A security framework for virtual knowledge communities

Ogunleye Gabriel Opeyemi
Department of Mathematical Sciences (Computer Science Programme), Redeemer's University, Redemption Camp, Mowe, Ogun State, Nigeria

Adewale O. S.
Department of Computer Science, School of Science, Federal University of Technology, Akure, Nigeria

Ogunde A.O.
Department of Mathematical Sciences (Computer Science Programme), Redeemer's University, Redemption Camp, Mowe, Ogun State, Nigeria

Alese B.K.
Department of Computer Science, School of Science, Federal University of Technology, Akure, Nigeria

ABSTRACT: Virtual Knowledge Community (VKC) is presently the new area of research that is currently coming of age in the research community. VKC which is a virtual place where knowledge agents can meet, communicate and interact among themselves. In recent times, many research works have been done in the area of VKC but the security aspect of the system has not received any considerable attention in the research community. Therefore, this paper presents a framework to secure agents in VKC against any malicious attacks in an encrypted form of sharing knowledge. The proposed approach will go along way in addressing the security issues in VKC.
KEYWORDS: Knowledge Management; Mobile Agent; Virtual Knowledge Communities; Encryption; Decryption;

Introduction

A virtual community can be defined as a set of people sharing interests and making use of electronic forms of communication for exchanges. Virtual knowledge community is a virtual place where agents can meet, communicate and interact among themselves [PJ09]. Virtual knowledge communities are made up of community of communities, Agents and community. Securing knowledge management is an important issue, because an organization's knowledge can be easy to view, steal, manipulate and delete [MC04]. However, there is no consensus on how multi-agent systems can be used to deal with security considerations in KM. Traditionally, multi-agent systems are developed without security considerations in mind, by focusing on the coordination of agents which are typically assumed to be cooperative. We assume that it is feasible for agents to encrypt and decrypt knowledge with arbitrary keys during the sharing of knowledge in VKC. Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. A lot of research works had been done proposing different schemes and algorithms on knowledge sharing and management in virtual knowledge communities [BM02]. The researchers had not really considered the possibility of securing the knowledge among the communicating agents. Therefore this work will focus on sharing knowledge among the participating agents in an encrypted format. While the knowledge communities domain might seem exciting and promising, measures of trust and security must be applied to each agent to establish a secure connection for securing knowledge in such a distributed environment. Knowledge to encrypt and decrypt material efficiently with arbitrary keys, and that these keys are not readily discoverable by exhaustive search or crypt-analysis. We assume that an intruder can interpose a knowledge communities in all communication paths, and thus can alter or copy parts of knowledge, or emit false material. Securing communication in physically vulnerable networks depends upon encryption of materials passed between machines **[**RMS78]. Our proposed system should be regarded as examples that expose the security issues in knowledge sharing communities rather than as fully engineered solutions to the overall security problems of a particular application. The paper is organized as follows. In section 1, knowledge management, mobile agents, Virtual Knowledge communities, Cryptography are reviewed. Section 2 presents our proposed system based on encrypted form of securing and exchanging knowledge in VKCs and conclusion is drawn in section 3.

1. Review of Related Literature

1.1. Knowledge Management

Knowledge is now recognized as the driver of productivity and economic growth, leading to a new focus on the role of information, technology and learning in economic performance [OEC96]. KM (Knowledge Management) in its broadest sense is a conceptual framework that encompasses all activities and perspectives required to gain an overview of, deal with, and benefit from the corporation's knowledge assets and their conditions. It pinpoints and prioritizes those knowledge areas that require management attention. It identifies the salient alternatives and suggests methods for managing them, and conducts activities required to achieve desired results [Wii93]. The initiation and spread of the internet has taken the information age to a new level of complexity. The information society now has so much information at its disposal that it is more important than ever to find effective techniques for managing the optimal distribution of this information, such that individuals are not overwhelmed with meaningless data. The objectives of knowledge management are well known; to improve the reuse of the knowledge within the processes of a system, by reducing the distance between tasks and generalized knowledge bases, and increasing accessibility to resources. In recent years many organizations have adopted knowledge management techniques that focus on building large, expensive, centralized knowledge management systems based on the standardization of the syntactical and semantic representations of all of the knowledge in the organization.

