ALMAS : A FRAMEWORK FOR AGENT BASED LEGAL MONITORING AUTOMATED SYSTEM FOR THE TRUSTED E-BUSINESS TRANSACTIONS

Mohammed Saleem A.S.Praveen A.Lakshmi Priya P.Haritha & J.Sheik Mohamed
Sreenivasa Institute of Technology and Management Studies,
Chittoor, Andhra Pradesh, INDIA.
sony24.jahan@gmail.com praveen.soundar@gmail.com a.l.priyaa@gmail.com, haritha.pr@gmail.com
sheik_50@yahoo.co.in

Abstract

In this paper we are proposing a model where we can establish a perfect and effective SCM with which an E-Business in E-Commerce becomes effective. In this model, we are mainly concentrating on the integrity along with security, confidentiality and atomicity of SCM. The centre of attraction of our model is Legal Monitoring Automated System (LMAS) along with the embedded Agent. The functionality of LMAS is to monitor the frauds, which occur during the different transactional flows. The key role in LMAS is with the secret Agent which is built on the concept of artificial intelligence. The Agent aets intelligently as a response to the LMAS whenever it detects fraud. We took care to the maximum extent with which there won't be any chance of occurring, fraud. We termed LMAS with its Agent as E-Commerce robot which acts autonomously without any ones assistance. According to us, the model proposed will give an optimal solution in the area of SCM integrity along with confidentiality, security and atomicity of the flows in SCM.

Key Words

E-commerce, E-Business, E- procurement, Third-Party(TP), Legal Monitoring Automated System(LMAS), Agent, Buyer, Supplier, Kerberos Server, IRS Server.

Supply Chain Management (SCM)

Supply Chain Management (SCM) is the set of processes that cover transforming and moving products and information from your Suppliers' Suppliers through your business to your customers' customers and back, when required. Many now look at Supply Chain Management from a view of managing Demand, Supply and Product [9].

1. INTRODUCTION

The total description of this paper circulates over the atomicity, confidentiality, integrity and security of the SCM by applying various techniques to promote that in a sensible manner. The SCM is the core for every B2B, B2C etc transactions without which the E-Commerce is meaningless. But the problem in E-Commerce is with the key factor i.e. with the SCM, because it looses its tendency and prominence as the business varies in terms of its functionality [1][2][3][4][5][6][7][8]. Many now look at SCM from a view of managing demand, supply and product though it is lacking its tendency towards the promotion of integrity, security, confidentiality and atomicity.

To understand this, let us have a brief account on the functionality of the SCM and its features. As a brief description on SCM, let us start with the types of flows in SCM. The flows are as follows: (1) Information Flow (2) Product Flow and (3) Cash Flow. Some SCM applications are based on open data models that support the sharing of data both inside and outside the enterprise (this is called the extended enterprise, and includes key Suppliers, Suppliers, and end customers of a specific company). Increasing numbers of companies are turning to Web sites and Web-based applications as

part of the SCM solution. A number of major Web sites offer **E-procurement** marketplaces (E-procurement is the business-to-business purchase and sale of supplies and services over the Internet) where Suppliers can trade and even make auction bids with Suppliers. An important part of many B2B sites, E-procurement is also sometimes referred to by other terms, such as **Supplier exchange**. Typically, e-procurement Web sites allow qualified and registered users to look for Buyers or sellers of goods and services. Depending on the approach, Buyers or sellers may specify prices or invite bids. Transactions can be initiated and completed. Ongoing purchases may qualify customers for volume discounts or special offers.

The application what we framed is totally dependent on the E-procurement with respect to SCM. The entire E-commerce is dependent on the loyal E-procurement (i.e.) nothing but the correct transactions, which finally maintains perfect SCM. In our application we are applying E-procurement criteria in between the Buyer, the Third-Party, and the Supplier.

In the application the key role player is the Legal Monitoring Automated System (LMAS) which controls and mitigates all the discrepancies which arise out during the E-procurement. And the interesting feature of the application is the Agent, which is the hidden one in LMAS, though it is the hidden one, it functionates in such a way that it alerts and warns the entities depending on its attitude during the transactions.

