhao Jiang et al. [26] presented a new approach to improve Ciphertext Policy-Attribute Based Encryption (CP-ABE) schemes, which offer safeguards against the issue of key-delegation abuse. The authors define the security requirements necessary for this property and subsequently develop a CP-ABE scheme that meets these new security standards.
- Alberto Ceselli et al. [27] have put forward a general data-driven framework intended for application use, which comprises an optimization core, a data pre-processing module, and a validation module to evaluate the accuracy of plans. This optimization core involves a combinatorial issue that is a multi-period variant of the Generalized Assignment Problem: this research formulates a Branch-and-Price algorithm that, despite being exact in nature, also performs admirably as a metaheuristic when integrated with early stopping. Comprehensive experiments conducted on both synthetic and real-world datasets indicate that the proposed strategy is both computationally efficient and accurate when applied to prospective analytics.

Pelin Angin et al. [28] have introduced a context-dependent computation offloading model for Mobile Cloud Computing (MCC), which is based on application segments organized into autonomous agents. This strategy requires only isolated execution containers in the cloud to establish a runtime environment for the agents, with minimal involvement from the mobile platform during the computation process. The agents in the proposed framework are designed to protect themselves from tampering through integrity-check pointing and a communication mechanism that utilizes authenticated encryption.

- Chiba, Zouhair et al. [51] provided a comprehensive overview of various intrusions in the cloud, along with the different detection techniques employed by Intrusion Detection Systems (IDS) and the categories of Cloud Computing-based IDS. Subsequently, the authors examined several relevant existing cloud-based intrusion detection systems, focusing on their types, positioning, detection time, and data sources. This analysis also highlights the strengths and limitations of each system to assess their ability to meet the security requirements of the Cloud Computing environment.
- Chiba, Zouhair et al. [52] introduced a Cooperative and Hybrid Network Intrusion Detection System (CH-NIDS) designed to identify network attacks within the cloud environment by monitoring network traffic while ensuring performance and service quality. The authors implemented Snort as a signature-based detection method for recognizing known attacks, and utilized a Back-Propagation Neural Network (BPN) for detecting network anomalies.
- Saadi, Chaimae et al. [53] introduced a novel cloud infrastructure architecture that integrates IDS-based mobile agents and employs three varieties of honeypots to identify attacks, analyze attacker behavior, enhance the value of honeypots and IDS-based mobile agents, address limitations in intrusion detection systems, and improve IDS knowledge bases, thereby increasing the detection rate within the cloud environment.
- Puthal, Deepak et al. [54] asserted that emerging applications in the domains of smart healthcare, smart cities, and precision agriculture are utilizing Internet of Things (IoT) sensing devices to gather data, which is then transmitted to remote Cloud Data Centers for analysis, including fusion, storage, and processing. The lifecycle of big data analytics, commencing with the collection of raw data and progressing to data analytics and decision-making, necessitates the intelligent coordination of activities among small IoT sensors, IoT gateways, and in-transit network devices located in an Edge Data Center (EDC), alongside the big data processing frameworks and hardware resources situated in extensive Cloud Data Center (CDC) farms.
- "Mobile cloud computing principles & paradigms by Abhirup khanna & Sarishma." This book has well researched and analyzed the topic of mobility management and this topic has been explained in detail very well. Mobility management of mobile cloud computing is a big challenge. It should be completed very wisely and this shortcoming should be removed because mobility management can be a very different issue for any person who wants to use mobile cloud. Whenever we use mobile cloud computing, we access it in the mobile itself and if we hold the mobile in our hand and are walking somewhere or traveling by car, then it is connected to the mobile network. It is his responsibility to connect to different networks. The cloud which is located in different networks should be connected to the network of the cloud, it should be connected to the particular mobile. And the services should be provided through mobile cloud computing because the data inside the cloud should be accessed, fetched and shown on the mobile screen. Here, due to this, the congestion of communication has also increased a lot because just as there is congestion of data, similarly there is congestion of communication too. As data traffic increases, when data is accessed through any Wi-Fi or broadband network, data congestion increases. Because data traffic increases, the data speed starts slowing down. Reason why internet runs very slowly. If many people are trying to run the Internet on the same network or try to access the Internet on the same network, then data congestion will increase, the load will increase and the Internet will start working very slow due to which many people will be Inconvenienced. Similarly, in today's time, every person has a mobile and the congestion of mobile is increasing, due to this the communication congestion or communication traffic also increases manifold. Due to which the mobile has to face difficulty in establishing communication with different types of networks because many people want to connect to the same communication at the same time. And due to this communication, the traffic of the mobile increases, the traffic load of the mobile communication increases due to which it is not able to work properly and due to this, the communication traffic of the mobile increases and it gets lost.

