Recommender Privacy Preserving Reputation Based Medical Services Scheme Using a Variant of ElGamal

Angolo Shem Mbandu*, Chunxiang Xu, Kamenyi Domenic Mutiria, Gabriel Kofi Armah
Department of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China.

* Corresponding author. Tel.: +8618781914305; email: asmbandu@gmail.com

Manuscript submitted October 15, 2014; accepted February 23, 2015.
doi: 10.17706/ijcce.2015.4.4.234-245

Abstract: Reputation based schemes are gaining popularity in all spheres of the service industry. In this paper, we have proposed a privacy preserving secure recommender reputation based medical services system. This system enables medical users to get a reputation score of a medical service provider before engaging in any services. Further, alongside the result of the query for the reputation score of the specific medical service provider in question, the scheme also avails reputation scores of other relevant medical service providers. This kind of approach ensures that the medical user has some apriority information of the quality of service to expect from the medical service providers and has a chance to choose the one with the best reputation from the ones presented. Our proposed scheme uses a variant of the ElGamal cryptosystem to preserve the anonymity of the medical user making the query. Further, our scheme too ensures the privacy of the reputation scores submitted by the medical users who give their reputation scores of the medical service providers queried.

Key words: Privacy preserving, reputation based services, healthcare, ElGamal cryptosystem.

1. Introduction

It is natural that when we seek for services we want the best. Therefore, there is need for a way to be sure that you get the best services especially for medical services due to their critical nature. There are many cases where patients get unsatisfactory medical services. In some instances the poor services lead to death or other permanent disabilities. In other cases it may lead to psychological traumas or just a bad feeling. Whatever be the case, the perceptions that clients get from medical services may be of great use to persons who may need similar services later. Some medical service providers ($MSPs$) have persistently offered poor services yet they still get clients due to lack of a way to determine the quality of services they offer beforehand. Moreover, it is not uncommon to have dissatisfied patients opening up legal cases against $MSPs$, only to loose the cases since most expert witnesses would be personnel from the same fraternity as the accused. The essence of reputation based systems is to discourage interactions with parties that repeatedly offer poor services. In the long run, this should have a positive effect on the quality of services offered. In this paper, we wish to propose a system that may improve the quality of service by giving the would-be clients a chance to find the reputation of a MSP before-hand using a privacy preserving reputation system. Now we wish to describe a scenario that motivates us to develop our scheme. Suppose a medical user (MU) wishes to know the best MSP in the neighborhood with regard to a specific medical condition. The MU may or may not be friends with an MSP who can treat their condition. However, since medical services are critical and an MU is keen on quality of service, the MU wishes to poll some MUs who have previously been treated for similar conditions. On the other hand, the medical users who will be polled wish to maintain anonymity since they may not want their reputation score to be known by anyone. In other words, they wish to maintain privacy of the rating they award an MSP. In this paper we wish to propose a scheme that will provide anonymity of the MU who wishes to get the reputation score, and the reputation score awarded by a participating MU in the reputation score computation.

1.1. Requirements

Our goal is to provide a way for medical users to make reputation requests in privacy preserving way to the group members, without anyone including the $Dealer$ i.e. the entity responsible for conducting the reputation computation, from being able to determine who has made a request for the reputation of a particular MSP and the rating awarded by a particular MU chosen to participate in the rating.

Subsequently, we define two requirements that must be met for our objectives to be achieved as follows:

1) The conspiracy of the dealer, group members and any other eavesdroppers cannot determine the member who has made a reputation request better than random guessing.
2) The conspiracy of the group members cannot determine the reputation score given by any MU participating in the reputation computation better than random guessing.

