



A primary resource for reliable information on the application and use of information technology in all aspects of health and health care nationally, regionally and internationally.

Inaugurating Free-Roaming Mobile Agent(FRoMA) Based Secured e-Health Model

S.Venkatesan¹, C.Chellappan¹

¹Department of CSE,Anna University, India

This article is available from: <http://www.ehealthinternational.net/>

Abstract

e-Health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the internet and related technologies. Mobile agent technology is suitable for the e-Health system to get the medical tips from the doctors or other medical information. The proposed model of this paper uses the advanced mobile agent technology for the distributed e-Health model is Free-Roaming Mobile Agent. It will roam around the network to collect medical information and suggestions. In addition this paper provides protocol to protect the security for the information collected by the FRoMA.

Introduction

e-Health is the new general "buzzword" used to characterize not only "Internet medicine", but also virtually everything related to computers, medicine and health care. e-Health is useful for physicians and patients through online sources and enabling information exchange and communication in a standardized way between health care establishments with minimal delay. Mobile agent based e-Health model is more effective than the direct link method because it avoids network traffic. Mobile agent is a software program, which moves from one system (sender) to another system (remote host) to collect the information on behalf of its sender and return back to the sender with the collected information. Physicians, patients or consumers in the e-Health model forward their agent in the network to collect information they require from the relevant server without direct interaction. Mobile Agent will get degraded in its performance when the information available in a large number of servers. Because if we want to collect the information from more than one server then the mobile agent moves to the first remote server, collects the desired information and returns to the sender. Next time the sender again forwards the agent to the another remote server

and back to the sender with the information. This will continue until all the information is collected by the mobile agent from all the remote servers. For this reason, we incorporate the FRoMA model[1] for the distributed e-Health model.

Free-roaming mobile agent is also the same software program to roam around the network to collect information. It moves from one host to another host continuously without returning to the owner each time like the ordinary mobile agent. The movement of the agent to the next host is decided by the remote host where the agent is currently residing. Decision is depends on the requirements and current conditions. In this paper we propose this type of free roaming mobile agent for the distributed e-Health model.

This paper is discussed as follows. In segment 2, we discuss the previous works in this environment. In segment 3, we specify the notations. In segment 4, we show the architecture of the FRoMA based model for the e-Health service. In segment 5, we analyze the performance of the ordinary and Free Roaming Mobile agent and in the segment 6 and 7 the security threats and the protections protocols for the FRoMA will be discussed,

segment 8 gives the experimental result and at finally in the segment 9, we conclude discussion of our model.

2.Previous Work

In reference paper[5], they proposed the security for the e-Health information which is carried out by mobile devices and passed to the medical server through mobile communicators. They concentrate on the issues of threats to confidentiality, threats to integrity and threats to authenticity. Security protection is provided in all the layers of the protocol. The information about the patient are periodically sent to the medical server.

The author of paper[6] provides an analysis of the reduction of medical expenditure through e-Health systems. Medical information is categorized as per patient visits to the hospital. It is based on type of diseases and medicine.

In paper[7], author provides a model for the mobile e-Health services. The proposed idea of the authors of [5] is also the same but with a different methodology.

3. Notations

The Notations used in this paper are represented in the following table

Table 1.Notations

Notations	Description
S	Server
Li	List of servers to visit
R	Requirements
$S_0= S_{n+1}$	Originator or Creator or Owner.
o_0	Offer from S_0 to identify the agent instance on return.
oi	Offer from S_i .
Pbi, Pri	Public and Private key of the host S_i .
$tPbi, tPri$	Temporary Public and Private key of the host S_i .
$EncPbi(m)$	Message m is encrypted with the public key Pbi of S_i .
$SigPri(m)$	Signature of S_i on message m with its private key Pri .
$H(m)$	Hash function.
$O_i, 1 \leq i \leq n$	Encapsulated offer.
$C_i, 1 \leq i \leq n$	Cryptographically encrypted offer of S_i .
$t0I$	Time taken to travel from Server S_0 to S_1
P_i	Processing time of the Server i . It also includes all the time taken for the security issue
T_i	Total time spent for each server

4.FRoMA based Model for e-Health Environment

Authors in the reference list cited about use the mobile e-Health model. Information is transferred to the medical server from the remote place using the mobile device. Here, we show the agent based e-Health model, which reduces network traffic. [5][8] It collects information about the patient and stores it in medical servers.