III. METHODOLOGY

Research Methodology :

The suggested methodologies for improving security within the Security and Privacy modules of Mobile Cloud Computing architecture. In the security module, the user authentication is enhanced through the proposed Optimized Elliptical Curve Cryptography (O-ECC) method, access control is improved via the proposed Data Sensitivity – Similarity based Access Control (DSSBAC) mechanism, intrusion detection is facilitated by the proposed Hybrid Classification Model, and the proposed Offloading method is employed to enhance security by minimizing task allocation time. In the privacy module, user data encryption is managed by the proposed O-ECC technique, which reduces the time required for both encryption and decryption. The proposed DSSBAC mechanism is utilized to safeguard user sensitive data.

Problem Statement :

Mobile Cloud Computing (MCC), which represents the evolution and expansion of Mobile Computing and Cloud Computing, has adopted both mobility and scalability. In light of its extensive applicability, it has emerged as a prominent area of research in recent years. However, several security-related challenges in MCC remain, as outlined below.

1) The allocation of CloudLets to users in MCC is characterized by significant time consumption, and the offloading strategy in MCC demands increased battery power, along with a strict deadline for each individual task on the available mobile device.

2) There is an absence of an efficient and rapid authentication scheme between the cloud and its users.

3) User data security within the cloud environment is insufficiently addressed.

4) There is a deficiency in techniques for detecting intrusions affecting both the cloud and mobile users.

Motivation :

The progress in mobile technology has facilitated the execution of complex computational tasks on the latest smartphones. However, Smart Mobile Devices (SMDs) exhibit lower processing speeds compared to laptops and other electronic devices, rendering them inadequate for performing intricate mathematical calculations and computations. Due to constraints in hardware and software configurations, limited battery life, storage capacity, and processor speed, Smart Mobile Devices possess diminished potential and capability. These limitations can be addressed through the implementation of cloud computing, which inspires the development of Mobile Cloud Computing, enabling the migration and offloading of complex computational tasks and data from smartphones to the Cloud environment. We have examined various frameworks for offloading, and most research has overlooked the security concerns related to data and code, indicating that there is no flawless method to secure the code. We also observe that current frameworks for computational data offloading continue to encounter challenges regarding privacy, security, and efficiency. This limitation of existing frameworks complicates the development and management of a proposed framework. Ultimately, it is essential to provide a solution for a secure and efficient framework or model that will assist in resolving complications and minimizing efforts in the design, deployment, development, and supervision of a secure offloading framework. The goal is to enhance the capabilities of smart mobile devices by offering security solutions, conserving power consumption, and reducing response time. In conclusion, this work improves the efficiency and overall performance of smart mobile devices.

IV. EXPERIMENT, RESULT & DISCUSSION

Proposed Methodology :

Decision Making Model :

In the context of Cloud Computing, client applications are executed in a distributed manner. In this scenario, service providers must ensure the quality of service for clients, as they expect their tasks to be processed with minimal cost and time. Each client application is divided into multiple resources, and tasks must be allocated for the smooth processing of all these tasks, which are distributed among the virtual machines in the data center. Each Virtual Machine (VM) may take a significant amount of time to complete the processing of a task depending on the number and type of tasks it is handling. Therefore, prior to execution, tasks must be assigned and reallocated to the necessary resource-dynamic computing nodes in the cloud environment. Thus, a precise decision must be made in allocating resources for effective task processing based on resource availability to meet client requirements. Consequently, an optimal and accurate decision-making process for the efficient distribution of tasks among the virtual machines is essential for achieving performance efficiency and improved quality of service.