1.2. Our Solution

The scheme that we propose meets all the requirements mentioned above. To meet the first requirement, our scheme uses an ElGamal [1], [2] based anonymous public key generation scheme. All members are in a group hence can send their requests anonymously. They send their reputation requests to the trusted authority. The trusted authority will only verify that the message is from a group member but not know who sent it. This message will be concatenated by a pseudo-public key of an MU. Through this, the anonymity of the MU making a reputation request will be assured. To avoid the anonymity of the MU to be violated upon receiving the reputation request results, the trusted authority will broadcast the results to the group. However, only the MU who requested for the reputation service will be able to decrypt the results. To meet the second requirement, our scheme shall use the multiplicative homomorphic property of ElGamal ciphertexts to encrypt the reputation score and compute it. In this way, it will be difficult for an adversary to determing the reputation score awarded by participating with the MU. Since our proposed scheme is also a recommender system, we wish to describe how the recommender component works. To do the, we shall employ the technique known as $Reputation\ Request\ (RRQ)\ Expansion$. To achieve this, the trusted authority (TA) who is the entity that receives the RR from the MU, and knows all the $MSPs$, will pick k other $MSPs$ depending on the requirements of the MU that made the query, and create a pool of $k+1\ MSPs$. These $k\ MSPs$ picked by the TA should be $MSPs$ who offer similar services as those of interest to the MU that made the query. This pool of $k+1\ MSPs$ will be passed to the dealer who is responsible for the coordination of the reputation computation. The group members elected to participate in the reputation computation will compute the reputation of all the medical services in the pool in a privacy preserving manner.

1.3. Our Contribution

In this paper, we propose to contribute the following;

1) Designing an architecture for a recommender privacy preserving reputation based medical services.
2) Designing an anonymous reputation computation mechanism using a variant of the ElGamal cryptosystem.
3) Designing algorithms for the implementation of our proposed scheme.

The rest of the paper is organized as follows, Section 2 discusses the literature review, Section 3 focuses on our proposed scheme, Section 4 discusses the security analysis and finally Section 5 discusses the conclusion and future work.

2. Literature Review

A lot of research has been conducted in the area of reputation systems. In this section, we shall discuss our motivation for this paper followed by a description of Elgamal cryptosystem and finally we look at the existing literature in reputation systems.

2.1. Motivation

In the real world, it is natural to make enquiries about the quality of service before engaging it. The seriousness of the enquiry will largely be influenced by what is at stake. Medical services are critical in nature. When a patient develops a new condition, they want some level of basic assurance that they are engaging services that are good. This also happens if you have moved to a new neighborhood, or country. A more pertinent reason, which motivated this research, is the number of poor medical services offered by some $MSPs$. We feel that, due to the lack of reputation based medical services, new MUs will often go for services from poor $MSPs$. Literature on poor medical services is a lot [3]-[7]. Our research does not focus on these poor medical services, but rather wish to use this as ground to present a platform that will warn potential MUs of these poor $MSPs$. Often than not, the only sure way to assess whether expected services are good or not depends on recommender systems. Reputation based service provision is all around us, especially in the area of ecommerce. However, the same is largely lacking in the medical field. There is very little research on systems that offer reputation based medical services in academia, despite the critical nature of medical services as opposed to other kinds of service provision such as ecommerce.

2.2. Elgamal Review

The ElGamal cryptosystem was proposed by Taher ElGamal [8]. This cryptosystem is made up of three procedures; the key generation, encryption and decryption procedures. The key generation procedure is as follows. Picking a large prime p and the generator g of a multiplicative group Z_p^* of integers modulo p. Picking a private key a from the group Z such that $1 \leq a \leq p-2$. Compute the $x = g^a mod\, p$. The public key is the tuple (p, g, x). To encryption procedure is as follows. To encrypt a message M, write M as a set of integers $(m_1, m_2, m_3, \dots)$ in the range of $\{1, \dots, p-1\}$. These integers will be encoded one after the other. Pick b at random and compute $y = x^b \; mod\, p$. Then, the ciphertext $c = m_1 \times y \; mod\, p$. Note: pick a new b for each message block m_i. The ciphertext message is (y, c). The decryption procedure is as follows. Compute y^{p-1-a}. Finally, $m_1 = y^{p-1-a} \times c$.

2.3. Reputation Systems

Reputation has been widely used in different areas of study. In computing, it has been applied to Multi-Agent systems [9]-[12], service oriented networks and ecommerce [13]-[15]. Despite a lot of research having conducted in trust and reputation systems, there is a lack of coherence as indicated by fact that most researchers propose new systems from scratch without trying to extend previous proposals [16]. Reputation may be defined as an expectation about an agent's behavior based on information concerning previous interactions. Research and proposals on reputation systems in the medical field are scarce. However, in their survey on general reputation systems, [16] discusses several challenges facing most of the proposed reputation based systems some of which are as follows:

2.3.1. Low incentive for providing rating

Since ratings are typically provided after a transaction has taken place, transaction partners have no direct incentive for providing ratings about the other party. [17] found out that 60.7% of buyers and 51.7% of sellers on eBay provided ratings.

