Received: December 5, 2016


INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# A Secure Client Aware Certification for Mobile Cloud Offloading Decision

**Uma Nandhini D[1*] Latha Tamilselvan[1]**

**Silviya Nancy J[2] UdhayaKumar Shanmugam[2]**

[1] *School of Computer, Information and Mathematical Science*
*B.S. Abdur Rahman University, Chennai, Tamil Nadu, India*
[2] *Department of Computer Science and Engineering,*
*Rajalakshmi Engineering College, Thandalam, Chennai, Tamil Nadu, India*
[*] Corresponding author's Email: umaudhay@gmail.com

**Abstract:** The advancements in smartphones with excellent feasibility and networking capabilities paved the way for rising leap in mobile communication, but their limitations incline users to next level paradigm called Mobile Cloud Computing. Despite the cloud services reaching far greater heights, the issues of to security and privacy needs to be addressed. Therefore, our proposed Client Aware Certification (CAC) model ensures to identify the authenticity of client devices connected to the cloud based on the behaviour predictability and security checks. A resource broker identifies the trustworthiness of the client devices before offloading any task. Integrity check, privacy protection, and access patterns are some of the attributes considered for offloading decision. The model achieves better security, privacy, and performance for resource migration. Identity management and certification feature ensure a better predictability with secure virtual communication. The model is experimented with AWS cloud platform and tested for a video conversion application.

**Keywords:** Mobile cloud computing, Computation offloading, Identity management, Client awareness.

## 1. Introduction

The incredible transformation and radical innovations in the organizational substructures of computing, particularly cloud computing, have been making history with on-demand services. Cloud computing, in essence, refers to the delivery of resources over the internet. Additionally, the computer's processing power is a shared pool of resources that can be accessed whenever needed, at any time, with a network. Cloud computing can provide the infrastructure necessary for integrating applications, monitoring and storing data, and client delivery. Cloud services are popular due to the reduced costs and complexity of the software, hardware and networks involved - the other potential benefits being scalability, reliability, and efficiency. The interaction between the mobile and the cloud is facilitated by the creation of large volumes of data. Mobiles are, intrinsically, constrained when it comes to storing and processing huge amounts of data and, consequently, with a handshake linking wireless access in mobiles and cloud services, Mobile Cloud Computing (MCC) has stamped its use in this integrated sector/segment/enterprise. In recent years, we have been experiencing massive upgrades in the realm of mobile computing, with promising applications in wireless access, music, maps, and much more. Mobile phones – and smartphones, in particular - are becoming smarter by the day with their value-adds, and this is accompanied by breakneck growth. The mobile phone is, indubitably, rightly considered to be a major and influential invention of the twentieth century. Since the creation of the first mobile phone, there has been a steady escalation in its technological aspects with the passing of each decade. Incredibly, the initial prototype of all handheld devices permitted only vocal communication, whereas today's smartphones

provide diverse applications (including remote communications). Likewise, to extend their platforms, it incorporates assorted services like messaging, internet connection and browsing; storing and playing music and videos. Also provides access to TV shows and current socio-political updates, all of these in collaboration with social networks. The era of mobile technology has crossed a new threshold with a recent survey clearly, predicts that the combined number of mobile devices and tablets have already exceeded the world's population [1]. At the same time, smartphone shipments would increase 2.5 times to 12 billion by 2018. As a result, over 6.6 billion people will own one or more mobile devices. In another survey by GSM Association [2], there will be a tenfold increase in the mobile data traffic by 2018 and it is fuelled by on-demand video.

On comparing the mobile devices with desktops and laptops, they are limited in their capabilities pertaining to certain parameters like low battery, resources, processing power and storage. Consequently, intensive applications cannot be processed as the mobile's storage capacity would exceed its limit, notifying users of a memory overload. Mobile Cloud Computing (MCC) is a proposed new solution that is expected to handle situations such as these. Mobile cloud computing can be defined as a piece of constructive infrastructure where storage is set outside mobile devices as seen in Figure 1, with far-reaching implications affecting the deployment of mobile services. Obstacles such as performance, environment, and security are expected to be better managed with a mobile - cloud handshake. It accomplishes the dream of "information at one's fingertips, everywhere and every time." Cloud computing is an online space, the culmination of various computing resources delivered on-demand.

Cloud computing has been identified as an attractive alternative to cutting costs in the IT industry and elsewhere. Further, it has also succeeded in catapulting computing - with its inherent capacity to cater to the assorted needs of all sorts of people, including personal use too. Despite the apparent benefits of cloud computing, a recent survey done by the researchers reveals that there is massive mistrust of the cloud in storage and processing [3], [4]. Ultimately, it is cloud providers who track data and concentrate on securing fool-proof hiding places, but the existing policies governing trust are not up to par in satisfying users. Obviously, the cloud can be quite literally perceived as a "magic box" - meaning that customers or users are unlikely to be aware of happenings inside the cloud; that space is always an abstraction. Even if cloud providers happen to be trusted authorities maintaining the servers, trust has still not been fully earned to the point where there is contentment. It is because cloud servers can be invaded by malicious system-operating admin, with the possibility that virtual servers can be tampered with, leading to the collapse of data confidentiality and integrity. Moving such sensitive services as mobile and computer communication services into a virtual environment implies that security concerns, such as the following, are valid: the ever-present risk of loss of sensitive information due to leaks between virtual machines and loss of service due to denial of service (as a result of attacks from adjacent virtual machines) on the same host. Moreover, regrettably, the same is the scenario for any mobile-cloud information upload, making authorization essential and authentication necessary for the safe retrieval of the original data.

