Quantitative Risk Analysis for Mobile Cloud Computing: a Preliminary Approach and a Health Application Case Study

Javeria Samad, Seng W. Loke, K.Reed
Department of Computer Science and Computer Engineering,
Latrobe University, Australia
jsamad@students.latrobe.edu.au, {S.Loke, k.reed}@}latrobe.edu.au

Abstract- **Mobile cloud computing is presented as the next logical step in the adoption of cloud based systems. However, there are number of issues inherent in it that may limit its uptake. These issues are best understood as "risks" which span the whole structure and the life cycle of mobile clouds and could be as varied as security, operations, performance, and end-users behaviours. This paper is a first step in developing a quantitative risk model suitable for a dynamic mobile cloud environment. We also use this model to analyse a mobile cloud based health application and report our findings, which have implications for cloud computing as a whole.**

Keywords- mobile cloud computing, risk model, quantitative risk analysis, context aware.

I. INTRODUCTION

Despite the increasing popularity and usage of mobile cloud computing, there are certain issues inherent with it that still prevail in the mobile cloud computing community, making it difficult to utilize the full potential of the clouds. These issues or 'risks' span the whole structure and life cycle of mobile clouds and could be as varied as security, operations, performance and end-users.

The intricacies of a mobile cloud system pose many risks. At system level, these include the risks of connectivity, limited resources, security, and limited power supply. As the system complexity increases, both the technical and non-technical risks increase and so is the need to manage these risks. The ad hoc nature and mobility in mobile cloud computing environments means that the development of these systems need more rigorous and specialized risk management to deal with all the risks. This further burdens the developers of mobile cloud computing frameworks and applications. In addition to the complexity of mobile cloud infrastructure, they also have to deal with the risks at framework/application level including but not limited to efficient job distribution, virtualization, scalability and so on.

Currently, there isn't any formal risk management process in place to deal with the risks arising in mobile cloud computing. As with any development and deployment activity, an effective risk management is integral to the success of any mobile cloud computing system, in particular for critical applications such as health (e.g., health monitoring) where failures due to bandwidth variations, battery limitations, and other infrastructure changes may be life threatening. However, our literature survey shows that the current work on mobile cloud systems focuses more on cost and resource savings, and there has been little progress towards the development of mobile cloud aware risk management methodologies. There is a need for the mobile cloud developers and users to realize the importance of effective and efficient risk management in place. Risk management doesn't only protect the systems from various risks, it also plays a critical role in enabling mobile cloud providers to achieve their goals by improved decision making through up-to-date risk reporting [1]. An efficient risk management can also protect the stakeholders from financial losses, and can also improve customer satisfaction/confidence in delivered cloud services.

The aim of this paper is to explore the possibilities of designing a quantitative risk management model suitable for dynamic mobile cloud environments, which is *context-aware* and would feed on the current context parameters as inputs, predict/identify potential risks, generate respective alarms and, where possible, manage risks autonomously.

The rest of this paper is organized as follows. Section II gives a brief background of our research aim and methodology. Section III describes the proposed risk model in detail. Section IV illustrates the model further by applying it to a case study and demonstrates how context-awareness can influence risk decisions. Section V presents the related work and Section VI briefly discusses the summary and future challenges.

II. BACKGROUND

We have analysed a range of representative frameworks, concepts and application models for mobile cloud computing [2-13], to see that how well they deal with inherent risks and to identify the extent to which they support risk management. The analysis showed that with exception of [9], none have comprehensively discussed the risks associated with the use of that particular framework (understandably because of their research focus). The next step was to examine the ways in which risk management can be made easy and possible for mobile cloud computing. Our understanding of mobile cloud frameworks and how they work, the risks faced by the mobile clouds, and the differences in traditional & mobile cloud based development, combined with our analysis of strengths and weaknesses of existing risk management processes formed the basis for the development/designing of our context aware quantitative risk approach. The term context-aware means being alert of present surroundings (i.e., locations, environment etc.) and situations continuously, and making use of these most-current context parameters for calculating risks at any given time, which is vital given the potentially dynamic nature of mobile clouds.

As with any new technology, cloud computing also has some inherent risks. In mobile cloud computing, the intricacies and complexity of the system makes it further risk prone and there is an ever increasing need for managing these risks effectively and proactively for successful and efficient utilization of clouds. In [14] the author holds the view that at present cloud computing is implemented without any proper risk management. In our view, the same holds for mobile cloud computing.

III. A QUANTITATIVE CONTEXT-AWARE RISK MANAGEMENT MODEL

Risk Management is the process of managing risks in a given system with the aid of formal processes, methods and tools, thereby providing a controlled environment for continuously analyzing the risk factors, involving calculating the relative importance of each risk item and designing strategies to deal with these risks.