2.3.2. Bias towards positive rating

There is a general positive bias when ratings are provided. [17] found out that only 0.6% of all the ratings provided by buyers and only 1.6% of all ratings provided by sellers were negative, which does not reflect reality. A possible explanation to this is that, positive ratings are given in the hope of getting positive ratings in return [18].

2.3.3. Unfair ratings

This refers to awarding ratings that are unfairly positive or unfairly negative. This is a fundamental problem in reputation systems. Many methods of avoiding this bias have been proposed a lot in literature.

2.3.4. Change of identities

Sometimes parties that have suffered significant loss of reputation might want to change identity in order to start afresh and de-link from the past. One way that this has been put to check is by discouraging change of identities by penalizing newcomers [19].

2.3.5. Ballot box stuffing

This means that the number of raters is higher than should be. It is obvious that ballot stuffing will usually contain too many unfair ratings. In ecommerce platforms such as eBay, ratings can only be offered after transactions are completed. Since each transaction has a fee attached to it, ballot box stuffing is made expensive.

Table 1. List of Parameters

Parameter	Meaning	Parameter	Meaning
MU	Medical User	b_i	Individual Ephemeral Encryption Key
MSP	Medical Service Provider	h	A quasi generator of a sub-group of G of order $(p-1)/2$
TA	Trusted Authority	$E_{y_{TA}}$	Encryption using public key of TA
RRQ	Reputation Request	$D_{x_{TA}}$	Decryption using private key of TA
RR	Reputation Results	TS	Time Stamp
G	Multiplicative Cyclic Group	σ	Digital Signature
p	A large prime in G	p_{rep}	A large prime in G for reputation computation
g	A generator of G	g_{rep}	A generator of G for reputation computation
a_i	Individual Private Key	a_{rep_i}	Individual Private Reputation Computation Key
y_i	Individual Decryption Key	x_{rep_i}	Individual Public Reputation Computation Key
x_i	Individual Public Key	y_{rep_i}	Individual Decryption Reputation Computation Key
k	Number of $MSPs$ used in Masking	b_{rep_i}	Individual Ephemeral Encryption Reputation Computation Key
l	Number of MUs used in Reputation Computation		

3. Our Proposed Scheme

3.1 Our Architecture

We now describe the architecture of our proposed privacy preserving reputation based medical service.

The parameters in this architecture are listed in Table 1. The architecture (see Fig. 1) is comprised of a number of processes as follows. First, an MU who wishes to get a reputation score of an MSP will contact the TA, with a Reputation Request (RRQ). The TA will expand this list of $MSPs$ through a process known as $RRQ — Expansion$, by adding k new $MSPs$ to make $k+1$ $MSPs$. The new $MSPs$ should be offering similar services as the MSP whose reputation is being queried. The TA will then pass the $Expanded — RRQ$ to the $Dealer$ who is responsible for the task of carrying out the Expanded Reputation Computation. The $Dealer$ will perform the reputation computation by randomly selecting a number of MUs to participate in the reputation computation. Upon completing the reputation computation, the $Dealer$ will pass the $Expanded\ Reputation\ Results$ (RR) to the group. The MU user who requested the service will then access the$Expanded — RR$. Armed with an array of reputation scores in his hands, the MU can make a better decision of who to consult for their medical condition. In other words, not only did the MU receive the reputation scores of the MSP of his interest, but also, received recommendations on others whose ratings may be higher or lower compared to the one he asked for.

3.2 Description of Our Proposed Scheme

3.2.1. System initialization

The TA will be responsible for initializing the system. He will register the MUs and $MSPs$ and set the stage for the process of electing a $Dealer$ and the $Backup - Dealer$ through some privacy preserving voting protocols. The $Backup - Dealer$ will act when the $Dealer$ is not available before the election of another $Dealer$.

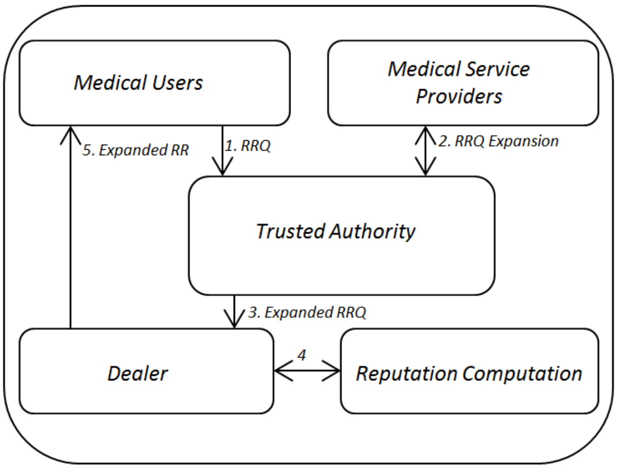

Fig. 1. Reputation based medical services architecture.