The proposed work is to provide a trusted and secure mobile-cloud model with the trustworthy paradigm. The true nature of the application users can be identified by advocating self-evaluation.

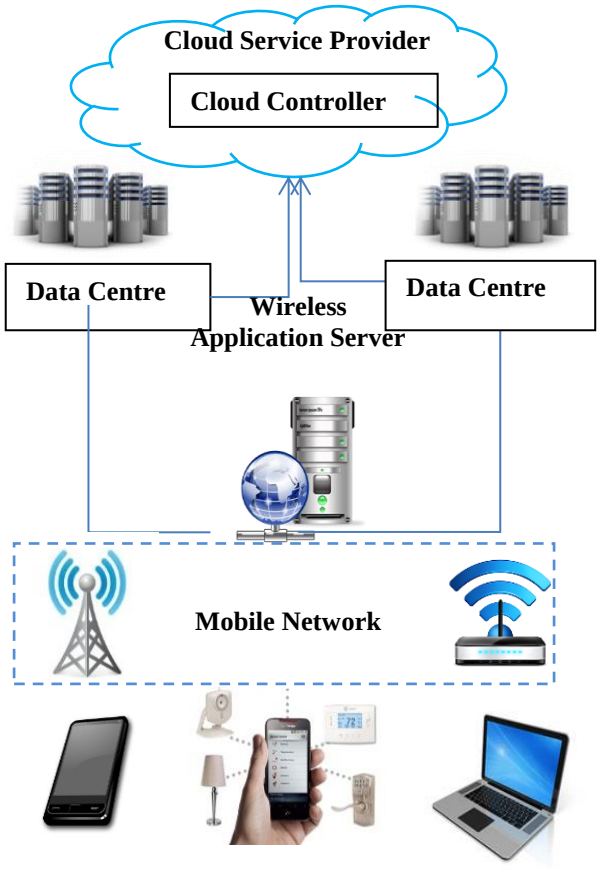


Figure. 1 Basic Architecture of Mobile Cloud Computing

The behaviour model also embraces the enhancement of mobile-cloud security features by issuing authentication certificates after evaluating the trustworthiness of the mobile client.

The primary benefit of the proposed model is, with the process of security check and analysis the fraudulent users can be identified, and they cannot gain access to the system because of which loss of trusted users will be prevented. It will also be helpful to determine the uniqueness and trustworthiness with which the frequent users will be offered more privilege and benefits of accessing the system with high-end security. Security breaches would be avoided with various trust check parameters such as geo-location status, data integrity, privacy and access rights.

The organisation of the paper is written as follows. The section 2 gives a detailed overview of the literature review and comparison of proposed model with previously existing techniques. Next in follow is Section 3, which depicts the organisation and structure of proposed Trusted Mobile-Cloud environment with decision methods and analysis of security checks using different parameters. Next in line is Section 4, with implementation and results of statistical analysis. Finally, conclusion and future work on Trusted Mobile-Cloud model is briefed in Section 5.

## 2. Literature Review

This chapter comments on the mainstay of the discussion with a review of the literature. The near-constant threat raised by security issues in cloud computing is a critical factor affecting widespread cloud computing functioning and features. This scenario is entirely likely to worsen when cloud applications are used by mobile users. Securing data in a mobile cloud platform has become essential since applications are becoming immensely popular and increasing in number. Today, every enterprise and organization are focused on serving mobile users, simply because its user-friendly handling has resulted in profits running into billions, particularly with the inception of numerous applications. The current study [2] nourishes that the mobile-cloud market would generate upto $45 billion in 2016.

Dimitrios [7] discuss the emergence of cloud computing from various evolutionary infrastructures and evaluate cloud security issues and solutions. This research examines cryptographic solutions and a Trusted Third Party who plays the role of the middleman in authentication. The Third Party would analyse (with various protocols) the user's credentials for security and also use certificates issued by the authorities concerned where sometimes the third party interference may have security breach by others. Ronnie [8], discuss security issues in mobile cloud computing, including the benefits of integrating mobile and cloud features in a variety of applications, as well as cloud services and models. Cong Wang [9], also remarks on the importance of preserving privacy by auditing the Trusted Third Party (TPA) without creating problems for cloud users. The use of a public key-supported homomorphic authenticator, along with random masking, ensures efficient auditing systems for the TPA as well as cloud service providers. In their paper, Bernd [10] elaborates on the primary issues faced with defining and elaborating possible areas of vulnerability. As the resource in mobile devices needs to be migrated to a nearby local cloud for complex executions, in the paper [11], a novel algorithm to assess the mobile through client awareness and make a decision to offload to a nearby cloud is proposed.