Information is gathered from the servers by the clients (physician or patient) for further processing. Our model shows how to free roaming mobile agent gathers information from the various servers. Information may be consultancy or patient details. Information may be available in a number of servers or the client needs the information from various remote servers. We propose the model for collecting information from various remote medical servers on behalf of the client.

FRoMA based e-Health model is shown in the Figure 1, with four servers and directory. Here, the patient or doctor forwards its mobile agent to collect health tips or patient information from various servers. Agent will first visit the directory or registry for the availability of servers having the related information. Information collected from all the servers collectively is called "full result". Information from a single server is "partial result". Where S_1, S_2, \dots, S_5 are the servers (medical servers) consist of medical information. The role of each in the e-Health environment by using free roaming mobile agent are as follows:

Patient or physician S_0 : Physician who needs information should forward the free roaming mobile agent with the requirements to the Directory to collect the list of servers.

Directory D : It receives the agent and gets the requirements from the agent of the physician. Then processes the requirements and provides the list of servers to the agent for which they visit.

S_0 : Receives the agent with the list of servers from the directory and makes a copy of the list for the future and forward the agents with the requirements and list to the next server, which is nearer to them.

Medical Server S_1 : Receives the agent and its requirements then processes the requirements and provides the information relevant to the requirements. After that, it checks the list and forwards

the agent to the next server S_2 with the list and information. This process is followed all other remote servers.

FRoMA: The function of the FRoMA is to only carry the information provided by the various servers.

The functions of the e-Health environment depicted in figure.1 are

- 1: $S_0 \rightarrow D$: Agent from client(physician or patient) to Directory D with some authentication id and requirements (id, R)
- 2: $D \rightarrow S_0$: Li, R
- 3: $S_0 \rightarrow S_1$: Li, R
- 4: $S_1 \rightarrow S_2$: o_1 , Li, R
- 5: $S_2 \rightarrow S_3$: o_1 , o_2 , Li, R
- 6: $S_3 \rightarrow S_4$: o_1 , o_2 , o_3 , Li, R
- 7: $S_4 \rightarrow S_5$: o_1 , o_2 , o_3 , o_4 , Li, R
- 8: $S_5 \rightarrow S_0$: o_1 , o_2 , o_3 , o_4 , o_5 , Li, R

The transaction 8 represents that the free roaming agent is returning to the home after collecting all the medical information from the various servers. After receiving the agent, patient or physician, it gets the information and make use of it.

Functions of the Remote servers in the distributed e-Health environments are as follows

Agent at S_1

- Receive Li, R
- Computer Offer o_1
- Decide next host S_2

$S_1 \rightarrow S_2$: o_1 , Li, R

Agent at S_2

- Receive o_1 , Li, R
- Computer Offer o_2
- Decide next host S_3

$S_2 \rightarrow S_3$: o_1 , o_2 , Li, R

Agent at S_5

- Receive o_1 , o_2 , o_3 , o_4 , Li, R
- Computer Offer o_5

Decide next host S_0 (all hosts are visited by the agent, so the host S_5 decided to forward the agent to the sender, creator or owner).