2. RELATED WORK

Related work deals with the functionality of SCM in Traditional Approach as well as with the Modern Approach. In the traditional approach, the SCM functionates in between the Buyer and the Supplier, when we talk about the modern approach the SCM functionates in between the Buyer, Third-Party and the Supplier. Though there is a functioning of SCM, all the approaches till now are lacking integrity, security, atomicity and confidentiality, we can't expect all these possible events to occur in the SCM. In order to achieve this, there has evolved many approaches where SCM failed to have an effective integrity, security, atomicity and confidentiality. Even in the modern approach there has been a use of NetBill server[11], which maintains the accounts of the Buyer and the Supplier, but still there is lack in the integrity and security of SCM.

3. BACKGROUND ANALYSIS

3.1 Traditional Approach

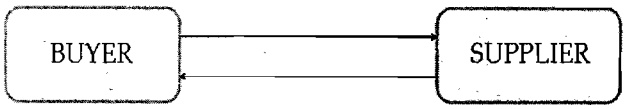

Fig1: SCM between Buyer and Supplier

In the Traditional Approach, the SCM prevails around the Buyer and the Supplier. Suppose, the Buyer wants any product from the Supplier, he/ she should browse the Supplier's website for the product details. After the ordering of the product, the Buyer receives a "token number" of the concerned product with which he can further contact (or) to validate the product.

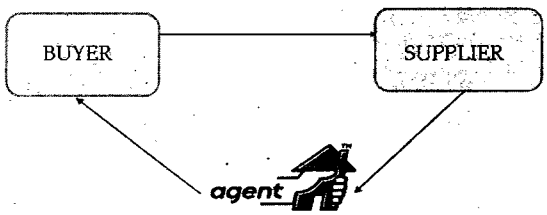

Fig2: SCM between Buyer and Supplier including Agent.

Suppose, if the Supplier has any query with the product Buyer, it should communicate but the communication via E-mail makes the Buyer to respond lately because he wont be in online regularly, this makes the Supplier lacking in instant communication. In order to have an instant communication with the Buyer, Agent is the appropriate one to communicate; it sends a message to the Buyer. Agent is the intermediary one which is independent of the entities.

3.2 Modern Approach

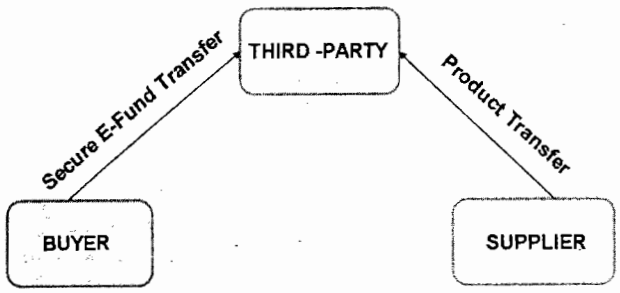

Fig3: SCM between Buyer and Supplier in association with the Third-party.

The third-party receives items from both entities, checks them and forwards them to the respective **entities**. The third-party arises only when the distrust arises between the two entities. The third-party should be in the mode of online all the time.

The third-party is the Kerberos server which ensures the financial atomicity and product atomicity by providing an encrypted individual token number to each other. This is the token number with which the frauds can be maintained to more extent.

Suppose, if the Supplier is delivering a product to the Buyer, prior to that Supplier should escrow (or) provide the token number in the encrypted format to the third-party (TP). The token number is for the purpose when the Supplier betrays the Buyer after receiving the payment; here the token number is with the TP. So, with that token number the Buyer can receive the product.

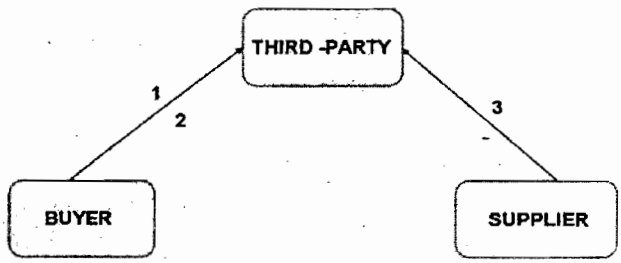

Fig 4: Transactions between Buyer, Third-party and Supplier

1 → Product request

2 → E-Fund transfer in the form of token number

3 → Product delivery with the token number to the third-party

Note: The Buyer should give his credit / debit card number to the TP in the form of a token number which is in the encrypted format which consists of a actual amount of the product including the tariff charges. The same is with the Supplier who gives the product token number which is in encrypted format to the TP.