Approach in Task Scheduling :

Client requests arrive following a Poisson distribution pattern and are organized into a Queue of Tasks, which are referred to as cloudlets (CLs). The task scheduler allocates resources to these cloudlets through the scheduler module to fulfill client requirements. An accurate decision is made to achieve the optimal task VM with maximum processing efficiency using a genetic algorithm, ensuring that the task is completed with minimal time consumption in the Cloud Computing framework. Let (VM1, VM2, VM3, VM4, VM5….VMn) represent the set of virtual machines available at the data center for processing the set of tasks or cloudlets (CL1, CL2, CL3, CL4, CL5, CL6… CLm). Assume that all these VMs operate in parallel and are interconnected. These VMs operate with their pre-allocated resources, which are shared with other VMs on hosts within the data center. During execution, if any task encounters a resource deficiency, it notifies the scheduler, which dynamically reallocates resources among the VMs to assist in completing the task execution. The quantitative analysis is conducted under the following assumptions:

1) The quantitative study is encompassed by the code guidance length.

2) Task arrivals are distributed according to a Poisson distribution.

3) Each hub handles one task at a time.

There are two intended scheduling goals:

- Minimization of the task completion time.
- Improvement of resource utilization.

Computation of Completion Time :

In a universal cloud environment, all computing hubs operate concurrently, meaning that in a Cloudsim scenario, all virtual machines (VMs) initiate simultaneously. If multiple cloudlets are assigned to a single VM, all cloudlets will be executed in a continuous stream. A two-dimensional (2D) time matrix is created by calculating the fitness value (FV) or finish time (FT) of each cloudlet (CL) on every VM, utilizing a fitness function based on the computational capacity of the virtual machines. Subsequently, for each VM, the completion time (FT) is determined by summing the consumption times of all cloudlets allocated to that VM. This completion time reflects the finish time of the last cloudlet assigned to that VM. The total time T consumed by cloudlet 'j' (CLj) on the 'ith' VM, denoted as $TCLj\ i$, is calculated by considering the total execution time $ETCLj\ i$, the resource reallocation time based

on the input size $CLj\ isz$ and output size $CLj\ osz$ of cloudlet j, as well as the network bandwidth BWI J. This analysis takes into account n number of VMs and m number of cloudlets.

Algorithms :

Stage 1: Establish a 2D time exhibit for FV or FT of every CL across all VMs.

Stage 2: Identify the number of cloudlets to be booked for j = 0 to m.

Stage 3: Define the number of Virtual Machines for i = 0 to n.

Stage 4: Construct the 2D time exhibit with $FTCL$.

Stage 5: End for loop.

Stage 6: End for loop.

Stage 7: Ascertain the completion time of the final CL assigned to each VM.

Stage 8: Define the number of virtual machines for I = 0 to n.

Stage 9: Identify the number of cloudlets to be booked for j = 0 to m.

Stage 10: Completion time of the last CL assigned in the VMi.

$$FT_i = \sum_{j=0}^{m} CL_j * E\ (i,j) \quad \text{……..(5.1)}$$

$$T_{CL_j}^{i} = ET_{CL_j}^{i} + \frac{\left(CL_j^{isz} + CL_j^{osz}\right)}{BW_j^{i}} \quad \text{……(5.2)}$$

Stage 11: Termination for loop

Stage 12: Termination for loop

Stage 13: Assignment of CL to the VM that concludes its processing at the earliest

Stage 14: While (all cloudlets are allocated to the suitable VM)

Stage 15: For each cloudlet that remains unscheduled

Stage 16: The total number of cloudlets to be scheduled for j = 0 to m.

Stage 17: The total number of virtual machines for i = 0 to n

Stage 18: VM that delivers the minimum FT for CLj. Determine the $VMi\ MinF(CLj)$

Stage 19: when CLj is distributed to VMi (i,j) = 1

Stage 20: Termination for loop

Stage 21: Termination for loop

Fitness Function :

The fitness function serves to evaluate the superiority of an individual chromosome, thereby determining the evolution of subsequent generations. Fitness indicates that each individual chromosome and those with high fitness possess a greater likelihood of survival. For each generation, the fitness value of every individual in the population is assessed; individuals with higher fitness values are selected from the current population, followed by the application of crossover and mutation operators to create a new generation. The new generation of solutions is then utilized in the next iteration of the algorithm. The overall fitness value of the chromosome is calculated using Equation (5.3), which takes into account the total time required to complete the failure probability (β) and the schedule (α).