Risk is defined as the possibility of something happening that can affect the outcome negatively; it is measured in terms of *probability* and *impact* [1], [15] and is usually derived by the formula:

$$RE = P(O) * L(O)$$

where RE is risk exposure related to an (negative) outcome O, P(O) is probability of the negative outcome and L(O) is the loss or impact of that negative outcome [16].

A. Context-Awareness and the Risks

In mobile clouds, as in other domains, the probability of a risk happening is dependent on many factors. Consequently, unconditional probabilities should not be assigned to any risk factor without considering the relevant risk triggers, controls and strategies. In a mobile cloud computing environment, one such trigger could be the change in context. Sometimes this change would be negligible, but sometimes it can cause ripple effects,, depending on the nature of the context change, e.g. a person moving from one room to another but staying within same connection boundaries, constitutes a less threatening context change than if the person moved from one place to another with different connection networks and settings.

An ideal risk management model is one that is always up-to-date, and this is especially critical in a mobile cloud environment owing to ever changing and ad-hoc characteristic of mobile clouds. Hence, including the current context in risk calculations is of utmost importance in mobile cloud computing for continuous proactive decision-making. Any change in context can cause a change in existing risk probabilities and hence the overall risk calculations. Although such changes in context might not affect the pre-defined impact values of risk factors considerably, the overall risk scenario would need to be revised and new risk priorities to be determined.

The context-aware risk management model should be able to update itself immediately when a change in the applications environment occurs, so as to deal with changed risk situations proactively. These risk scenarios, calculations and other relevant data can be added in a repository continuously. Besides assisting in current decision making and risk management, the results from this repository can be used while planning the later implementations of the model and new applications, as well to identify the vulnerable areas i.e. the context changes which are more prone to risk and its effects, or the context changes which are producing highest ratios of risks and probabilities. This information can help in further improve or restrict the usage of given mobile cloud framework accordingly.

B. A Quantitative Risk Model

Any risk management model usually includes these main activities [1],[17],[18],[25]:

- risk identification,
- probability calculation,
- impact analysis,
- priority determination,
- treatment alternatives identification,
- monitoring (general, look-out for new risks).

In our case, we will refer to *monitoring* as done via a tool for identifying any change in context so as to adjust risk calculations and the risk management strategy accordingly.

Mathematically, risk is presented as a product of probability (*P)* and impact (*I)* [17],[18],[44], that is:

$$Risk=P*I \quad (1)$$

Probability refers to the relative frequency or expected number of occurrences of risk in a given time frame. Impact represents the relative expected consequences (or loss) in the event of that risk happening. So, the actual risk is calculated on basis of these two criteria.

In order to calculate the risk value for a mobile cloud system/application precisely, we utilize the following procedure. The first step is the identification of all possible risks R relevant to the current usage of the mobile cloud system i.e. $R_T = \{R_1, R_2, \ldots, R_n\}$, where R_T represents the complete risk set. The next step is to identify all possible risk factors r contributing to each R_i, i.e. determining all the possible context situations that can cause that particular risk R_i to happen (see Fig. 1).

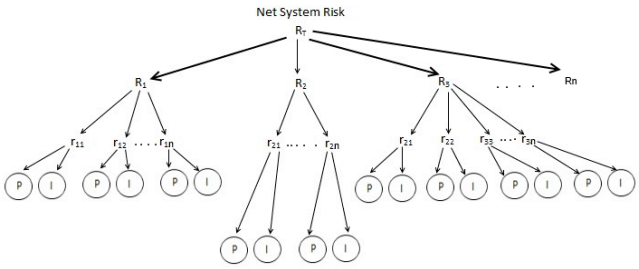

Figure 1. Graphical representation of risk and risk factors

For each risk R_i, we would need to have a corresponding sub-set of risk factors given as:

$$R_1=\{r_{11}, r_{12}, r_{13,}\ldots, r_{n1}\}$$
$$R_2=\{r_{21}, r_{22}, r_{23,}\ldots, r_{n2}\}$$
$$\vdots$$
$$R_n= \{r_{n1}, r_{n2}, r_{n3,}\ldots, r_{nn}\}.$$

where each nj represents the number of elements within each set R_j.

The next, we determine the initial values of *P* and *I* for each of these factors. Since risk is given as product of probability and impact, we write:

$$r_{ij} = P_{ij}I_{ij} \quad (2)$$

The risk values for each identified risk item can then be described as follows:

$$R_1 = (r_{11} + r_{12} + \ldots + r_{n1}) / n1$$
$$R_2 = (r_{21} + r_{22} + \ldots + r_{n2}) / n2$$
$$\vdots$$
$$R_i = (r_{i1} + r_{i2} + \ldots + r_{ni}) / ni \quad (3)$$