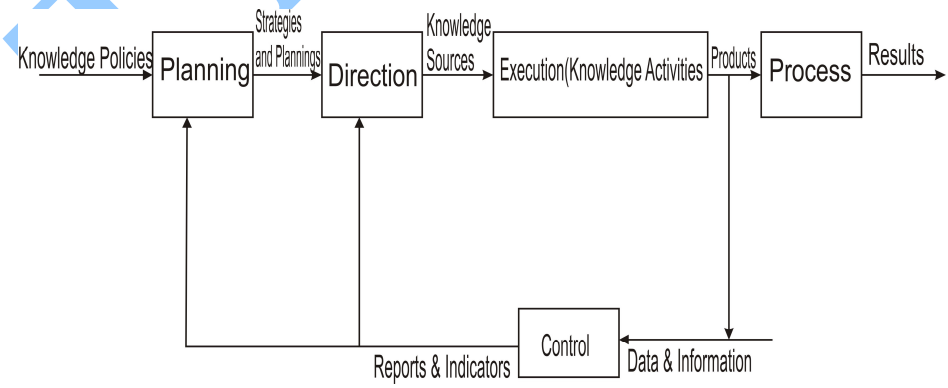

Figure 1: Knowledge management model

1.2. Mobile Agents

A mobile agent is a software program that can migrate or move from one host to another in a heterogeneous network [HC07]. They are called travelling agents, because these programs can shuttle their being, code and state among resources.

Mobile agents are network nomads that function as personal representative, working autonomously through networks. They are able to visit network nodes directly using available computing power and are not limited by platform. The technology has become another approach for the design and implementation of distributed systems to the traditional Client/Server architecture.

Mobile agents can travel from one system to another during their execution and communicate amongst one another, clone, merge and co-ordinate their computations. Mobile agents are autonomous agents in the sense that they control their relocation behavior in pursuit of the goals with which they are tasked [MHS00]. Possible applications of mobile agents include network management, information retrieval, distributed simulation, electronic commerce and mobile computing [ZZ00].

1.3. Virtual Knowledge Communities

Virtual communities are becoming increasingly popular, particularly on the Internet, as a means for like-minded individuals to meet other individuals they can learn to trust and to share and gain access quickly and efficiently to the information they are mostly interested in. The concept of a community of practice or a community of interest can be supported in a virtual community in order to bring the appropriate parties together and to share their knowledge [PJ09]. The advantage of this is that the members of a community centered on one specific topic or practice will only be presented with knowledge from domains they are, or at least are relatively likely to be, interested in. This knowledge needs not be something they have specifically asked/searched for.

Many virtual communities applications already exist on the Internet. Some are using agents in various forms as part of the back office system. [PJ09] proposed an approach that extends the abstraction of an agent, such that it acts within the system, searching for or delivering knowledge within

other agents and through communities. With such a model, agents can choose to join, leave, create and destroy a community, they can ask for information and send information to the community, and they can be member of several communities simultaneously. Virtual Knowledge Community (VKC) was called the virtual place where agents can meet, communicate and interact among themselves. Basically, a VKC is centered on a topic, corresponding to a domain of interest for which the interested agents have joined this community. This notion allows an increased availability of data and knowledge within the various communities.

A community consists of a domain of interest (a knowledge cluster), a leader (an agent), a policy and an unspecified number of member agents. Also [FER97] gives the following definition for a multi-agent system: "a system composed of a population of autonomous agents which cooperate with each other to reach common objectives, while simultaneously each agent pursues individual objectives." We can thus see a Multi-Agent System as a system in which autonomous agents can communicate, exchange their individual knowledge and cooperate in order to solve complex problems and to achieve collective or individual goals [HS99]. This is the natural and most general available model for an agent-based knowledge sharing system.

Hence, knowledge sharing is now a common practice on the internet today and if not properly secured especially when the agents and communities increased, agents will be pruned to attack in the process of sharing or exchanging resources.