$Fitness\_Chromosomei = \alpha\ (Total\_time) + \beta(FPi)$ ……(5.3)

Where $Total\_timei = \sum i{=}i{-}n\ (T\_Len \div VM\_MIPSi)$ $\alpha + \beta = 1$, VM_MIPSi is defined as

Each processor of VMj executes millions of instructions per second, while FPi represents the network delay between nodes.

Result :

1) Experimental Setup :

This section details the experimental setup and the results achieved with the proposed offloading method. The proposed offloading method is evaluated using Java Cloudsim. The initial record is executed within the default package, which takes input regarding network bandwidth, delay, and the number of tasks. The number of tasks refers to the amount of cloudlets that can be modified by adjusting the value to enable cloudlet() to function. The algorithm is tested by configuring the parameters as shown in Table 3.2. The simulation has been conducted with two distinct scenarios, considering different sets of CLs and VMs for each scenario. A decision must be made to determine which cloudlet can be executed in the VM and how long it will take to complete. Time consumption may vary for different cloudlets running on the same VM, and similarly, the same tasks may require significantly different durations to complete their execution in different VMs. The faster the VM, the lesser the execution time allocation. The larger the tasks, the more time it consumes, especially with a high bandwidth network.

Table 5.2 : Cultural Algorithm Parameters

Parameters	Value
Population size	100
Maximum Evaluation	500
Cross over operator	Single Point
Cross over probability	Pc
Mutation Operator	Bitflip
Mutation rate	0.15
Knowledgebase	Normative Knowledge

Table 5.3 presents the beginning and ending times for the CloudID and Virtual Machine ID according to the proposed offloading strategy.

Table 5.3 : Completion time for the proposed offloading approach, including Cloudlet ID and Virtual Machine ID

Cloudlet I3D	Virtual Machine ID	Start Time	End Time	Time
1	0	1164.52	1164.98	0.46
10	1	1172.5	1175.2	2.7
2	2	1175.52	1176.65	1.13
11	3	1163.64	1164.01	0.37
4	4	1166.6	1167.01	0.41
9	5	1163.7	1163.89	0.19
11	6	1167.12	1167.78	0.66
2	7	1165.52	1165.94	0.42
6	8	1165.41	1166.2	0.79
8	9	1162.3	1162.65	0.35
3	10	1162.2	1162.64	0.44
3	11	1168.01	1169.52	1.51
5	12	1168.95	1171.71	2.76
7	13	1164.51	1165.74	1.23
0	14	1172.1	1172.58	0.48

Result :

1) Dataset Description :

A dataset sourced from Twitter has been acquired through the use of an API. The datasets, which vary in size from 100 MB to 1000 MB, are utilized for the evaluation of the proposed Data Sensitivity-Similarity based access control method. The performance metrics examined in this study include running time (in seconds) and the number of sensitive items within the dataset.

2) Performance Analysis of the Proposed Data Sensitivity – Similarity Based Access Control

The performance of the suggested Data Sensitivity and Similarity-based Access Control (DSSBAC) is evaluated against the Content-Based Access Control (CBAC) method. Table 7.1 illustrates the execution time (in seconds) for the proposed DSSBAC method compared to the existing CBAC method across various dataset sizes. Figure 7.2 provides a graphical depiction of the execution time (in seconds) for the proposed DSSBAC method alongside the existing CBAC method for different dataset sizes. From table 7.1, it is evident that the proposed DSSBAC method requires less execution time (in seconds) than the existing CBAC method. This finding is also visually represented in figure 7.2.

Table 7.1: Running Time (in Seconds) for the Proposed DSSBAC method and existing CBAC method for different size of Datasets.