Substituting values from (2) in (3), we get*:*

$$R_i = ((P_1I_1) + (P_2I_2) + \ldots. (P_{ni}I_{ni})) / ni$$

i.e.,
$$R_i = \Sigma^{ni}_{j=1} P_jI_j / ni \quad (4)$$

An important point to be noted here is that not all the risks would be applicable in different mobile cloud systems and their relevance or suitability for each individual system would depend mainly on the purpose, scope and level of the particular implementation. For example the risk "poor/faulty access control mechanism" could be highly dangerous in a security critical mobile cloud system (like confidential governmental databases, records, etc.) but perhaps negligible in entertainment based mobile cloud applications like YouTube or MP3 media player. The same goes for *r* as well as all risk factors that will be contributing differently to a risk *R* in different situations. Similarly, as not all the risks have same priority/influence within different scenarios, so we need a mechanism for assigning priorities to each of the factors. To handle this situation appropriately, we can take following measures:

- During the planning phase, the stakeholders can be asked to assign weights to each R according to their own perspective of the system usage. For irrelevant risks, that weight would be assigned a 0 value. However for the other risks, weight would be assigned according to their potential influence on the system functionality. The risks with more weights will give a higher net value, and multipliers can be used to represent dominating risks – we discuss the determination of these weights later. Hence, (4) becomes

  $$R_i = (\Sigma^{ni}_{j=1} P_jI_j / ni).W_i \quad (5)$$

- Instead of assigning weights to each possible context change situation *r*, we can simply use their respective impact values *I* to serve the purpose. For each risk *R*, those context situations that are not applicable in a particular scenario, would be assigned an initial impact value of 0, hence removing them the calculation.

Now the net value of risk would be given as:

$$R_T = (R_1 + R_2 + R_3 + \ldots. + R_n) / n \quad (6)$$

Combining (5) and (6) we get:

$$R_T = (\Sigma^{n}_{i=1} (\Sigma^{ni}_{j=1} P_jI_j / ni).W_i) / n \quad (7)$$

where *n* represents the total number of risks identified, i.e. the number of elements in set R_T.

C. Calculating Probabilities and Impact

Calculating probabilities and impacts correctly (or as nearly correctly as possible) is the next major challenge. In mobile clouds, the environment always keeps changing as the mobile devices potentially move in and out of cloud zones (i.e., vicinity of resources). The number of devices in a cloud varies tremendously at all intervals and as do the overall networking conditions, connections and locations and so on, making the continuous identification, calculation and prediction risk outcomes complex. In order to calculate the net risk, the probabilities and impacts have to be calculated first individually. Calculating probabilities is more difficult than impacts as any change in context can change the probability values quite unexpectedly.

A lot of work has been done in areas of risk analysis using Bayesian networks and probabilities for probability estimation [19-21]. As we need to calculate probabilities on the basis of changes in context, Bayesian conditional probability approach is the most suitable tool for the purpose of updating probabilities in view of updated or new context information. As per our hypothesis, in mobile clouds, the probabilities of risk factors will vary (in most cases) if there is a change in context which creates a similar notion as conditional probabilities. For this reason, Bayesian seems to be most suitable choice for calculating probabilities for r in our model. In this approach, probability is always conditional on background knowledge and the probability of an event is calculated by comparing the uncertainty of the current situation with a standard event [21].

The Bayesian probability is given as follows:

$$P(r|E) = (P(E|r) / P(E)) * P(r)$$

where, in the scope of our research,

E= event of a context change happening
P(E) = probability of event happening
P(r) = probability of risk factor r before event E
P(r|E) = probability of risk factor r with event E
P(E|r) = probability that E will cause risk to happen (i.e., given r, what is the probability that E is observed, or in our interpretation, E is the cause)

The possible impact is difficult to calculate solely quantitatively, especially initially. On other the hand, a total qualitative approach is not appropriate in this scenario as we numerical values of impact *I* are required. The most commonly used strategy for impact analysis combines the qualitative and quantitative approaches, so as to have a numerical value, while still preserving the qualitative aspect. This would mean assigning a scale for impact values and then determining the most suitable value; this can be done on the basis of past historical records of system and risks, relevant statistical surveys, or asking stakeholders for selecting the values as per their experience and desire. The scale we use here can be simply defined as: I= {low, medium, high} where: I= Low for values ranging (1-3), I= Medium for values ranging (4-6), I= High for values ranging (7-10).

In mobile clouds, some of the risk factors have constant impact values i.e. within a given system, these values won't change rapidly over time and the impact would be more or less the same if any of those risks occur. For example, the impact of server failure would always be constant over the

whole cloud i.e. 'very high' holding a numerical value of 10. However, there are some risks factors that cannot be assigned a constant value owing to their nature; for example the impact of bandwidth failure would always be different depending on the amount of change in bandwidth value and determining the exact impact value for each bandwidth change is problematic. One way to tackle this issue is to use impact as a function, which generates a graph based on the distinct abstract/generalized bandwidth values, making it possible to extract the intermediate values from the resulting graph.