Authors Deyan Chen and Hong Zhao [12], present looming security concerns in cloud computing by elaborating on various security standards like the Advancement of Structured Information Standards (OASIS), Key Management Interoperability Protocol (KMIP) and several cloud delivery models and platforms which extend viability for cloud security. To address the problem of authentication in the cloud for the smart card users, a mutual authentication scheme using Elliptic Curve Diffie Hellman (ECDH) is proposed in [13]. Safiriyu Eludiora et. al. [14], dwell on the Identity Management (IAM) protocol for the secure use of cloud services - under all delivery models and methods - by users. Pankaja [15], propose an Identity Management Protocol that seeks to override the existing authentication protocol by maintaining user log records which show the detailed pathway of user access rights and policies. Antonio [16] proposed and discussed various scenarios like heterogeneity. The implementation methodology holds Security Assertion Markup Language (SAML), defining authentication both for hosting cloud servers and users.

Thus various surveys and reviews have confirmed that there are quite a lot of issues on security and privacy in the mobile-cloud environment. There hasn't been much interest shown in establishing a security policy for mobile devices accessing cloud structure. Most of the discussions in previous work enlighten about the third party intervention, cryptographic techniques like using digital signatures, key management, OTPs for protecting the users' access and data.

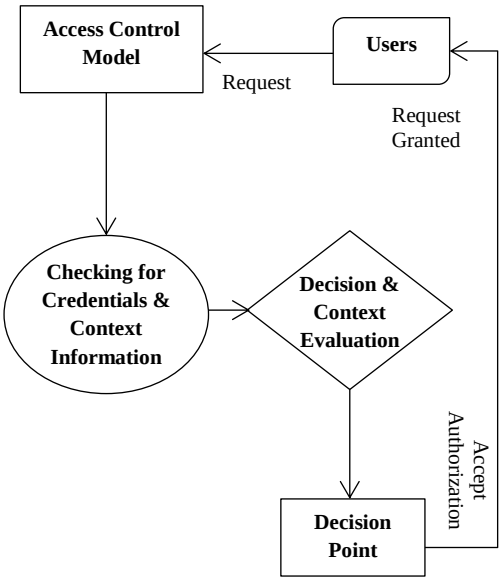


Figure. 2 Security design check for credentials and context information

These techniques may have less protection when compared to the proposed model. Hence, our proposed work concentrates on behaviour analysis with which users' credentials are monitored. With this context, the identity management can be improved in providing high-end security to the users. The outline of the recommended model is depicted in Figure 2 above.

## 3. Trusted Mobile Cloud Environment

The key challenge for mobile cloud development is security breaches affecting both users (clients) and servers. Much research has discussed the implementation and maintenance of server security. However, a major factor to be taken into consideration is user authentication while offloading data to the cloud and the type of authorization users are provided with to store data. Consequently, to overcome security violations among mobile cloud customers, there needs to be put in place an observatory scheduler who can oversee the process of user "data offloading" efficiently without affecting the policy certification of cloud service providers or the trust of the user in that environment. This assurance can be easily provided by a third-party ruler called the IAM (Identity Access Management), which can help avoid infringements of security to a large extent. The IAM, which plays a vital role in handling public data in the cloud, has become a crucial part of all organizations and academic institutions. Whenever particular items of data are to be stored, security plays an important role in maintaining integrity. The greatest advantage of IAM, simply put, is: "Access from anywhere and anytime" This means that a user can upload or retrieve information, at his convenience, when the protection offered is enabled with recommended policies or certification.

With the prevalence of growing security breaches, workable solutions - such as OpenID digital signatures with user names and passwords, digital signatures including encryption techniques and certain authentication services were introduced [20]. But not all of these served well in every environment. Behavioural analysis plays a part in the inception of a cloud model for mobile users. Instead of working on cloud servers' security certificates and policies, the solutions can begin with the mobile user.

For experimental purposes, let's consider the model of computational offloading. The theory of offloading deals with the transportation of intensive applications to the cloud server for storage and computation. Computation Offloading is most useful for mobile devices, constrained as they are by heavy battery consumption - a result of processing intensive applications - due to which processor capacity is also drained. Another major drawback is storage because mobile devices cannot hold huge files with large data, so the concept of Mobile Cloud Computation (MCC) meets the needs of mobile devices for a variety of applications – particularly, image processing and Photoshop. These can be easily processed because of wireless access and the availability of the service everywhere.

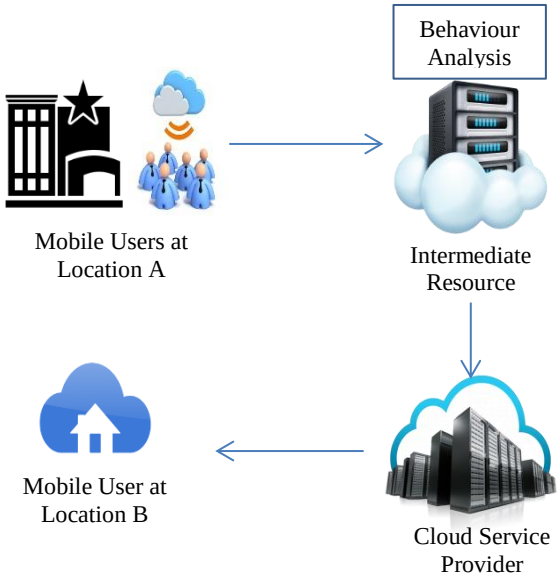


Figure. 3 Mobile Cloud Trust Architecture

Consider a scenario where a user wants to process a video file (change a video format). If the user is at a mall, and he offloads a complex and large-sized video application to the respective cloud server through the available networks (2G, 3G, or Wi-Fi), the offloaded video file will be saved for computation and the required change of format (.avi, .mp4, etc.) will be made and stored in the storage space allotted for the particular user. The user can download it whenever necessary (probably later at home, as shown in the example). The trusted cloud architecture is shown in Figure 3.