Size of the Dataset (in MB)	Running Time (in Seconds) by Access Control Methods	
	Existing CBAC Method	Proposed DSSBAC method
100	41	23
200	65	39
300	88	52
400	102	71
500	132	94
600	159	113
700	188	133
800	203	158
900	269	196
1000	297	216

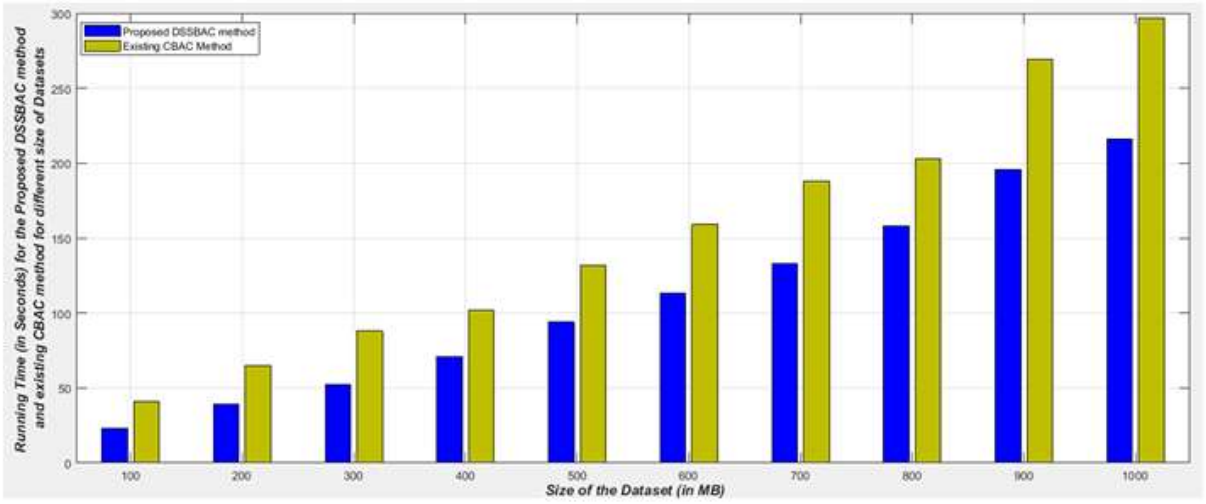

Figure 7.2: Graphical representation of the Running Time (in Seconds) for the Proposed DSSC method and existing CBAC method for different size of Datasets.

The proposed DSSBAC method and the existing CBAC method identify the number of sensitive items across various dataset sizes, as illustrated in table 7.2. Figure 7.3 provides a graphical representation of the number of sensitive items identified by both the proposed DSSBAC method and the existing CBAC method for different dataset sizes. Table 7.2 demonstrates that the proposed DSSBAC method identifies a greater number of sensitive items compared to the existing CBAC method, as depicted in figure 7.3.

Table 7.2: Number of sensitive items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets.

Size of the Dataset (in MB)	**Number of Sensitive Items identified by Access Control Methods**	
	Existing CBAC Method	**Proposed DSSBAC method**
100	3	8
200	5	14
300	8	17
400	11	22
500	16	25
600	17	30
700	21	38
800	26	45
900	29	53
1000	34	65

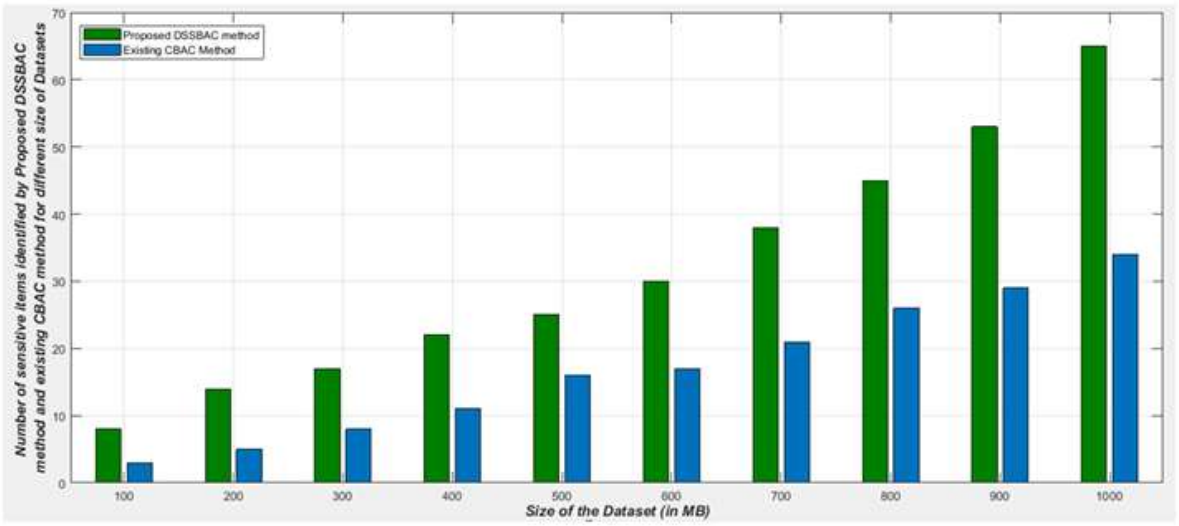

Figure 7.3: Graphical representation of the Number of sensitive items identified by Proposed DSSBAC method and existing CBAC method for different size of Datasets.