$S_5 \rightarrow S_0$: o_1 , o_2 , o_3 , o_4 , o_5 , Li, R

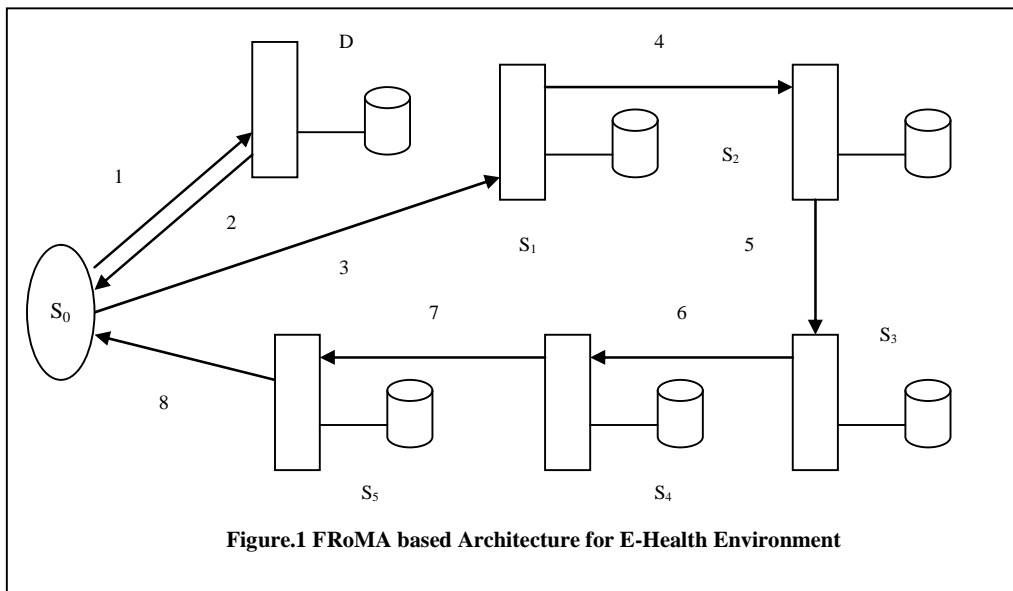


Figure.1 FRoMA based Architecture for E-Health Environment

5.Performance between ordinary mobile agent and FRoMA

The performance among the two is represented in the following table for the three servers. Here the time taken to collect the list of servers from the directory is not included because it is common for both the ordinary mobile agent the FRoMA model.

Table.2 Performance

Agent from S0	S ₁	S ₂	S ₃	Total time
Ordinary Mobile Agent	Tt ₁ =t ₀₁ +P ₁ +t ₁₀	Tt ₂ =t ₀₂ +P ₂ +t ₂₀	Tt ₃ =t ₀₃ +P ₃ +t ₃₀	$\sum_{i=1}^3 Tt_i$
FRoMA	Tt ₁ =t ₁₂ +P ₁	Tt ₂ =T ₂₃ +P ₂	Tt ₃ =t ₃₀ +P ₃	$\sum_{i=1}^3 Tt_i + T_{01}$

Performance given in the table between the ordinary mobile agent and the free roaming mobile agent differs by a ratio of 3:2

6.Security issues in the FRoMA based e-Health model

The various security issues in the free roaming mobile agent models are

- Unauthorized persons can access the medical information from the servers.
- Information collected from one server can be destroyed or altered by another server.
- Server providing medical information can deny that this is not my offer.
- Medical information collected from the server will be understandable by the others.
- The visited server can be visited again and again [4].
- Fake malicious information can be inserted into the middle of the collected offers [8].
- More than one server can collude with one another and destroy the collected offer or alter the data [1]:.

7.Protection Models

Protection for the above security issues can be provided by the following mechanism.

- **Authentication:** Unauthorized access can be avoided by giving the personal identification information to the patient or physician to collect the information from the medical servers. The client should contact the directory with the personal

identification and requirements. The directory should check the ID with the database and provide the requirements(list of servers) if they are valid users.

- **Data Confidentiality:** Information collected from the servers is encrypted with the public key of the owner of the agent. Only the owner of the free roaming mobile agent can decrypt the information with their private key.
- **Data Integrity:** It is impossible for an attacker to modify or replace any offer because of the hash function used.
- **Non Repudiation:** Each piece of information must have to signed by the corresponding server. So, the server cannot deny its information after the client receives the information.
- **Insertion Defense:** No information can be inserted in the middle by malicious server because the identities will repeat more than once in the chain [1].
- **Colluded Attacks & Revisiting Attack:** These are protected by the identity checking model.