IV. CASE STUDY

To see how the risks can affect any application, and how our context-aware risk model will behave in such situations, we have taken an example of a mobile cloud based e-health application proposed in [22]. They have designed a scalable real-time health monitoring and analysis system and have used an Electrocardiogram (ECG) analysis system prototype as their case study. This prototype system collects patient data (e.g., pulse and heart beat rates) through an ECG sensor device attached to a patient's body. This sensor device transmits the data to the patient's mobile device via Bluetooth without manual intervention. Client software on a mobile device then transfers the data to an ECG Analysis Web-service hosted on a cloud computing stack, either using Wi-Fi or the 3G network. They have used the Aneka cloud computing platform and Amazon's S3 storage services. The analysis software then analyses patient's data, generates results and appends the latest findings to the patient's medical record. Depending on analysis, the data could be sent to the patient, doctors or emergency services as needed. Fig. 2 shows the ECH health monitoring application architecture as proposed by [22] However, note that this is not a critique on ECG Analysis prototype as, understandably, risk is not their research focus.

Applying our approach, and identifying the inherent risks and their consequences, we see that the design could be disastrous failures (e.g., leading to gaps in records or, at worst, or even threatening human life if danger situations are not detected) if no proper risk management is implemented. It is a time-critical application that requires extreme levels of reliability for the results to be being generated and needs to be always up-to-date with the latest findings.

We have selected a few risks for demonstration as space does not permit the listing of each identified risk here. These risks are selected to include at least one from the more relevant and topical risk issues within mobile cloud domain namely security, mobility, device limitations, and network & connectivity [23-41].

The selected risks and their possible respective context situations are given in Table 1. We selected risk factors from the column "risk factors" in Table 1, and have assigned probability and impact values to them for calculation demonstrations (see Table 2). These values are assigned from the perspective of the ECG data analysis app.

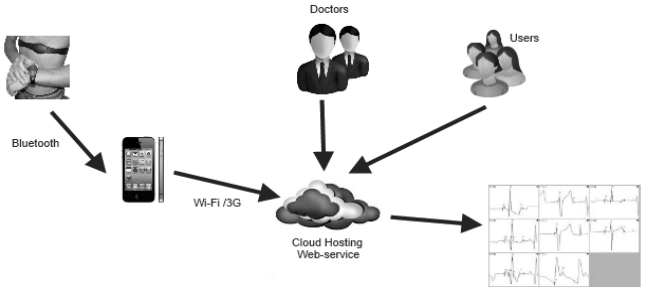

Figure 2. ECG Data Analysis Software as Service [22]

An interesting fact here is that there are some risks due to human or environmental factors (e.g. bad weather, noise and so on) and there is no way of determining the probabilities of such risks accurately. We can only assign the probability values based on our observation. For human factors (like forgetting to charge a battery, etc.), we have assigned the initial probabilities on the basis of our close observation of some subjects (in this case colleagues, friends etc.) and their behavioral patterns (note that real data of frequency of charging can be obtained for an individual to determine such a probability for that individual).

A. Understanding Probabilities and Impacts with respect to context changes

The idea is to design a model such that it will be able to extract the current values (e.g., remaining battery power, data network signal strength, remaining memory, and location service availability) and use them as input in our quantitative model. There are some mobile apps and mobile APIs that provide this functionality and in the future we intend to explore the possibility of using their outputs as a means to extract current context parameters. For demonstration however, we will be restricting ourselves to using the initial values from Table 2.

For calculating impacts, we need two distinct functions, each corresponding to the nature of the impact factor. For constant impact values, the impact is simply calculated as

$$I_i = C(r_i)$$

where $C(r_i)$ represents the constant value for risk factor r_i at all times. For continuously varying impact values, we need to represent impact as a function of time where, for some continuous function f, we have

$$I_i = f(t)$$

. For each of these time dependent factors, we need to determine a function that would precisely project the context-to-impact ratio (i.e. how each change in context value will proportionally correspond to the resulting impact value) for that particular risk factor. However, in this paper, we will be focusing on constant impact values to demonstrate or approach. In the future, we plan to introduce more functions for calculating impacts and hence obtain more targeted values.

For discrete risk factors, we need to calculate the probability and impact values on the basis of current context parameters. For this purpose, we have created some scenarios that would depict the relative change in probability and impact values because of change in current context.

Let us say an elderly person X with a coronary condition who has been advised by his doctor to use the above mentioned ECG analysis app. He must wear the heart-rate-monitor all the time (preferably) so that his condition could be monitored by his doctors. Now consider this person X in following scenarios:

Scenario 1: X is working in a well-developed city which has many offerings in terms of security and mobile and network services at better speeds.

Scenario 2: X is travelling to his home village that's not very well-developed and hence offers fewer options for network and mobile services.

Scenario 3: X goes to a 3rd world country for an official assignment for 2 years. The crime rates in that country are noticeably higher than his own country. The quality of mobile devices isn't very good and the most commonaly used mobile devices different from those in X's home country.