1.4. Cryptographic mechanisms

Cryptography is used in security fields. The concept of using has a long history. One of the earliest cryptographic systems, Julius Caesar sent military messages to his generals [Par02]. The cryptography mechanisms are used to make secure communication among different parts. It has many concepts:

Encryption: This process converts a message from readable to be unreadable by using a key. The key is a numerical value used by the encryption process to change the information.

Decryption: This is opposite to the encryption process. It converts the encrypted message to its origin by using the same key or another key (depend on the mechanism). Algorithm: The well-defined set of roles that are used to encrypt and decrypt the message. It is represented in

mathematical function. In cryptography world, the message that needs to be secured is called plaintext. After the message is encrypted it is called cipher text. The cryptography mechanisms are used in wide areas of the data communication fields. The researcher continually improves the cryptography mechanisms to be more trustful and powerful. There are many cryptography mechanisms as follows:

A. Symmetric Encryption

Symmetric encryption is known as one of the cryptography mechanisms. It makes use of the same key for encrypting and decrypting. The key is named a secret key. All the users who exchange data and use this mechanism must be able to have this key protected. The algorithm that is used in this mechanism is called a Secret-Key Algorithm. The key is used to encrypt the message and the same key to decrypt the message. There are some well-known secret-key algorithms and key size such as:

- RC2 – 64 bits.
- DES – 64 bits.
- 3DES – 192 bits.
- AES - 256 bits.
- IDEA – 128 bits.
- CAST -128 bits (CAST256 uses 256 bits key)

Figure 2 shows the encryption and decryption processes:

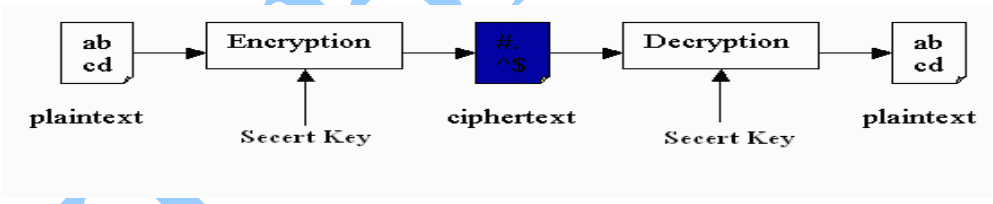

Figure 2: Symmetric Key Encryption

B. Hashing Algorithm

A hash function is mathematical function that is used to generate message-digest from a message [Par02]. It uses the original message as an input and the output is a message-digest. The message-digest is a unique for the message (fingerprint of the message). Also, this function is called one way hash function.

1.5. Secure-image mechanism

Secure-Image is a modern method to safe mobile agent against malicious hosts. The idea behind this technique is to use symmetric encryption and the hash function in the cryptography science. The approach prevents eavesdropping and alteration attacks. The major advantage of this method is to allow the mobile agent to continue its journey without problem incase these types of attacks occurred. SIM is made up of many entities and each one has a significant role.

The following sections describe the role of each one:

1.5.1. Security issues and threats

Security of mobile agent is very vital in any mobile agent based application. Besides security of agent platform is also crucial. In order to discuss the security aspects of a mobile agent system, the following security service should be considered: Confidentiality, Integrity, Authentication, Authorization and Non-Repudiation.

A. Confidentiality

Confidentiality guarantees that, data and code carried by an agent are not accessible by unauthorized parties (unauthorized agent or unauthorized agent server).

B. Integrity

Integrity assures that agent's code and baggage cannot be changed or modified.

C. Authentication

Authentication allows a mobile agent to verify its identity to an agent server as well as an agent server to a mobile agent. Without authenticity an attacker could masquerade an agent's identity and could gain access to resources and sensitive information.

D. Authorization

Authorization certifies that an agent can access the resource or information only when they are allowed to access.

1.5.2. Non-Repudiation

Non-repudiation assures that the agent-server or the mobile agent cannot repudiate the activities it has performed.

Threats in a Mobile Agent system are classified as [WT10]:

- *Threats from mobile agent to agent server*
- *Threats from agent server to mobile agent*
- *Threats from mobile agent to mobile agent*

F. Threats from Mobile Agent to Agent server

Possible threats from a mobile agent to an agent server can be enumerated as: illegal access to services and resources of agent server, steal or reveal of secret information from server, denial of service, damage of software and data, penetrate virus/worms and finally action repudiation.