V. CONCLUSION AND FUTURE SCOPE

Conclusion :

The combination of Mobile networks and Cloud Computing leads to the development of Mobile Cloud Computing (MCC), which is an important research area that has emerged from mobile devices and Cloud Computing. Data protection is a significant concern in Mobile Cloud Computing (MCC). This thesis outlines four contributions that aim to bolster security in MCC. The primary technique emphasizes an efficient Offloading approach to decrease the time required for resource allocation. The second method has been shown to lower Encryption and Decryption time by employing an Optimized Elliptical Curve Cryptography technique. The third method proposes a way to identify sensitive data through a Data Sensitivity and Similarity access method, while the final technique works to reduce the Error rate using a Siamese Neural Network. The results obtained from these proposed techniques contribute to enhanced security.

Future Work :

Future research will aim to enhance the proposed methodologies and perform more comprehensive evaluations. Furthermore, there may be initiatives to integrate multiple wireless connections, such as 5G and Bluetooth, along with various cloud resources like cloudlets, public clouds, and mobile ad-hoc networks. Another potential direction for future work is the deployment of the proposed algorithms on real-time mobile devices to evaluate their true effectiveness.

References

1. Youssef, Ahmed E, "Exploring cloud computing services and applications",*JournalofEmergingTrendsinComputingandInformation Sciences*, vol.3 (6), pp. 838-847, 2012.
2. Arockiam,L.,S.Monikandan,andG.Parthasarathy,"Cloudcomputing:a survey", International *Journal of Internet Computing,* vol.1 (2), pp. 26-33, 2011.
3. Rahimi, M. Reza, et al., "Mobile cloud computing: A survey, state of art and future directions", Mobile *Networks and Applications*, vol.19 (2), pp. 133-143, 2014.
4. Soyata,Tolga,etal.,"Acceleratingmobile-cloudcomputing:A survey",*Cloud Technology: Concepts, Methodologies, Tools, and Applications*. IGI Global, pp. 1933-1955, 2015.
5. Wang, Yating, Ray Chen, and Ding-Chau Wang, "A survey of mobile cloud computing applications: Perspectives and challenges",*Wireless Personal Communications*, vol. 80(4), pp. 1607-1623, 2015.
6. Grover, J., & Kheterpal, G., "Mobile cloud computing: an introduction", InResource Management of Mobile Cloud Computing Networks and Environments, pp. 1-23. IGI Global, 2015
7. Jana, Debasish, and Debasis Bandyopadhyay, "Efficient management of security and privacy issues in mobile cloud environment", *2013 Annual IEEE India Conference (INDICON)*.IEEE, 2013.
8. Shahzad, Abid, and MureedHussain, "Security issues and challenges of mobile cloud computing",*International Journal of Grid and Distributed Computing*, vol.6 (6), pp. 37-50, 2013.
9. Mollah, Muhammad Baqer, Md Abul Kalam Azad, and Athanasios Vasilakos, "Security and privacy challengesin mobile cloud computing: Survey and way ahead", Journal *of Network and Computer Applications,* vol.84, pp.38-54, 2017.
10. Jiang, Qi, Jianfeng Ma, and Fushan Wei, "On the security of a privacy- aware authentication scheme for distributed mobile cloud computing services", *IEEE systems journal*, vol.12 (2), pp. 2039-2042, 2016.

Book :

11. https://unidel.edu.ng/focelibrary/books/mobile-cloud-computing-models-implementation-and security.9781498796033.72976%20(10).pdf
12. https://industri.fatek.unpatti.ac.id/wp-content/uploads/2019/03/210-Cloud-Computing-Sandeep-Bhowmik-Edisi-1-2017.pdf