### 3.2 Behavior analysis and security check

An important strategy in our trust model is behaviour analysis and checking user authorization by means of the certification generated for the particular application that is accessed by the user. The outcome is depicted as follows. First, the user's authorization with the cloud server is checked to ensure that he is indeed the holder of the account being accessed. When the user has been authenticated, he is allowed to use the relevant application. At the backend, the cloud service provider monitors user activity for better service. The sequence model in Figure 4, explains the step-wise process for a trusted mobile cloud environment. When the user wants to offload an intensive task to the server, the server reverts with a certificate check, which includes confirmation of user authentication, the location of user, and network service provider the user is united with. Then the mobile device is scanned by the trust checker for authorization, and a vulnerability analysis program is installed, which checks the mobile device when it is idle. After this initial verification, offloading service begins from the mobile to the server. Next, the server checks client activity to note whether he/she is invading the server using malware. The identification of malware injection is found by analyzing the data traffic between the parties and comparing it with the test traffic pattern. If misconduct is identified, the computation offloading process is automatically ended by the server. The authorized check would have been completed by the server by this time. If not, the computation of the task continues with behaviour analysis commencing by observing data loss protection, suspicious security behaviour, geo-location privacy, personal privacy, and so on. Thereafter, any flaws are reported and computation offloading automatically ended. If not, a policy assurance affirmation is done, based on the classification of the particular vulnerability.

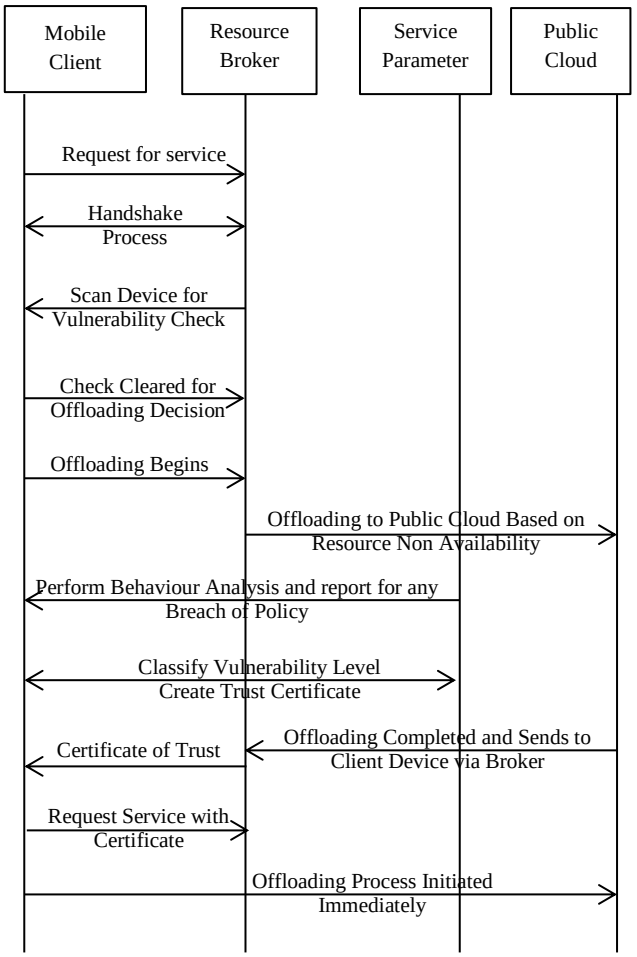


Figure. 4 Sequence depiction of Trusted Mobile-Cloud Environment

In the course of time, the computation offloading process is completed. If needed, a trusted certificate could be generated for future communication. This is a background process that protects the integrity and standards of the application by means of a client authentication certificate. In between these client authentications, every mobile device's vulnerability is assessed and its corresponding value in given as a rating to that mobile. This rating mechanism helps every user to involve them in establishing a reputation score, which can be a source of trustworthiness of that mobile, in-turn to build a trusted mobile cloud.

### 3.3 Decision methods and formulation

The key aim of this work is to promote the security for the applications in the cloud that are accessed through mobile devices. Trust is considered the most important factor of the cloud computing environment [3]. Certain formulas are set forth, as follows, to establish user behaviour and authorization identity. There are certain parameters through which the users have to be authenticated

and provided service; they include the following features,

1) Type of service requests given by the user.
2) Maintaining proper access boundary users.
3) Different attributes like time, location, and the number of previous access should be identified simultaneously.
4) Predicting the state and behaviour of the user by background monitoring while registration and using the service.
5) Service access logs will be maintained periodically to obtain the frequency of user application services.

**Step 1:** The user is allowed to access the cloud server's application based on the request projected.

$$M_{app}: c \rightarrow user$$
$$M_{app}(user) : \Phi (\alpha \wedge \beta) \quad (1)$$

Where $M_{app}$ refers to the mobile application, c the cloud server, α is the authorization by the certifying authority, and β is the authentication approval by the cloud server. So, Φ (α ^ β) refers to the fact that only if these variables are satisfied will the user be allowed to process the application.

$$M_{app}: c \ \ user$$
$$M_{app}(user): \Phi (\sim\alpha \wedge \sim\beta) \quad (2)$$

The above condition explains when the user is malicious.