G. Threats from Agent server to Mobile Agent

Similarly, is also likely for an agent to face some threats from an agent server and these can be listed as: illegal access to mobile agent's resources, steal code and valuable information carried by agent, reveal private or sensitive action performed by mobile agent, damage of code and baggage, execute agents code incorrectly, sending agent to unintended destination, cheat agent with false information and information or action repudiation.

H. Threats from Mobile Agent to Mobile Agent

Lastly an agent might face threats from another agent. These threats are stealing agent information, convey false information, render extra messages, accusing processor time, denial of service, information or action repudiation and unauthorized access.

1.6. Security of mobile agent in Ad hoc Network using Threshold Cryptography

[S+10] proposed a result for securing mobile agent in an ad hoc network. Threshold Cryptography was used in their model to provide a solution to the problem of central certificate authority (CA) and trusted third party in PKI, by distributing trust among several network nodes. Their framework went a long way to secure not only mobile agent, but also the agent server and the agent platform. It gave prime security services like confidentiality, integrity, authenticity. In relation to threshold cryptography, the value t was taking into consideration as a threshold value for the ad hoc network. Which means the system can tolerate up to t compromised servers. Here the point of trust is the consideration that - the compromised servers cannot generate correct private key of the Key Management Service and to sign certificate, because the compromised servers can generate maximum t partial signatures. Although is very possible only when the other servers in the network know about the compromise of those servers and then they will not co-operate those servers by providing their partial signatures.

1.7. Using Secure-Image Mechanism to Protect Mobile Agent against malicious Hosts

[Tar09] introduced a new mechanism called Secure-Image Mechanism. SIM aims to protect mobile agent against malicious hosts. They used cryptography mechanisms to achieve the tasks. The authors raised some salient point that the mechanism can prevent the eavesdropping and alteration attacks. It also assisted the mobile agents to continue their journey normally incase these attacks occurred.

1.8. Partial Result Authentication Codes (PRAC)

[Yee97] proposed an approach, Partial Result Authentication Codes (PRAC), which protects partial result with a Message Authentication Code (MAC) computed on partial results by using a secret key. The agent originator (owner) and mobile agent are given a secret key for each host to be visited. The current secret key used to encrypt the partial result is destroyed before the agent migrates to the next host. Destroying secret keys before agent migration ensures that the previous partial results are secure and intact. Since the agent originator maintains the secret keys, the partial results can be verified on the originator's home site.

PRACs also provide a reasonable protection to mobile agent systems by focusing primarily on integrity issues in the mobile agent system. PRACs have several positive aspects. First, PRACs improve the integrity of partial results, because the secret key(s) used to create PRACs are destroyed before an agent's migration. Second, unless secret keys are compromised, the agent originator can pinpoint which malicious host attempted an attack through comparing the PRAC generated by the malicious host to the PRAC generated by the correct secret key stored in the agent originator. The third advantage of the PRAC approach is that it guarantees forward integrity, which states that even though the current host is malicious, all the previous partial results are safe, because the secret key for each previous host is destroyed before an agent's migration. There are negative aspects to the PRAC approach also. First, it provides protection to partial results for mobile agents, but not to agent code and other aspects of the agent. Second, if the secret keys are compromised by malicious hosts, then those malicious hosts can read and modify any partial results. Third, although secret keys are destroyed before agent migration, it does not ensure that future results are secure, if a host is ever revisited by an agent.

1.9. Environmental Key Generation

The next approach, Environmental Key Generation proposed by Riordan and Schneier, generates the decryption key for an agent's encrypted code and data by searching through the execution environment [RS98]. The agent originator sends a cipher-text message (i.e., encrypted data and instructions) and a method for searching the environment for the data that is required to generate the decryption key. If the proper environmental data is found through the given data channel, then the key is generated to decrypt the encrypted mobile agent. Environmental key generation has many strengths over other approaches. First, environmental key generation improves the integrity and privacy for agent code and data, which are both encrypted by the agent. Second, the decryption key is kept secure. The programmer can choose any kind of data channel that best suits the application such as a file system, Internet newsgroup, or e-mail. Even though the attacker may know which data channel the agent is searching, he or she must know which data portion of the data channel is required for the key generation. The environmental key generation can protect the code and data from integrity and privacy attacks, but this approach also has weaknesses. First, the environmental key generation approach is vulnerable to group conspiracy attack. Second, data channel protection is another security issue. Third, although this approach can improve the integrity and the privacy for its code and data, it does not provide any protection for results. Fourth, once the code and data are decrypted, they can be attacked by a malicious host who can insert his or her own decrypting routine and data channel for new hosts.