If we consider scenario 1, we see that the probability values for risk factors like battery hardware problem, memory leak by apps, and different memory sizes would have similar values as those in scenario 2 and 3. However, the risk factors such as poor connection, blind spots, infrastructure problems etc. will have higher probability in scenarios 2 and 3, than in scenario 1. Moreover, in scenario 3 the risk factors such as compatibility issues, and different data formats supported by devices will have higher probability values than scenarios 1 and 2. Similarly, the probability of the risk "device theft" will be highest in scenario 3. (However, even though the probability will be high in this case but as mentioned above, this is precisely the kind of risks for which calculating exact probability is difficult due to human factor involvement, even if they can be estimated from historical data, e.g., history of crime rates in the area).

To understand role of context parameters in calculating impacts, we need to consider these factors from a different perspective. In scenario 2, the probability of X facing low bandwidth or noise issues is understandably high, but the impact would be dependent on the level of bandwidth deterioration or level of noise, e.g., if the bandwidth deteriorates from 79 Mbps to 50Mbps, then its impact would be say medium but if it drops from 79Mbps to 20Mps, then its impact would be high or very high and so should be assigned a respective value accordingly. For example, to calculate the new probabilities in the event of context change of X being at the village, we used the initial probability values from Table 2. Using Bayes' theorem, we get:

P(E) = 0.2 (probability of X being at village)

P(r) = 0.3 (probability of low bandwidth at any time/location, estimated from some dataset say)

P(E|r)= 0.6 (probability of X being at village will cause low bandwidth (or given low bandwidth))

If P(r|E) is the probability of risk with context change event, then using Bayes' theorem, we get:

$$P(r|E)=(0.6/0.2)*0.3=0.9$$

i.e. the updated probability that X will face low bandwidth issues, given that X is at the village; note that the impact (i.e., P(E|r) / P(E)) of being in the village on the probability of low bandwidth is 3 (i.e., if low bandwidth, X is three times more likely to be at village than if no low bandwidth).

B. Calculations and Resulting Values

The risks R and respective context changes or risk factors r are given in Table 2. Each risk has also been assigned a weight, the details of which will be given in following section. Entering the P and I values from Table 2 in (2) and (3) for each of risk factors, we get a matrix of values as follows:

$R1= (r_{11+} r_{12 +} r_{13+} r_{14}) /4 = 6.1/4=1.5$

$R2= (r_{21+} r_{22 +} r_{23}) /3 = 4.3/3 =1.4$

$R3= (r_{31}+r_{32})/2 = 9/2 =4.5$

Where:

r_{11}= battery hardware problem

r_{12} = type of connection being used

r_{13} = memory size differences

r_{14}= data allowance on 3G plan

r_{21}= low bandwidth

r_{22} = poor connection

r_{23} = noise

r_{31}= not compatible for my mobile device

r_{32} = different data format on multiple devices

Multiplying respective weights, we get:

R1=150

R2= 1400

R3=45.

We can see that R3 had highest value initially, however, after weight assignment, the risk values have changed considerably, reflecting the actual severity of each risk.

Inserting these values in (6), we get

$$R_T = (R_1+ R_2+ R_3) /3 = 1595/3= 531$$

which is the net risk value for the system in the given context. How the context will affect the probabilities and resulting net risk values are discussed in the following sections. The calculated R_T can be compared to a set threshold T where warnings or actions can be taken, and R_T is computed continually as context changes or via context prediction techniques so that the risks are continually assessed as the context changes or when significant changes are predicted (context prediction is not within the scope of this paper, but an example is the prediction of 3G bandwidth for a particular location based on previous readings) – context changes affect the values of the probabilities associated with each risk factor (and possibly affect the impact values too), so that the value of R_T could indeed change as context changes. Hence, the algorithm for continual risk assessment is essentially as follows as in Algorithm 1.

Algorithm 1:

Loop

{

sense context or predict context

update probabilities and impact on risk factors

recalculate R_T

compare R_T with threshold T, to decide on action

}

end loop

Or, risk assessment could be done in an event-driven manner in response to significant context changes, as in Rule 1.

Rule 1:
On sensing context change or on predicting a context change

If context change significant
then
update probabilities and impact on risk factors
recalculate R_T
compare R_T with threshold T, to decide on action

C. Assigning Weights

For priority or weight assignments, we need to categorize the identified risks according to their severity towards the system. We can categorize these risks in four categories: highly critical, critical, important, and transferable. Each of these scales would represent the situation as follows:

- Transferable: potential for performance degradation.
- Important: operational but performance degrades; potential for minor loss
- Critical: operational but performance degrades significantly; potential for major loss
- Highly Critical: not operational; potential for complete system shut-down

To reflect these severity levels in net risk value, we need a mechanism such that if the value of a highly critical risk exceeds an acceptable threshold, the net risk value should represent a 'distress mode'. We can see that risk value for each R will always remain within a normalized scale of 0-10. So, one way of dealing with this is to assign appropriate weight values to each factor. This however would be problematic as the resultant value will still be low unless the weight assignment is done on a much larger scale of say 0-100, which is not very practical as the weight assignment will be dependent on stakeholder perspectives and its usually difficult for people to think in terms of such large scales and that could cause a risk of improper weight assignments. For this reason, for weights, we will be using fixed multipliers of different orders of magnitude for each category and the multiplier is multiplied with whatever value the stakeholder assigns for the weights (on the convenient scale of 0-10), the multipliers will make the resultant net values reflective of the severity of the risk. We are looking at some other mechanisms for achieving this task as well and in future we intend to explore the possibility of devising functions that would deal with weight assignments and the rest of the calculations automatically.