**Step 2:** When the user is allowed to access the application Φ(α ^ β) having bypassed all constraints, certain factors like time are essential in the analysis of user behaviour. These factors are identified for each access by the user.

$$Time: c \rightarrow Time$$
$$Time (\alpha \wedge \beta): \Phi (u \wedge v) = \Phi(u) \wedge \Phi(v) \quad (3)$$

Where, Φ(u) is user login authentication and Φ(v) is user identity verification.

**Step 3:** Step 2 and Step 3 work together, permitting the user to offload the intensive task to the server for conversion.

$$Offloading: c \rightarrow offloads$$
$$Offload (v): \Phi(w) \quad (4)$$

Φ (w) denotes the resultant task, which is in our case, the conversion of file format of a particular video. This step can be repeated for n number of conversions. On successful completion of offloading, the condition mentioned below in equation 1, stands at,

$$\sum_{i=1}^{n} \phi(w) = 1 \quad (5)$$

**Step 4: Case (a): Intrusion Detection:** Any system is to be provided security so as to eliminate intrusion, which can lead to deactivation or misuse of the system/application. The following equation explains the intrusion detection policy.

$$Intrusion: c \leftarrow \rightarrow M_{app}$$
$$Identity (user) : (\sim\beta \wedge \sim\Phi(v)) \quad (6)$$

This can be co-related with Step 1, the initial area for user login, if the unauthorized user β and Φ(v) are negative and login fails.

**Case (b): Behaviour Analysis:** Another form of intrusion is caused by faulty access to information by the authorized user itself.

$$Behaviour: c \leftarrow \rightarrow \mu (B)$$
$$Trust: (\sim\mu (B) \wedge (\sim\beta \wedge \sim\Phi (v))) \quad (7)$$

If μ (B) is false, then (~β ^ ~Φ (v)) becomes false, showing that the user is not to be trusted and is thereafter prohibited from using the application.

**Step 5:** This step displays user frequency in using the application and calculates trust based on subsequent access.

$$Access\ frequency: c \leftarrow \rightarrow \Omega (f)$$
$$\Omega (f) - Usage\ frequency \quad (8)$$

**Case (a):** Frequency of the user interacting with the system and stipulated behaviour

$$\Omega (f) \{user\} = \sum_{i=1}^{n} \phi(v) + \sum_{i=1}^{n} \phi(w) = 1 \quad (9)$$

In this case, n denotes the no. of times the user logs in [Φ (v)] to use the application [Φ (w)].

**Case (b): Checking user behaviour continually:** If the above condition is true, then the following formula is satisfactory with regard to past performance.

$$\mu(B) = 1$$
$$\phi(v) + \phi(w) = 1 \quad (10)$$

**Case (c): Trust analysis:** Based on the constraints mentioned above, trust analysis can be determined as in equation 3.

$$Trust = \Omega (f) = \sum_{i=1}^{n} \phi(w) = \mu(B) = 1 \quad (11)$$

**Case (d): Weighted trust factor:**

$$Trust = W1 + W2 + W3 + W4 = 1 \quad (12)$$

W1 – Authorization by certifying authority (0.3)
W2 – Authentication by cloud server (0.2)
W3 – Trusted behaviour (0.3)
W4 - Reliable time factor (0.2)

## 4. Implementation and Result

The proposed trusted model enhances the security by predicting the behaviour of the user by series of steps. The implementation follows authorization by certificate authority, and

Table 1. Hardware components of Mobile Device and Online and Offline Server

| Hardware | Client Device | Cloud Server (offline) | Wi-Fi Router | AWS Server (m3.large) |
|---|---|---|---|---|
| Processor | Qualcomm | AMD A6 | Broadcom | Intel Xeon E5 |
| Speed | 1.0 GHz | 1.8GHz | 54Mbps | 2.5GHz |
| Memory | 1 GB | 4GB | Nil | 7.5GB |
| Connectivity | Wi-Fi/3G | Wi-Fi/ADSL | IEEE 802.11 b | Cloud |
| Op. Sys. | Android 4.4 | Ubuntu | WLAN A23 5.10 | Ubuntu |

authentication by cloud server by analysing the behaviour of user and uniqueness of user is identified by trusted behaviour and time factor with access frequency. To evaluate our security policy and credentials, we have implemented our work using Samsung android mobile ver. 4.4, by generating an application called Webview App. The process of mobile cloud requires a cloud server, which in our simulation environment we have created a private cloud setup for offline simulation. For online simulation, Amazon Web Services (AWS) instance with Ubuntu Linux is utilized as shown in Table 1.

### 4.1 Offline Simulation Arrangements

The procedure for offline simulation of the cloud setup can be explained as follows. Based on the proposed architecture, the user is currently in the shopping mall (an example to show that the user can access the service from anywhere). Now, if users want to store data or compute heavy tasks which are beyond the limited scope of mobile devices, the same can be offloaded to the nearest server. With the network connection available, the user gets connected to the application by requesting a connection to the server. During this stage, a client-side certificate is prompted by the application and user authentication will be enquired into, as shown as in Figure 5.