2. Proposed Model/Architecture

Trust and security are the most important issues in the mobile agent system. Our new approach provides a mechanism for securing knowledge among the knowledge agents, based on the cryptography scheme. According to Threshold Cryptography, to sign a certificate there is a Master public/private key pair (Kpb / kpr) which is called the key pair of the Key Management Service. The master public key is known by all the knowledge agents in the communities and the master private key (kpr) is known by only the two participating knowledge sharing agents in real time in the communities.

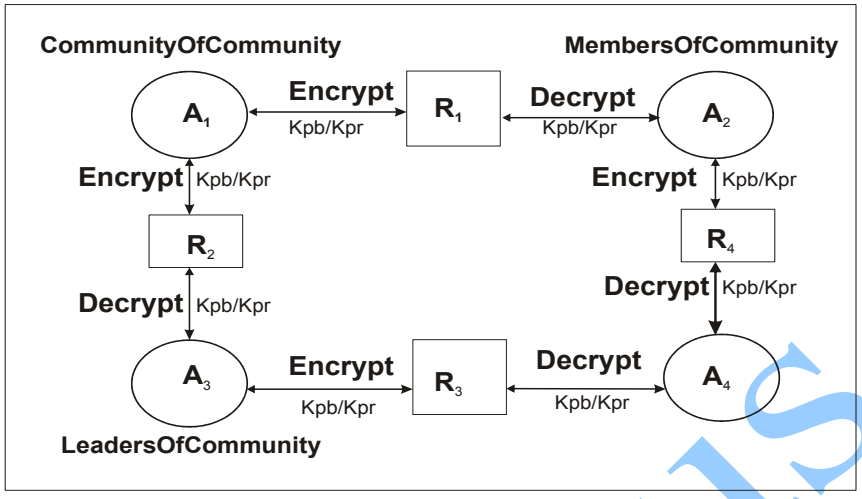

Figure 4: Security framework for Virtual Knowledge Communities

In the above model, we have different community of interests in the VKC. They are CommunityOf Community, MembersOfCommunity, LeadersCommunities. Thus, agents exist in each of the communities which are agent A_1 in the CommunityOfCommunity, agent A_2 in MembersOfCommunity and agent A_3 in LeadersOfCommunity. The resource R depicts the knowledge that is being shared among the agents. Suppose agent A_1 wants to send knowledge (R_1) to agent A_2. A_1 has to encrypt R_1 using the key Kpb/kpr and then send it to A_2. When A_2 receives the resource from A_1, it has to decrypt R_1 using an arbitrary numbers to generate the private key which is only known by A_1 and A_2(kpr). After then, it then verifies the signature of agent A_1. It should be established that the key kpb is a public key and is known by all the agents in the communities. The private key (kpr) is only known by the two agents that are currently sharing knowledge. The first goal of our approach is to enhance the privacy so that malicious agents are not able to read the contents of important knowledge. Also to check the case of eavesdropping: threat that involves the monitoring and interception of the secret information which is being communicated between authenticated agents. The last goal is that no one except the knowledge receiver must be able to decrypt the knowledge and result. The algorithm to represent our proposed work is shown in figure 5:

If knowledge (R) is not encrypted
Then declare R as unsafe
Else
For all agents (in parallel) such as A_i which has registered with Community (C) (internally or externally) and has its R encrypted
Then declare R as safe
End for
End if
On detecting that R has been altered by intruder
If agent A on noticing that R has been altered by intruder
Then Inform the sender of R to re-send R again in an agreed encrypt format
Else
Knowledge sharing continues
End if

Figure 5: A security algorithm for virtual knowledge communities

Conclusion

This paper has provided a solution for securing knowledge using cryptography scheme in VKC. However, it is difficult to provide 100% protection for securing knowledge especially in a multi- agent's environment. As the contribution of this research, the agents would be able to share encrypted knowledge without any fear of interfering by intruder. Full implementation of our proposed system is still underway. As the network is increasing, future work will center on developing a very powerful algorithms and models that are scalable enough to give a complete protection to the knowledge.