For extremely critical risks, the weights will be assigned a multiplier of 1000, for critical: 100, for important: 10 and for transferable: 1. For example, service unavailability is a extreme risk that can cause the total system failure. So, any weight assigned to this risk will be multiplied by a factor of 1000. After defining the acceptable value of this risk, any change/increase in any associated risk factor *r* will cause this risk value to go higher in multiples of 1000, generating an immediate alarm. These multipliers are to reflect dominating risks, relative to others, and act as drivers.

If we take the example of the ECG app we discussed that probability of low bandwidth, poor connection, noise etc. is higher in scenario 2 whereas it would be comparatively low in scenario 1. Assume person X moves from scenario 1 to scenario 2. The context parameters as input would lead to an update of the probabilities according to Table 2, and so higher probability values are obtained accordingly (in this case r_{21}, r_{22} and r_{23} increase from 0.3 to 0.9, 0.2 to 0.7, 0.1 to 0.5, respectively), which in turn will generate a relatively higher risk value for each relevant r and hence R_2 (which would increase from initial 1.4 to 5.0). This change (delta) in itself would have been negligible and very difficult to compare with the threshold, but now as its being multiplied by 1000, any slightest change would result in values as high as a hundred times with multiplicative effect (R_2 increases from 1400 to 5000); triggering the necessary alarms.

V. RELATED WORK

Although risk management isn't a new concept [15], [16], [17], [18], we see a lack of work in this area in mobile clouds or in cloud domain in general. The significant contributions in highlighting the potential issues in clouds have been given by [13],[23], [24], [26-41]. Some authors have suggested at using context awareness in cloud domains [42], [43] but their focus is not on using this information for risk management. An important contribution has been made by [44] in which they have proposed a model for assessing security risks in cloud platforms.

[19], [20] have also used the Bayesian approach for probability assessment; however their work is focused on qualitative risk assessment.

VI. CONCLUSION AND FUTURE WORK

We have presented a preliminary context-aware quantitative risk management model that takes the current context values (from the mobile cloud infrastructure and user device) as input parameters and then uses this current context information to continually calculate the current risk value of the system. We have then applied this model to a mobile cloud based ECG Data Analysis app proposed by [22] to determine how the current context is important in assessing risks in mobile cloud systems and how any slightest change in context parameters can influence the whole risk picture. We used this analysis to demonstrate that how our context-aware risk model can help in calculating and hence managing risks accurately, including representing how context changes affect changes in overall risk assessment, and how the model can represent dominating risks via suitable weight multipliers.

Our future work will explore the means of extracting accurate context parameters from a mobile cloud system and using this information to continuously monitor the system for any risks arising. We also intend to further expand the probability, impact and weight assignments and devise more context-specific calculation methods for individual risk-context situations. We are also working on implementing the approach on Android as a middleware that continually monitors risks in the background.

TABLE 1. SELECTED RISKS AND FACTORS FOR ILLUSTRATION

Risk (R)	Relevance	Associated Risk Factors (r)	
Resource Exhaustion W= 8 (Critical) Multiplier: 100	Resource exhaustion can directly affect availability and it's a possibility in this scenario as the target population can be huge with different resource type and sizes, personal preferences, and app set installed on their devices.	Battery/Power	battery hardware problem
			type of connection being used (wi-fi or 3G)
			heavy app processing
			more users per app
			more apps per server
			didn't charge
		Memory	heavy app processing
			memory leak by app
			memory size differences
		Access Plan	data allowance on 3G plan
Service Unavailability W= 10 (Very Critical) Multiplier: 1000	Data availability, service availability and reliability risk factors are extremely critical owing to the nature of this application. Any error in these aspects can be life threatening for a patient with heart risks. Application crashes and downtimes can be very dangerous, e.g. due to battery or memory shortage on continual execution for long periods of time. For media applications, we can tolerate some risks, but in applications like this ECG monitoring and analysis system, such risks are intolerable.	(Various)	low bandwidth
			poor connection
			noise
			bad weather
			blind spots
			infrastructure hardware problem
			server issues
			geographical location
			malfunctioning OS
Portability W= 6 (Important) Multiplier: 10	As this application aims to target a wide patient population, the mobile devices involved could be hugely varied which poses a risk of application portability for multiple devices. The analysis software is hosted by Cloud services but the client software resides on mobile devices itself and so it should be extensively assessed for processing efficiency for multiple devices and the mobile platform. Any problems with portability could mean a percentage of patients being unable to use this application. Also, the compatibility of mobile devices with cloud services should also be risk free or else the use of this application will be limited to a subset of patients only.	App mobility	prob in next connecting station
			already exhausted next connecting station
			not compatible for my mobile device
			different data format
			different interfaces
			different file system
	As the patients won't be static at one geographical location (a single patient can be frequent traveller) so the device's connectivity to the cloud (depending on network bandwidth variation) and availability of services accordingly is very risk prone.	Device mobility	connectivity to wrong station
			connectivity with other devices
			theft risk
			device hardware problem
Data Location W= 5 (Important) Multiplier: 10		(Various)	jurisdiction
			time to process
			security