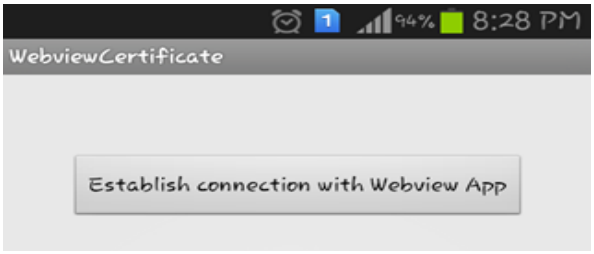


Figure. 5 Connection establishments with server and application (Webview)

Table 2. Sample Offline Behaviour Analysis for Client-Side Authentication

| Parameters | Trust Check |
|---|---|
| Data integrity | Checked for data privacy with certificate authority |
| Security | User authentication is analyzed |
| Geo-location status | Geographical status of the user is analyzed |
| Personal privacy | User mobile credentials are examined |
| Access rights | Provided access is checked with user logs |

This is the phase where client authentication is initiated. The application will be monitored in the background by the hosting server, regardless of whether the client requesting the service is a legitimate user of the respective server (cloud) or an unauthorized one. As the algorithm of the trust model states, the user is checked for activity based on access rights given to the user for logging onto that particular application. This would separate a trusted user from an untrusted one. This experimental setup ensures that the mobile user is authenticated by means of a client certificate and, as an additional feature; the behavioural analysis of the client is taken into consideration.

The Table 2, above explains in detail the various parameters making up the analysis and portrays sample checking at the server for client authentication. When the connection is recognized, the user has permission to access the Android application for offloading intensive tasks to the server. Here the example application that is being executed is the video conversion task, considered a heavy task that cannot be carried out on mobile and handheld devices. Figure 6 presents a view, where the client chooses to offload the file to the server, from where the intensive file would be moved to the server and computation takes place. Figure 7 Predicts the successful conversion of the file sent earlier. After the computation of the task by the server, the user can download it in the mobile device whenever necessary, as seen in Figure 8.

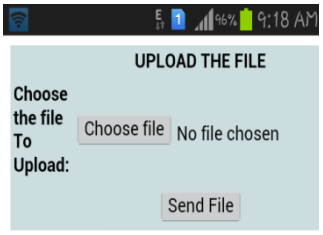


Figure. 6 Offloading to server (File upload)

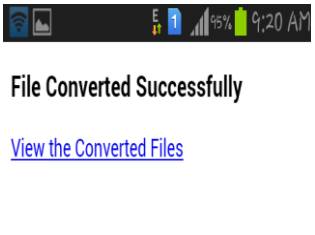


Figure. 7 Video file format conversion successful

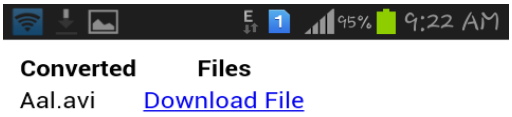


Figure. 8 Download page

### 4.2. Experimentation System in Amazon S3

The previous section has demonstrated that offline transfer and processing of intensive applications is effective. This section concentrates on real cloud servers and processing. Amazon Web Services has been considered for the purpose of experimentation. The storing of an intensive file is carried out by creating a bucket in Amazon S3 storage, with the required folders for storing the files necessary. The following sub-sections explain actions taking place in the client and server side. The snapshots in Figure 9 portray how the user can upload the file to the cloud bucket and Figure 10 shows successful uploading.

**Client Side (Cloud Storage)**

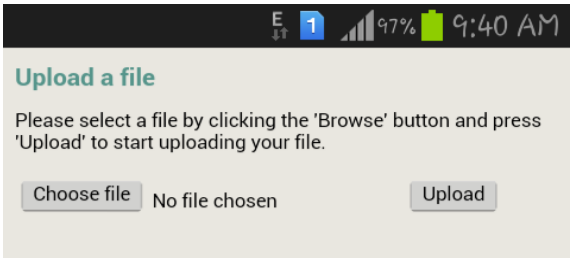


Figure. 9 Cloud upload

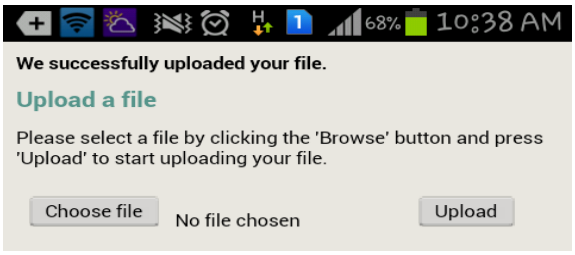


Figure. 10 Upload successful

**Server side (Cloud storage)**

The screen shot in Figure 11 shows the uploaded file in the S3 bucket.