3. PROPOSED MODEL

The model proposed here is for the purpose of secure and integrated SCM. In this model, the SCM proved a positive result to the maximum extent. Before going to discuss SCM in detail let us have a brief description about the model. The model comprises of three entities, LMAS and Agent in which is under hidden state. The role of LMAS and the Agent is the centre of attraction in maintaining a SCM. We proposed this model as betterment to the modern approach.

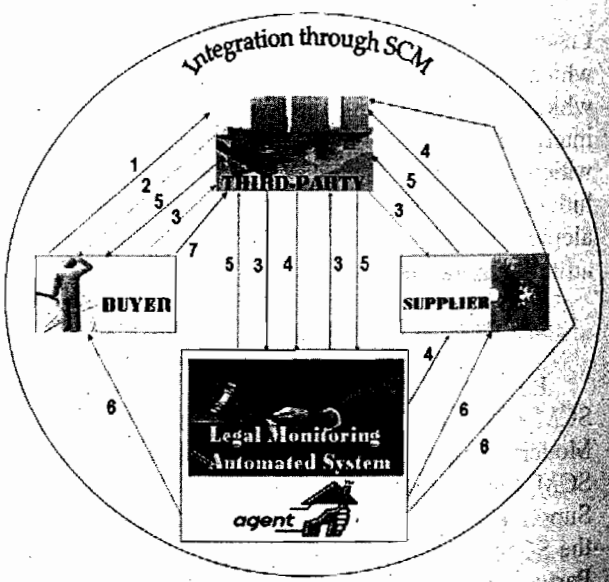

Fig 5: Model for effective Integration of SCM

The numberings in the figure denotes the functionality of the entity with respect to their transactions. It is as follows.

1. Buyer → Third-party :Product Request.
2. Third-party → Buyer :Displays Product details.
3. Buyer→ Third-party→ LMAS→ Third-party→ Supplier: Electronic Payment Token with a key.
4. Supplier→ Third-party→ LMAS→ Supplier: Electronic Payment Token validation.
5. Supplier→ Third-party→ LMAS→ Third-party→ Buyer: Product Encryption key to the Buyer while receiving the product.
6. Alerts / warns the entities depending on their behavior at that instant through messages by the secret Agent.
7. Buyer → Third-party: Acknowledgement of the product receiving.

4.1 Assumptions

1. The Buyer approaches the third-party for the product details.
2. The third-party displays the product details as expected by the Buyer and there by the Buyer chooses the product suitable to his idea.
3. The Supplier provides a token number for the product ordered by the third-party on behalf of the Buyer.
4. Before any transaction (or) report generation by the third-party it should send the information for validation, to the LMAS.
5. Though the care taker of the Buyer and the Supplier is the third-party, implicitly the care taker is LMAS in association with an Agent.
6. The LMAS checks for validation and there by it returns to the third-party for further proceeding. It is the case when the validation is optimal, suppose if the validation is not optimal one, then the secret Agent alerts the third-party by sending a warning message and an alert message regarding the party who is going to affect.
7. The secret Agent acts as a mobile Agent because it can host anywhere in the manual autonomously to provide atomicity to the entities perfectly.

Let us have a detail description of the model in detail including the functionalities of the entities present in the model.

4.2 Functionalities of Third-party

The third-party is the protocol which acts as a intermediary between the two basic entities i.e. Buyer and Supplier.

The main functionalities of the third-party is as follows:

The Third-party consists of

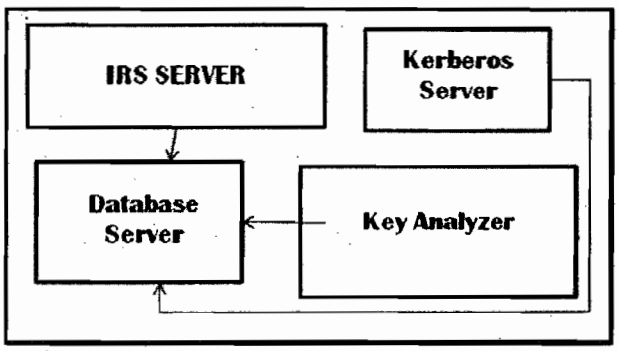

Fig 6: Block Diagram of the Third Party

- Kerberos Server → used for authentication purpose both for the money and product atomicity and transfer atomicity [10].
- IRS Server → used for information retrieval of the product as requested by the user.
- Database Server → which stores the entire transaction details of both the Buyer and the Supplier.
- Key Detecting Server (or) Key Detector → which scrutinizes the keys as sent by the respective entities.