3.2.2. Communication keys setup

The TA also will initiate the process of key agreement. Using the multiplicative Cyclic Group G, he will choose p to serve as group's shared public key and distribute it to all the MUs. To achieve anonymity, we create a feasible system of calculating and submitting anonymous public keys in the group. First, the messages must be sent to a group of addresses to maintain anonymity on hardware level. This means that numerous people's messages will be sent to the same place. Secondly, an anonymous public key encryption should hide the recipient's identity as much as possible regardless of whether the senders are correlating their data with each other.

To achieve this anonymity in Elgamal's encryption, the recipient's public key is given to senders as a power of the generator. Because the recipient's private key is obscured by the generator, it is possible for the recipient to use the same key with multiple different generators without giving away the private key. Then a group of people can conceal their identities by having all their messages sent to the same address by using multiple public keys. These keys will be disposable, so that no information can be gained by their reuse.

Each MU is required to generate a number of generators for the previously agreed value of p. Since this value of p is large, and there is no known efficient algorithm for computing generators, MUs will generate quasi-generators using their private keys. Care must be taken to generate quasi-generators that are secure. To generate a quasi-generator we use $h = g^2(\text{mode}\, p)$. These have order $(p-1)/2$, the largest possible factor of p – 1. For large p, these quasi-generators will be large enough to allow the generation of many pseudo public keys that can be used with a single private key. The message space is described as the set of integers which are generated by h. Then, each MU chooses a private key and publishes multiple public keys using it, where for every new encryption a random exponent number b is used for encoding. That is, group member chooses various $g's$ and then calculates the values of x which correspond to their private key. Each group member calculates their corresponding public keys; $x_{ind} = g_{ind}{}^{a}$ (where a is individual secret key). Anyone can verify that these were computed correctly by asking for a zero knowledge proof. x_{ind} for all $ind = 1, \dots, n_{indk}$ will then be published and verified.

3.2.3. Implementation

The implementation of the scheme will run as follows:

1) An MU_i with the need for a reputation score of a certain MSP_j will make an RRQ to the TA in the following format.

$$RRQ_{MU_i} = E_{y_{TA}}(TS_{MU_i}||RRQ_{MSP_j}||x_{ind_{MU_i}}||\sigma_{MU_i})$$

2) The TA will decrypt the message and verify the signature using the public key in the message.

$$D_{x_{TA}}\left(RRQ_{MU_i}\right) = (TS_i||RRQ_{MSP_j}||x_{ind_{MU_i}}||\sigma_{MU_i})$$

3) The TA will then expand the request by carefully adding k more $MSPs$ who offer similar services as the queried MSP to make $+1$ $MSPs$. The value of k depends on the requirements of the MU_i.

$$Expanded - RRQ = (TS_{TA}||RRQ_{MSP_1}|| \dots ||RRQ_{MSP_{k+1}}||x_{ind_{MU_i}}||\sigma_{MU_i}||\sigma_{TA})$$

4) The TA will then encrypt the new RRQ_i, for $i = 1\ to\ k + 1$ and send it to the $Dealer$.

$$E_{y_{Dealer}}(Expanded - RRQ)$$

5) The $Dealer$ decrypts the message and verifies that the first signature belongs to the TA and the second one belongs to a valid MU.
6) The $Dealer$ randomly picks l MUs to participate in the reputation computation score, where l depends on the confidence level requirement of MU_i.
7) The $Dealer$ then conducts a reputation computation process as explained in the next section and obtains a $Expanded - RR$.

$$Expanded - RR = (RRQ_{MSP_1}|| \dots ||RRQ_{MSP_{k+1}}||RR_{MSP_1}\ || \dots ||RR_{MSP_{k+1}}||x_{ind_{MU_i}}||\sigma_{MU_i})$$

8) The $Dealer$ encrypts and sends the $Expanded - RR$ back to the group.

$$x_{ind_{MU_i}}(TS_{Dealer}||Expanded - RR_{MU_i}||\sigma_{Dealer})$$

9) MU_i who made the RRQ is now able to access the $Expanded - RR$ and take a decision.