TABLE 2: RISK FACTORS AND THEIR PROBABILITIES AND IMPACT IN DIFFERENT SCENARIOS

Risk (Ri)	Risk Factor	Notation (rij)	Impact	Probability Scenario 1	Probability Scenario 2	Probability Scenario 3
Resource Exhaustion (R1) W= 8 (Critical) Multiplier: 100	battery hardware problem	r11	9	0.2	0.2	0.3
	type of connection being used (Wi-Fi or 3G)	r12	7	0.5	0.5	0.5
	memory size differences	r13	3	0.2	0.2	0.2
	data allowance on 3G plan	r14	2	0.1	0.1	0.5
Service Unavailability (R2) W= 10 (Very Critical) Multiplier: 1000	low bandwidth	r21	7	0.3	0.9	0.9
	poor connection	r22	8	0.2	0.7	0.8
	noise	r23	6	0.1	0.5	0.7
Portability (R3) W= 6 (Important) Multiplier: 10	not compatible for my mobile device	r31	9	0.5	0.5	0.5
	different data format	r32	9	0.5	0.5	0.5

REFERENCES

[1] J. Samad, N. Ikram, M. Usman, "VRRM: A valuebased risk management process," SE '08 Proceedings of the IASTED International Conference on Software Engineering, pp. 184-191, 2008.

[2] Hadoop: http://hadoop.apache.org/.

[3] J. S. Rellermeyer, O. Riva, G. Alonso, "AlfredO: An Architecture for Flexible Interaction with Electronic Devices", in Proceedings of the 9th ACM/IFIP/USENIX International Conference on Middleware (Middleware 2008), pp. 22-41.

[4] J. Flinn, S. Young, M. Satyanarayanan, "Balancing Performance, Energy and Quality in Pervasive Computing", in IEEE 22nd International Conference on Distributed Computing Systems, pp. 217-226, 2002.

[5] R. K. Balan, M. Satyanarayanan, S. Young, T. Okoshi, "Tactics-Based Remote Execution for Mobile Computing", in ACM 1st International Conference on Mobile Systems, Applications and Services, pp. 273-286, 2003.

[6] S. Srirama, E. Vainikko, V. Šor, M. Jarke, "Scalable Mobile Web Services Mediation Framework", in IEEE 5th International Internet and Web Applications and Services Conference, pp. 315-320, 2010.

[7] G. Huerta-Canepa, D. Lee, "A Virtual Cloud Computing Provider for Mobile Devices", in ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond. MCS'10, San Francisco, California, USA, 2010.

[8] R. Kemp,N. Palmer,T. Kielmann, H. Bal, "Cuckoo: a Computation Offloading Framework for Smartphones", in IEEE 2nd International Conference on Mobile Computing, Applications and Services MobiCase '10, 2010.

[9] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, S. Jeong, "Securing Elastic Applications on Mobile Devices for Cloud Computing", in ACM Cloud Computing Security Workshop (CCSW'09), Chicago, Illinois, USA, 2009.

[10] M. Satyanarayanan, P. Bahl, R. Cáceres, N. Davies, "The Case for VM-Based Cloudlets in Mobile Computing", IEEE Pervasive Computing, pp.14-23, October- December 2009.

[11] B. G. Chun, P. Maniatis, "Augmented Smartphone Applications Through Cole Cloud Execution", Intel Research Berkeley (HotOS 2009), 2009.

[12] E. Cuervo, et al., " MAUI: Making Smartphones Last Longer with Code Offload", in Proceeding of ACM MobiSys'10, SanFrancisco USA, pp.49-62, 2010.

[13] D. Huang, X. Zhang, M. Kang, J. Luo, "MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication", in Proceeding of Fifth IEEE International Symposium on Service Oriented System Engineering, pp.27-34, 2010.

[14] G. Shipley, "Cloud Computing Risks", Information Week-Cover Story, 2010.

[15] ACTIA, "Guide to Risk Management: Insurance and Risk Management Strategies", Report by Australian Capitol Territory Insurance Authority, 2004.