References

[BM02] **M. Bonifacio, P. Maret** – *Knowledge Nodes: the Building Blocks of a Distributed Approach to Knowledge Management,* Journal of Universal Computer Science, Vol. 8 No. 6, pp. 652–661, 2002.

[Fer97] **J. Ferber** - *Les systems multi-agents: un aperu general,* Technique et Science Informatiques, Vol. 16, No. 8, pp. 979-1012, 1997.

[HC07] **K. Huang, Y. Fang Chung -** *Efficient migration for mobile computing in distributed networks.* Elsevier, February 2007.

[HS99] **M. Huhn, L. Stephens** – *Multi-agent systems and societies of agents*, in Multi-agent Systems, A Modern Introduction to Distributed Artificial Intelligence, MIT Press, Cambridge, USA, pp. 79-120,1999.

[MC04] **D. Mundy, D. Chadwick** – *Secure knowledge management*, in Creating Knowledge Based Health Care Organizations, Idea Publishing Group. pp. 321-337. 2004.

[MHS00] **J. Meng, S. Helal, S. Su** – *An Ad-Hoc Workflow System Architecture Based on mobile agents and Rule-Based Processing*, The special session on Software Agent-Oriented Workflows, Proceedings of the International Conference on Parallel and Distributed Computing Techniques and Applications, Las Vegas, Nevada, pp. 245-251, 2000, http://www.harris.cise.ufl.edu/projects/publications/adhocWF.pdf

[OEC96] **OECD** – *The Knowledge Based Economy*, Paris, STI, pp. 57, 1996.

[Par02] **G. Paramasivam -** *Cryptography in Microsoft.NET Part II: Digital Envelop and Digital Signatures*, technical paper, http://www.csharpcorner.com/Code/2002/Dec/DigitalEnvelop.asp, 2002.

[PJ09] **M. Pierre, C. Jacques** – *Agent-Based Knowledge Communities,* International Journal of Computer Science and Applications Technomathematics Research Foundation Vol. 6, No. 2, pp. 1-18, 2009.

[RS98] **J. Riordan, B. Schneier** – *Environmental key generation towards clueless agents,* in LNCS, Springer, pp. 15–24, 1998.

[RMS78] **M. Roger, D. Michael, X. P. Schroeder** – *Using Encryption for Authentication in Large Networks of Computers*,

Communications of ACM, Vol. 21, No.12, pp. 993-999, December 1978.

[S+10] **S. Sarwarul, S. Zinat, S. Bo, W. Md** – *Security of Mobile Agent in Ad hoc Network using Threshold Cryptography*, World Academy of Science, Engineering and Technology 70, pp. 424-427, 2010.

[Tar09] **M. Tarig** – *Using Secure-Image Mechanism to Protect Mobile Agent against malicious Hosts,* World Academy of Science, Engineering and Technology 59, pp. 439-444, 2009.

[Wii93] **K. M. Wiig** – *Knowledge Management Foundations*, Schema Press, Arlington (Texas), 474 p, 1993.

[WT10] **J. Wayne, K. Tom** – *NIST Special Publication 800-19 – Mobile Agent Security*, [Online] National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/nistpubs/800-19/sp800-19.pdf [Accessed 1 March 2010].

[Yee97] **B. Yee** – *A sanctuary for mobile agents*, DARPA Workshop on Foundations for Secure Mobile Code Workshop, March 1997.

[ZZ00] **P. Zoran, B. Zoran** – *Mobile agents-a new and advanced concepts*, Proceedings of the TARA 2000 Conference Novi Sad, Yugoslavia, September 6-7, 2000, vol. 30, no. 2, 113-123, 2000.