An algorithm providing the protection model is represented below. Server Si receives the agent from the previous server Si-1 and verify the offers identification. After that it will generate its data and forward the next server Si+1.

$$\begin{aligned}
 S_i: & \text{Receive } O_0, O_1, O_2, O_3, \dots O_{i-1}, tPb_{i-1} \\
 & \text{Recover } C_{i-1}, h_{i-1} \text{ by } tPb_{i-1} \\
 & \vdots \\
 & \text{Recover } C_0, h_0 \text{ by } Pb_0 \\
 & \text{Ver}(Sig_{tpri-3}(S_{i-2}, tPb_{i-4}), Sig_{tpri-2}(S_{i-1}, tPb_{i-3}), \\
 & \quad Sig_{tpri-1}(S_i, tPb_{i-2}), tPb_{i-1}, r_0) \\
 & \text{recover } S_{i-2}, S_{i-1}, S_i \\
 & \vdots \\
 & \text{Ver}(Sig_{pr0}(S_0), Sig_{tpri}(S_1), Sig_{tpri}(S_2, tPb_0), \\
 & \quad tPb_1, r_0) \text{ recover } S_0, S_1, S_2 \\
 & \text{Ver}(Sig_{pr0}(S_0), Sig_{tpri}(S_1), tPb_0) \text{ recover } S_0, S_1
 \end{aligned}$$

It receives the computer offer, recovers the identities and compares the last two and first two identities. If both are same, the host decides no

attack on the data. Otherwise, an attack is identified and then the host sends the agent to its home.

It will match from O_0 to O_{i-1} for reliability of the chain. After the verification process, the host S_i generates its offer, makes the hash function and forwards the agent to its next host S_{i+1} .

Generate offer o_i
 Compute $C_i = Enc_{pb_i}(Sig_{pri}(o_i), pb_i)$
 Generate tPr_i, tPb_i
 Decide next host S_{i+1}
 $h_i = H(Sig_{tpri-2}(S_{i-1}, tPb_{i-3}), Sig_{tpri-1}(S_i, tPb_{i-2}), Sig_{tpri}(S_{i+1}, tPb_{i-1}, tPb_i))$
 $O_i = Sig_{tpri}(C_i, h_i)$

$S_i \rightarrow S_{i+1}: O_0, O_1, O_2, O_3, \dots, O_i, tPb_i$

The owner of the agent (patient or physician) will decrypt and check the signature of all the medical information server (may be physician) and they can use the information.

8.Experimental Result

The proposed model is implemented using the IBM Aglet server using Java. It is tested in our laboratory (LAN) with the bandwidth of 50mbps

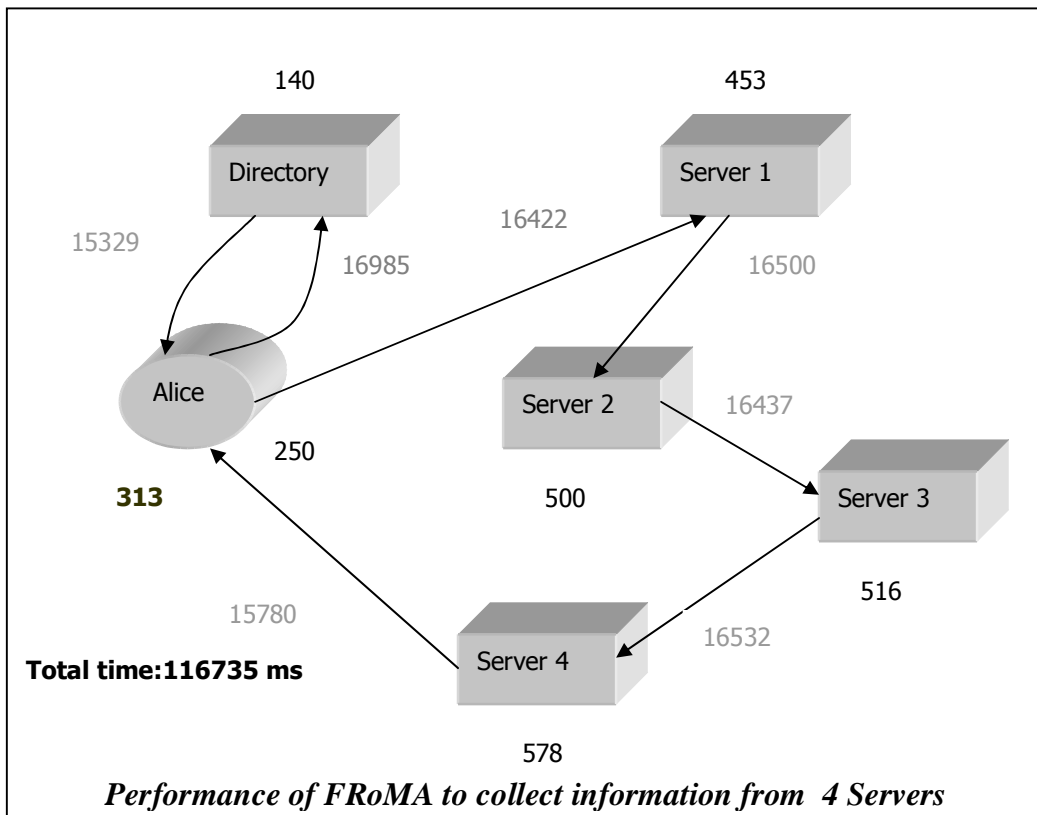
connected with 100 machines, where all machines are sharing the data with one another. We have shown the result in Figure.2