- The third-party should functionate in such a way that it posses the capability of self decision-making. Here the self decision-making is needed compulsorily for the purpose of validation check. It should be in such a position that after scrutinization of the information or message it should send that information or message to the Legal Monitoring Automated System (LMAS) for the information or message validation.
- The third-party should loyally send the information or message to the LMAS of the respective entities.
- Actually, the third-party is the key entity which posses a powerful authentication / authorization for the different transactions to perform.
- The third-party is the care taker of the Buyer and the Supplier; it should bare all the complexities which may arise with the Buyer and the Supplier.
- The third-party acts as the protocol for the promotion of security in the E-Fund transfer, information transfer and the product transfer respectively.
- The third-party is the active protocol which is in online all the time.
- It gives an assurance to the respective **entities** which will approach its corridor. It takes the responsibility if there is anything unwanted occurs.

4.3 Functionalities of LMAS

LMAS denotes Legal Monitoring Automated System which plays a vital role in this application based on SCM.

The main features of LMAS are follows:

- ✓ LMAS is an automated system which consists of many types of servers, which maintains the policies, issues, pros and cons of the respective entities.
- ✓ Every transaction except the PR from the Buyer – Supplier transaction, should approach the LMAS via third-party. Any information or message which comes from the third-party is put under validation defaultly with respective to the policies related to the entity at that instant, it is done automatically without any manpower, since it is the automated one.
- ✓ As a contrast to the above statement, if under validation any problem exist i.e. respective entity violating the policies and issues then there is a need of an Agent which alerts the affected entity and warns the affecting entity.

4.4 Functionalities of Agent

- ✓ Agent is the hidden part in the LMAS which functionates effectively and intelligently by remaining implicitly in the LMAS.
- ✓ It is the software which is built using the concept of Artificial Intelligence which functionates cleverly depending on the situation may arise.
- ✓ Agent is the core of LMAS.
- ✓ The Agent responds to the LMAS and performs a scrutinization technique with which it evaluates the policies and issues of the affected entity and the entity which is affecting the entity and sends messages of alert and warning to the respective entities depends on its behavior at that instant.

The main notion of the Agent is to alert the affected party with its security alerts.

4.5 Analysis of the Model

The contribution of the secret Agent to the LMAS makes a powerful approach to adopt in the modern era. Since both LMAS and Agent are the automated ones, it provides security, integrity, atomicity and confidentiality to maximum extent to the user. Though the major part of the functionality is with LMAS, the Agent priority is more because it performs intelligent functions such as sending the alert message and warning message by deciding autonomously. It is to be noted that as soon as the LMAS detects the fraud from any of the entity, the Agent responds and sends the message to the entities depending on its behavior at that instant, with which the security of the transaction can be expected. Hence this contribution made us to react optimally in the security, integrity, atomicity and confidentiality of the SCM.

Let us discuss this model in UML approach (i. e) with the Sequence Diagram which covers the entire functionalities of the model.