3.2.4. Reputation feedback

Now we describe the reputation feedback process. The $Dealer$ randomly selects $l\, MUs$. These are the MUs who will compute a reputation score for the $Expanded - RRQ$ for user MU_i received from the TA. Each of these MUs will compute a reputation score for all the $k+1\, MSPs$ in the $Expanded - RRQ$. Each participating MU will encrypt his reputation feedback. First, the $Dealer$ will choose p_{rep} and g_{rep} and ask each individual to create private keys a_{rep_i}, for $i = 1\ to\ l$ and compute;

$$x_{rep_i}{=}g_{rep}^{a_{rep_i}} mod\ p \tag{1}$$

To create their public keys. Again, anyone can verify these were computed correctly by asking for a zero knowledge proof.

The resulting individual public keys will be multiplied together forming the last portion of Elgamal's public key. We call this value X_{rep}, which is calculated as follows:-

$$X_{rep} = \prod_{i=1}^{l} x_{rep_i} \tag{2}$$

Recall that in Elgamal encryption the cipher text is represented as a pair (y, c). In order to calculate this pair, the sender must choose an integer b from z_{p-1} using a uniformly random method. This means that the possibility of randomly choosing any number should be $1/(p-2)$. Every MU must publish a decryption key:

$$y_{rep_i} = X_{rep}^{b_{rep_i}} mod\ p \tag{3}$$

Anyone can verify that these were computed correctly by asking for a zero knowledge proof. We need to multiply all y_{rep_i} for all $i = 1\ to\ l$ to incorporate all the private keys in our decryption. We call this value Y_{rep}. Y_{rep} is the shared secret calculated as follows:

$$Y_{rep} = \prod_{i=1}^{l} y_{rep_i} \tag{4}$$

The protocol allows each to score a "yes" by encrypting $m_{rep} = 2^1$, "neutral" by encrypting $m_{rep} = 2^0$ or "no" by encrypting $m_{rep} = 2^{-1}$, to get the second ElGamal ciphertext c_{rep} as follows:

$$c_{rep_i} = X_{rep}^{b_{rep_i}} m_{rep_i}\, mod\ p \tag{5}$$

where X_{rep} is the computed shared public key, m_{rep} is the secret message (in our case, private reputation feedback) and a random exponent b_{rep_i}. It is unlikely that two votes will look the same because of random exponent b_{rep_i} that is referred to as ephemeral key and that was used to generate decryption key y_{rep_i}.

Again, we need to perform a check. This time we need to make sure that no one is trying to cheat by voting with "extra" confidence. For example, 2^2 would be counted as two positive reputation votes when they are totaled. The way to check for this is by use of Zero Knowledge Proof that can also be achieved non-interactively.

3.2.5. Reputation computation

Since Elgamal's encryption is multiplicative homomorphic, we utilize the exponential ElGamal to calculate the encryption of all reputation scores Enc_{Total} as follows:

The individual encrypted private reputation score of each MU; $Enc_{rep_i} = c_{rep_i}$, for all i, where $i = 1\ to\ l$. The total encrypted private reputation score of all the l participants is;

$$Enc_{Total} = \prod_{i=1}^{l} Enc_{rep_i} \tag{6}$$

The Dealer then Decrypts this message:

$$Decrypt\ (Enc_{Total}) = \frac{Enc_{Total}}{Y_{rep}} = \prod_{i=1}^{l} m_{rep_i} \tag{7}$$

Since, m_{rep_i} takes the values $2^{-1}, 2^{0}$ or 2^{1}, the $Dealer$ sums up the exponents so that the resulting exponent is the total reputation score.