Client sent the free roaming mobile agent to the e-learning environment to gather information from the 4 medical servers. Figure 2 shows the migration time of the agent from one host to another host in gray color and the computation time of the each server is in black color.

Value darken in the client is the time taken by the machine to give the collected original information after decrypting and checking the signature. Computation time includes the offer generating time, next server selection time, cryptology time and verification time. Values in the Figure 2 are in milliseconds.

9.Conclusion

Nowadays e-Health model is emerging to improve e-service and well being of all people. Mobile agent is preferred for the e-Health model to collect the medicinal information with out network traffic. Free roaming mobile agent visits the remote servers, which are nearer to the current server. By this we can reduce the time to collect the information with the full security through our protocol.



Patient or physician can get qualified consultation or idea from other physicians using this model. Our model should improve e-Health services to the medical community.

Acknowledgment

This Work is supported by the NTRO, Government of India. NTRO provides the fund for collaborative project "Smart and Secure Environment" and this paper is modeled for this project. Authors would like to thank the project coordinators and the NTRO members.

References

1. D.Xu, L.Harn, M.Narasimhan, J.Luo. "An Improved Free-Roaming Mobile Agent Security Protocol against Colluded Truncation Attacks." In Proceedings of the 30th Annual international Computer Software and Applications Conference (COMPSAC,06), Volume 2, Page(s):309 – 314, Chigago, Sept. 2006, IEEE Computer Society Press.
2. Hasan Al-sakran "Developing E-learning system using Mobile Agent Technology" In Information and Communication Technologies of IEEE, volume 1, pages 647-652, 24-28 April 2006
3. H. Al-Sakran, "An Agent-based Architecture for Developing E-learning System", Information Technology Journal 5(1), 2006, pp: 121-127.
4. J. Zhou, J. Onieva, and J. Lopez. "Analysis of a Free Roaming Agent Result-Truncation Defense Scheme". In Proceedings of 2004 IEEE Conference on Electronic Commerce, pages 221--226, San Diego, USA, July 2004, IEEE Computer Society Press.
5. Ramon Marti, Jaime Delgado and Xavier Perramon, "Security Specification and Implementation for Mobile e-Health Services". In Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04), 2004
6. Masatsugu Tsuji, Fumio Taoka and Masaaki Teshima, "An Analysis of Reduction in Medical Expenditures by e-Health Systems: Case of Nishiaizu Town, Fukushima Prefecture, in IEEE transactions, pages(46-51), 2007.
7. Abhishek Bansal, "Mobile E-Health for Developing Countries", in IEEE Transactions, pages(224-227), 2006.
8. G. Karjoth, N. Asokan, and C. Gülcü. "Protecting the computation results of freeroaming agents". In Proc. Second International Workshop on Mobile Agents (MA'98), K. Rothermel and F. Hohl, editors, LNCS 1477, pp.195 - 207, Springer-Verlag, 1998
9. B.S. Yee. "A sanctuary for mobile agents". Technical Report CS97-537, UC San Diego, Department of Computer Science and Engineering, April 1997.

Address reprints to:

*S. Venkatesan
Department of CSE,
Anna University
Chennai-600025, India*

E-mail: venkalt_s@yahoo.co.in