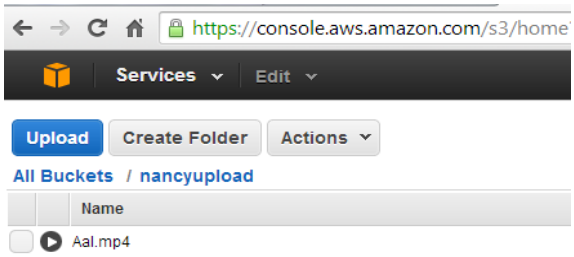


Figure.11 Bucket storage in AWS

Table 3. Service Parameters

| User Type | Service Type | Authorization by CA | Service location | No of previous access | Access freq. (%) |
|---|---|---|---|---|---|
| New user | Registration | 0.95 | 192.22.7.2 | 0 | 60 |
| Registered user | Data service | 0.99 | 192.22.5.8 | 10 | 99 |
| Visiting user | IdM | 0.94 | 198.55.4.7 | 0 | 50 |
| Frequent user | Data service | 0.99 | 192.55.7.8 | 20 | 100 |
| Unknown user | IdM | 0.89 | 194.88.7.4 | 0 | 20 |

Assuming the above criteria, the following features are analyzed and simulated. Consider, Security, privacy, integrity to be 100%, Initial error rate = 0, Marginal threshold value for certificate authority = 0 – 1. Based on the frequency of access, future access will be defined. Table 3, depicts the various cloud parameters. The result for security components shows that most of the parameters satisfy the criteria for performance. The following analytical graph in Figure 12, emphasizes the access frequency of the user type from the service parameters depicted in Table 3. The plot simulates the priority and the service provided to the users of the various categories defined in the table. On comparing the Figure 12 and Figure 13, the frequent and registered users can who have has been trusted already will be provided a platform to access the required service with few basic security check in O(n) time. Whereas the new user need to go the following checks like client check, security check, the visiting users should also undergo minimum check and will be provided only limited service with O(N+M) time. The Malicious or unknown users have to gain by additional security validation that takes O (N log N) time.

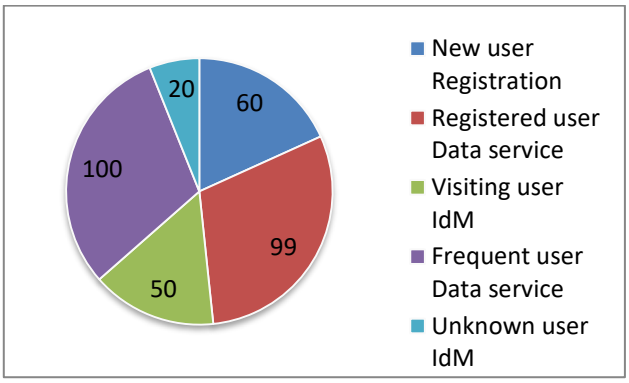


Figure. 12 Access Frequency of Users

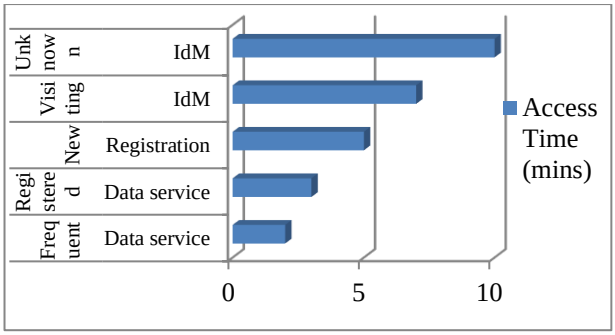


Figure. 13 Access Time of different categories of Users

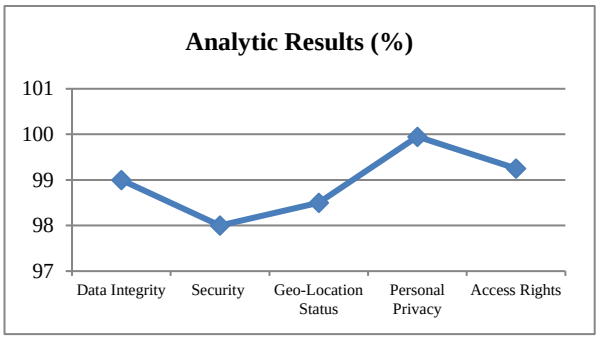


Figure. 14 Analytical results of various service parameters

The recommended system is done with Amazon Web Services (AWS), offline use added benefits to AWS. If there is any network failure with AWS, it can be mitigated by offline server.

### 4.3 Comparative Analysis

The analysis of similar offloading schemes given in Table 4, suggest that most of the earlier models have not concentrated on security attributes an offloading condition.

Table 4. Comparative Analysis of the Existing and Proposed Model

| **Offloading Decision Schemes** | **Application Type** | **Cloud Migration** | **Local Server** | **Static /Dynamic** | **Decision Attributes** | **Security Attributes** |
|---|---|---|---|---|---|---|
| Proposed CAC model | Video Conversion | Yes | Yes | Dynamic | Context, Power, | Trust, Privacy |
| Weblets [21] | Augment Reality | Yes | No | Static | Latency | No |
| Context-aware [22] | TOPSIS | Yes | No | Dynamic | Context of Device | No |
| COSMOS[23] | Face Recognition | Yes | No | Static | Response Time | No |
| Hyrax [24] | Image Search | No | Yes | Static | Network | No |

## 5. Conclusion and Future Works

This paper proposes to provide a mobile-cloud infrastructure designed to efficiently manage the security and privacy of user data. Alongside, this paper also investigates security challenges and privacy issues. The proposed solution identifies users based on their past behaviour and tries to minimise the need for a complete security check. Various behaviour evaluation based decision methods are formulated for computation offloading process. The client aware mobile cloud computing model is a novel attempt in identifying trusted and untrusted in situations of offloading to cloud. Results have been verified in a real time cloud environment to make the model feasible and test cases and analysis have proved to judge the clients efficiently. Frequented users would have less overhead making it suitable for regular consumers. As a future research and implementation, the whole offloading process can be executed and tried in public cloud space. Further offloading can also be implemented using Hadoop which would minimize the complexity and overhead.