3.2.6. Correctness of the reputation computation

$$\begin{aligned} Enc_{Total} &= \prod_{i=1}^{l} Enc_{rep_i} \\ &= \prod_{i=1}^{l} c_{rep_i} \\ &= \prod_{i=1}^{l} X_{rep}^{b_{rep_i}} m_{rep_i} \\ &= \prod_{i=1}^{l} X_{rep}^{b_{rep_i}} \prod_{i=1}^{l} m_{rep_i} \end{aligned} \tag{8}$$

Recall from equation 3 that

$$y_{rep_i} = X_{rep}^{b_{rep_i}} mod\ p$$

Hence equation 6 becomes

$$= \prod_{i=1}^{l} y_{rep_i} \prod_{i=1}^{l} m_{rep_i} \tag{9}$$

Following from equation 4, equation 7 becomes

$$Enc_{Total} = Y_{rep} \prod_{i=1}^{l} m_{rep_i}$$

Hence

$$\frac{Enc_{Total}}{Y_{rep}} = \prod_{i=1}^{l} m_{rep_i} \tag{10}$$

Since these were constructed as 2^{-1}, 2^{0} or 2^{1}, the exponents will be added together so that the resulting exponent is the total reputation feedback. The resulting value should be the same as the encrypted ciphertexts value which was earlier computed homomorphically.

However, it should be noted that every participating group member should publish his/her values of x_{rep_i} and y_{rep_i}. Refusing to publish these values will cause other participants to recalculate the privacy reputation feedback result after omitting that defaulting member feedback. Further, since all the encrypted totals as well as the decryption keys are all public, the results may be verified by any of the participants. This means that in order to find out what one participant's reputation feedback was, the entire group would have to work together to find this because the reputation feedbacks are combined before they are decrypted.

Algorithm 1: Recommender Privacy Preserving Reputation for Medical Services (RPPRMS)

```
Input: $< RRQ >$
Output: $< Expanded - RR >$

1. $MU_i$ makes $RRQ$ to the $TA$ as follows $RRQ_{MU_i} =$
     $E_{y_{TA}}(TS_{MU_i}||RRQ_{MSP_j}||x_{ind_{MU_i}}||\sigma_{MU_i})$
2. Decryption by $TA$: $-$
     $D_{x_{TA}}\left(RRQ_{MU_i}\right) = (TS_i||RRQ_{MSP_j}||x_{ind_{MU_i}}||\sigma_{MU_i})$
3. Implement $RRQ$ Expansion:
     $Expanded - RRQ$
     $= (TS_{TA}||RRQ_{MSP_1}|| \dots ||RRQ_{MSP_{k+1}}||x_{ind_{MU_i}}||\sigma_{MU_i}||\sigma_{TA})$
4. Encrypt $Expanded - RRQ$ and send to dealer:
     $E_{y_{Dealer}}(Expanded - RRQ)$
5. Dealer decrypts and execute Algorithm 2 and obtain:-
     $Expanded - RR = (RRQ_{MSP_1}|| \dots ||RRQ_{MSP_{k+1}}||$
     $RR_{MSP_1} || \dots ||RR_{MSP_{k+1}}||x_{ind_{MU_i}}||\sigma_{MU_i})$
6. Encrypt Expanded and broadcast to the group:
     $E_{x_{ind_{MU_i}}}(TS_{Dealer}||Expanded - RR||\sigma_{Dealer})$
7. $MU_i$ decryption:
     $D_{x_{ind_{MU_i}}}\left(E_{x_{ind_{MU_i}}}(TS_{Dealer}||Expanded - RR||\sigma_{Dealer})\right)$
     $= (TS_{Dealer}||Expanded - RR||\sigma_{Dealer})$
8. Return: $Expanded - RR$
```

Algorithm 2: Reputation Feedback Collection

```
Input: $< Expanded - RRQ>$
Output: $< Expanded - RR >$

1. Dealer randomly select $l\ MUs$;
2. Dealer select $p_{rep}\ and\ g_{rep}$ and distribute to the $l$
     MUs;
3. Each $MU$ computes $x_{rep_i}$=$g_{rep}^{a_{rep_i}} mod\ p$, ($a_{rep_i}$ is
     secret) – (Eq. 1) and publish $x_{rep_i} mod\ p$ for
     verification;
4. for $i = 1\ to\ l$ do (Calculate group shared key)
5.     $X_{rep} = \prod_{i=1}^{l} x_{rep_i}\ mod\ p$ (Eq. 2);
6. endfor
7. Each MU computes decryption key:- $y_{rep_i} =$
     $X_{rep}^{b_{rep_i}} mod\ p$ ($b_{rep_i}$ is random exponent) - (Eq. 3)
     and publish $y_{rep_i}$ for verification;
8. for $i = 1\ to\ l$ do (Calculate shared decryption key
     (Share secret))
```

```
        $Y_{rep} = \prod_{i=1}^{l} y_{rep_i} mod\ p$ - (Eq. 4);
endfor
Each MU computes second Elgamal ciphertext as
    follows:- $c_{rep_i} = X_{rep}^{b_{rep_i}} m_{rep_i}\ mod\ p$ - (Eq. 5)
for $i = 1\ to\ l$ do (compute total reputation scores)
        $Enc_{Total} = \prod_{i=1}^{l} Enc_{rep_i}\ mod\ p$ - (Eq. 6)
endfor
Dealer will decrypt as follows:-
    $Decrypt\ (Enc_{Total}) = \frac{Enc_{Total}}{Y_{rep}} = \prod_{i=1}^{l} m_{rep_i} mod\ p$ -
    (Eq. 7)
Return $\boldsymbol{Expanded - RR}$
```