[16] B.Boehm, "Software Risk Management: Principles and Practices", in IEEE Transactions, pp. 32-41, 1997.

[17] IEEE Standard for Software Life Cycle Processes-Risk Management. Software Engineering Standards Committee of the IEEE Computer Society, (IEEE Std. 1540-2001), IEEE-SA Standards Board.

[18] R.P. Higuera, & Y. Y. Haimes, "Software Risk Management", Technical Report (CMU/SEI-96-TR-012) Software Engineering Institute, Carnegie Mellon University, 1996.

[19] N. Fenton, M. Neil, "Managing Risks in Modern World- Application of Bayesian Networks", London Mathematical Society Knowledge Transfer Report, November 2007.

[20] J. M. Dambacher, et al., "Qualitative modelling and Bayesian network analysis for risk-based biosecurity decision making in complex systems", Project report- ACERA project 06/01, Australian Centre of Excellence for Risk Ana;ysis, September 2007.

[21] T. Aven, "Quantitative Risk Assessment", Cambridge university press, ISBN 978-0-521-76057-7, 2011.

[22] S.Pandey, W. Voorsluys, S. Niu, A. Khandoker, R..Buyya, "An autonomic cloud environment for hosting ECG data analysis services", Elsevier Future Generation Computer Systems, vol. 28, pp.147-154, , 2012.

[23] J. Brodkin, "Seven Cloud Computing Risks", Network World Canada. Downsview: Aug 1, 2008, vol. 24, 2008.

[24] S. Mansfield, "Danger in Clouds", Network Security- Cloud Security, pp. 9-11, 2008.

[25] PMI, "A Guide to Project Management Body of Knowledge", Third Edition, PMBoK Guides, PMI Standard, 2004.

[26] S. Ovadia, "Navigating the Challenges of the Cloud", Behavioral & Social Sciences Librarian,vol.29:3, pp233-236, , 2010.

[27] S. Paquette, P. T. Jaeger, S. C. Wilson, "Identifying Security Risks associated with Governmental use of Cloud Computing", Elsevier:Government Information Quarterly, vol.27, pp.245-253, 2010.

[28] G. Shipley, "Cloud Computing Risks", Information Week-Cover Story, 2010.

[29] B. Glimmer, "Navigating the Clouds", Broadcast Engineering; ProQuest Telecommunications, vol.53:9, pp.24-26, 2011.

[30] R. Livingstone, "Navigating through the Clouds", publishded by Rob Livingstone Advisroy, ISBN 978-1461152859, 2011.

[31] W. Jenson, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication 800-144, Computer Security Division- National Insititue of Standards & Technology (NIST) under U.S. Department of Commerce, 2011.

[32] S. Subashini, V.Kavitha, "A Survey on Security Issues in Service delivery Models of Cloud Computing", Elsevier: Journal of Network and Computer Applications, vol.34, pp.1-11, 2010.

[33] D. Catteddu, G.Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security", European Network and Information Security Agency (ENISA), 2009.

[34] R.Glott, E.Husmann, A. Sadeghi, M. Schunter, "Trust Worthy Clouds Underpinning the Future Internet", Future Internet Assembly 2011: Achievements and Technological Promises, ISBN 978-3-642-20897-3, pp. p 209-221.

[35] K. Kumar, Y. Lu, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?", IEEE Computer 2010.

[36] A.Wasserman, Software Engineering Issues for Mobile Application Development", in Proceedings of ACM FoSER 2010, November 7-8, 2010, Santa Fe, New Mexico, USA, 2010.

[37] A.K. Gupta, "Challenges of Mobile Computing", Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008), pp.86-90, 2008.

[38] S. Sakthivel, "Managing Risk In Offshore Systems Development", Communications of ACM, vol 50:4, pp.79-75, 2007.

[39] M. Armbrust, et al., Above the Clouds: A Berkeley View of Cloud Computing", Research Report: UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.

[40] D. Kovachev, D. Renzel, R. Klamma, Y. Cao, "Mobile Community Cloud Computing: Emerges and Evolves", Eleventh International Conference on Mobile Data Management, pp.393-395, 2010.

[41] B. S Kaliski, W. Pauley, "Towards Risk Assessment as Service in Cloud Environments", 2nd Unisex Workshop on Hot Topics in Cloud Computing (HotCloud'10), 2010.

[42] H. J. La, S. D. Kim, " A conceptual framework for provisioning context-aware mobile cloud services", in Proceedings of the IEEE 3rd International Conference on Cloud Computing (CLOUD), pp.466-473, 2010.

[43] P. Papakos, L. Capra, D. S. Rosenblum, " Volare: context-aware adaptive cloud service discovery for mobile systems", in Proceedings of the 9th International Workshop on Adaptive and Reflective Middleware, ARM '10, pages 32–38, New York, NY, USA, 2010.

[44] P.Saripalli, B. Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security", IEEE 3rd International Conference on Cloud Computing, pp.280-288, 2010.