## References

[1] S. Radicati, “Mobile Statistics Report, 2014-2018”, *A Technology Market Research from The Radicati Group*, USA, February, 2014.

[2] GSMA Global Mobile Economy Report, GSM Association, 2015.

[3] S. M. Habib, S. Hauke, S. Ries and M. Mühlhäuser, “Trust as a facilitator in cloud computing: A survey”, *Journal of Cloud Computing: Advances, Systems and Applications*, 2012.

[4] S. Udhayakumar, S. Chandrasekaran, T. Latha and F. Ahamed, “An Adaptive Trust Model for Software Services in Hybrid Cloud Environment”, *15th WSEAS International Conference on Computers*, pp. 497-502, 2011.

[5] R. S. Chang, J. Gao and V. Gruhn, “Mobile Cloud Computing Research - Issues, Challenges and Needs”, *International Symposium on Service Oriented System Engineering (SOSE)*, 2013.

[6] R. Los, D. Shackleford and B. Sullivan, “The Notorious Nine Cloud Computing Top Threats in 2013”, *Top Threats Working Group, Cloud Security Alliance*, February, 2013.

[7] D. Zissis and D. Lekkas, “Addressing Cloud Computing Security Issues”, *Future Generation Computer Systems*, p. 583–592, 2012.

[8] R. D. Caytiles and S. Lee, “Security Considerations for Public Mobile Cloud Computing”, *International*

*Journal of Advanced Science and Technology*, Vol. 44, July, 2012.

[9] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", *IEEE INFOCOM proceedings.* 2010.

[10] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud Computing Vulnerabilities", *IEEE Computer and Reliability Societies*, 2011.

[11] U. Nandhini and T. Latha, "Computational Analytics of Client Awareness for Mobile Application Offloading with Cloud Migration", *KSII Transactions On Internet And Information Systems*, Vol. 8, No. 11, 2014.

[12] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", *IEEE International Conference on Computer Science and Electronics Engineering*, 2012.

[13] H. Li, F. Li, C. Song and Y. Yan, "Towards Smart Card Based Mutual Authentication Schemes in Cloud Computing", *KSII Transactions On Internet And Information Systems,* Vol. 9, No. 7, 2015

[14] S. Eludiora, O. Abiona, A. Oluwatope, A. Oluwaranti, C. Onime and L. Kehindel, "A User Identity Management Protocol for Cloud Computing Paradigm", *Int. J. Communications, Network and System Sciences*, p. 152-163, 2011.

[15] P. A. Hadole, J. Rohankar ,P. Ambatkar, and A. Katara, "Development of Secure Mobile Cloud Computing Using Improved Identity Management Protocol", *International Journal on Recent and Innovation Trends in Computing and Communication*, 2014.

[16] A. Celesti, F. Tusa, M. Villari and A. Puliafito, "Security and Cloud Computing: InterCloud Identity Management Infrastructure", *19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*, WETICE, Greece, 2010.

[17] P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. B. Othmane, L. Lilien and M. Linderman, "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing*", Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems*, p. 177-183, 2010.

[18] S. Nancy, D. Uma and T. Latha, "Credential and Identity Access Management for Client Awareness in Mobile Cloud Computing Framework*", Australian Journal of Basic and Applied Sciences*, vol. 9 issue 11, pp. 624-630, 2015.

[19] S. Udhayakumar and T. Latha, "A Cooperative Trust Model with Adaptive Migration for Secure Cloud Services", *Advances in Information Sciences and Service Sciences,* Volume 6, Number 6, 2014.

[20] E. Ghazizadeh, Z. Dolatabadi, R. Khaleghparast, M. Zamani, A. A. Manaf, and M. S. Abdullah, "Secure OpenID Authentication Model by Using Trusted Computing, Abstract and Applied Analysis", *Hindawi Publishing Corporation*, Vol. 2014.

[21] X. Zhang, S. Jeong, A. Kunjithapatham, and Simon Gibbs, "Towards an Elastic Application Model for Augmenting Computing Capabilities of Mobile Platforms," *Third International ICST Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, LNICST 48, Springer, pp. 161-174, 2010.

[22] B. Zhou, A. V. Dastjerdi, N. Rodrigo, Calheiros, S. N. Srirama, and R. Buyya, "A Context Sensitive Offloading Scheme for Mobile Cloud Computing Service" IEEE 8th International Conference on Cloud Computing, pp. 869-876, 2015.

[23] C. Shi, K. Habak, P. Pandurangan, M. Ammar, M. Naik and E. Zegura, "COSMOS: Computation Offloading as a Service for Mobile Devices", 15th ACM international symposium on Mobile ad hoc networking and computing, pp. 287-296, 2014.

[24] E.E.Marinelli, "Hyrax: cloud computing on mobile devices using Map Reduce, "*DTIC Document, Tech. Rep*.", September, 2009.