4. Security Analysis

Our proposed architecture derives its basic security on the security of the ElGamal cryptosystem and the ElGamal digital signature. Further, it is secure against the replay attacks by way of using timestamps along the communication channels.

Identity privacy preserving: we claim that the conspiracy of the dealer, other group members and any other eavesdroppers cannot determine the MU who has made a reputation request better than random guessing. Privacy preservation of the MU requesting for reputation scores of a MSP is guaranteed by the use of pseudo-public keys which are disposable after a single use. Since, reputation rating requests is not a very frequent events, this is possible to have several pseudo-public keys lasting for a long time. As such the probability of linking a particular RRQ a particular MU is:

$$\Pr\left(MU_{RRQ}\right) = \frac{1}{n} \tag{11}$$

where MU_{RRQ} refers to an MU that made a particular reputation request.

Reputation score privacy preserving: in our proposed scheme, the reputation score of an MU on a certain MSP is kept private. This meets our second requirement which requires that, the conspiracy of the group members cannot determine the reputation score given by any MU participating in the reputation computation better than random guessing. Subsequently, it can be shown that the probability for linking a particular reputation score to an MU is given by:

$$\Pr\left(MU_{Ind\_Rep\_Score}\right) = \frac{1}{3nl(k+1)} \tag{12}$$

where $MU_{Ind\_Rep\_Score}$ refers to the individual reputation score of an MU that is participating in the reputation computation.

5. Conclusion

In this paper we propose a novel architecture for a recommender privacy preserving reputation based medical services system. The architecture provides privacy preservation to both the party that makes a request for the reputation request of an MSP and the reputation score awarded by particular participating MU. Further, the scheme recommends other $MSPs$ which offer similar services to the MU that initiated the request. This way, all entities participating in the protocol have the privacy of their contributions is assured. Our architecture uses a novel version of the ElGamal cryptosystem to perform the identity privacy preservation as well individual reputation score privacy. In our future work, we wish to implement this system on mHealth systems based on cloud computing.

References

[1] Helgeson, M. (2007). Security and applications of ElGamal's encryption algorithm. University of Minnesota, Morris.

[2] Waters, B. R., Felten, E. W., & Sahai, A. (2003). Receiver anonymity via incomparable public keys. *Proceedings of the 10th ACM Conference on Computer and Communications Security* (pp. 112-121).

[3] Casey, A. T. (2014). The ugly face of medical negligence: Where has justice gone? *European Spine Journal*, *23*, 1-3.

[4] Muller, J. G. (2013). Medical liability reform in the United States: A comprehensive approach to medical error. *Proceedings of the GREAT Day*.

[5] Bryden, D., & Storey, I. (2011). Duty of care and medical negligence. *Continuing Education in Anaesthesia, Critical Care & Pain*, *11*, 124-127.

[6] Gogos, A. J., Clark, R. B., Bismark, M. M., Gruen, R. L., & Studdert, D. M. (2011). When informed consent goes poorly: A descriptive study of medical negligence claims and patient complaints. *Med. J. Aust.*, *195(6)*, 340-344.

[7] Kessler, D. P. (2011). Evaluating the medical malpractice system and options for reform. *The Journal of Economic Perspectives: A Journal of the American Economic Association*, *25*, 93.

[8] ElGamal, T.(1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *Advances in Cryptology* (pp. 10-18).

[9] Sabater, J., & Sierra, C. (2002). Reputation and social network analysis in multi-agent systems. *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1* (pp. 475-482).

[10] Huynh, T. D., Jennings, N. R., & Shadbolt, N. R. (2006). An integrated trust and reputation model for open multi-agent systems. *Autonomous Agents and Multi-Agent Systems*, *13*, 119-154.

[11] Ramchurn, S. D., Huynh, D., & Jennings, N. R. (2004). Trust in multi-agent systems. *The Knowledge Engineering Review*, *19*, 1-25.

[12] Pinyol, I., & Sabater-Mir, J. (2013). Computational trust and reputation models for open multi-agent systems: A review. *Artificial Intelligence Review*, *40*, 1-25.

[13] Zhao, H., & Li, X. (2013). VectorTrust: Trust vector aggregation scheme for trust management in peer-to-peer networks. *The Journal of Supercomputing*, *64*, 805-829.

[14] Li, Z., Shen, H., & Sapra, K. (2013). Leveraging social networks to combat collusion in reputation systems for peer-to-peer networks. *IEEE Transactions on Computers*, *62*, 1745-1759.

[15] Xue, W., Liu, Y., Li, K., Chi, Z., Min, G., & Qu, W. (2012). DHTrust: A robust and distributed reputation system for trusted peer-to-peer networks. *Concurrency and Computation: Practice and Experience, 24*, 1037-1051.

[16] Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*, 618-644.

[17] Resnick, P., & Zeckhauser, R. (2002). Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. *Advances in Applied Microeconomics*, *11*, 127-157.

[18] Chen, M., & Singh, J. P. (2001). Computing and using reputations for internet ratings. *Proceedings of the 3rd ACM Conference on Electronic Commerce* (pp. 154-162).

[19] Zacharia, G., Moukas, A., & Maes, P. (2000). Collaborative reputation mechanisms for electronic marketplaces. *Decision Support Systems, 29*, 371-388.

Angolo Shem Mbandu received his B.Ed. degree in technology from Moi University, Eldoret, Kenya in 1997. He received his M.Sc. degree in information systems from the University of Nairobi, Nairobi, Kenya in 2009. Currently he is a PhD candidate in the Department of Computer Science and Engineering at the University of Electronic Science and Technology of China, Chengdu, PR China. His research interest is applied cryptography.

Chunxiang Xu received her B.Sc., M.Sc. and Ph.D. degrees at Xidian University, in 1985, 1988, and 2004 respectively, PR China. She is presently engaged in information security, cloud computing security and cryptography research as a professor at the University of Electronic Science Technology of China (UESTC).

Kamenyi Domenic Mutiria was born in Kenya on September 4, 1972. In October, 1996, he obtained a B.Sc. degree in statistical math's and computing from the Kenyatta University, Kenya. Then he graduated with a M.Sc. degree in information systems from the University of Nairobi, Kenya, in March, 2005. In June, 2014, he graduated with a Ph.D. degree in computer science and technology from the University of Electronic Science and Technology of China (UESTC), PR China.

From July 1997 till date, he has been working in Nairobi, Kenya with the Office of the Auditor-General as an assistant manager in charge of ICT Audit. He has four years part-time teaching experience in IT with Kenya Methodist University. Previously, he worked with Teachers Service Commission of Kenya and Group 4 Security, Kenya. Some of his publications are 1) Kamenyi, D. M., *et al*., Authenticated privacy preserving for continuous query in location based services. *Journal of Computational Information Systems*, *9(24)*, 9857-9864; 2) Kamenyi, D. M., *et al.* Preserving users' privacy for continuous query services in road networks. *Proceedings of 2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering*: *Vol. 1* (pp. 352-355); 3) Kamenyi, D. M., *et al*. Optimizing placement of mix zones to preserve users' privacy for continuous query services in road networks. *Proceedings of 2013 9th International Conference on Advanced Data Mining and Applications* (pp. 323-335).

His current research interests are network security and privacy, location based services privacy, cloud based systems, reputation systems, and security protocols.

Dr. Kamenyi is a CISA holder (certified information systems auditor). He also holds the CCNA (cisco certified network associates) and CCNP (cisco certified network professional) certificates.

Gabriel Kofi Armah received his B.Sc. degree in computer science in 1997 from the KNUST in Ghana and obtained the master degree in MIS from the University of Ghana in 2003. Currently he is doing with his Ph.D. program in software engineering at the UESTC in China. He has done a two year compulsory national service in Ghana. He is a computer science lecturer at the University for Development Studies, Ghana. He also has some publications to his credit. His research interests include software engineering, algorithms, data mining using machine learning and Weka.