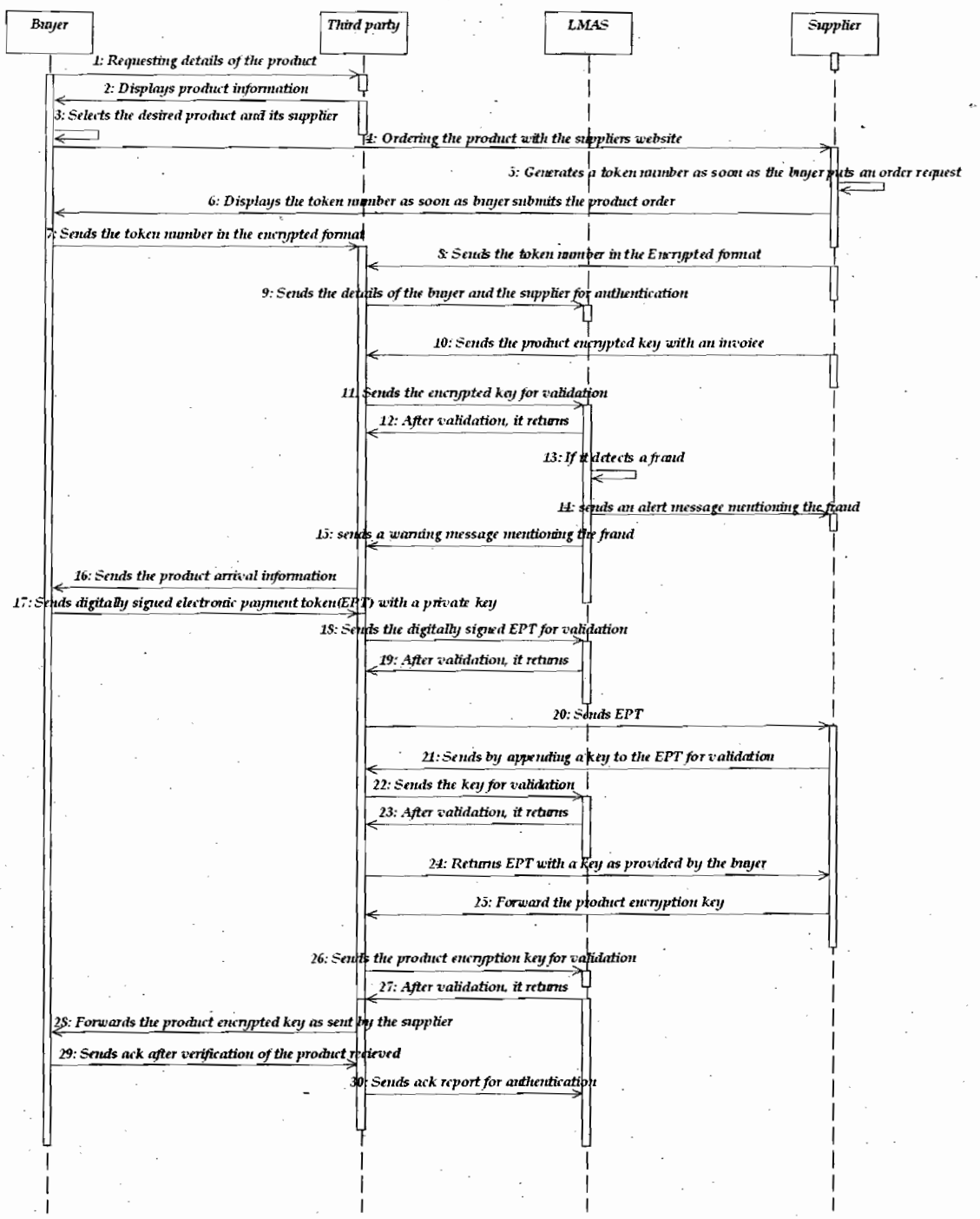

Fig 7: Sequence Diagram representing the entire functionality of the Proposed Model

CONCLUSION:

In order to have a secured E-Business transaction between the buyer and the supplier, the Third party came into existence in the modern approach to reduce the traffic in E-Business. Even with the existence of Third party, the problem of security and integrity is not yet solved up to the mark. In that situation, the model proposed by us mitigates the problem to the maximum extent. The main area in our model is the Legal Monitoring Automated System (LMAS) which controls transactions of all the entities in an optimal manner. The interesting area in our model is the Agent, which is present in LMAS internally to send the alert and warning messages. By combining these two systems in our model, we can expect a full-fledged authentication with respect to integrity, security, atomicity and confidentiality of the SCM in the E-Business. The model proposed by us is just a frame work, we can expect the attainment of integrity and security of the SCM in the E-Business transactions in future, if it is implemented.

REFERENCES

[1] Cox B, Tygar J. D, and Sirbu M, "NetBill Security and Transaction Protocol", *Proceedings of the First Usenix Workshop on Electronic Commerce,* 1995, pp 77-88.

[2] Zhou J, and Gollmann, "A Fair Non-repudiation Protocol", *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pp 55-61.

[3] Ray Indrajit, Ray Indrakshi, and Natarajan Narasimhamurthy, "A Fair-exchange E-commerce Protocol with Automated Dispute Resolution", *DBSec 2000*, pp 27-38.

[4] Vogt Holger, Pagnia Henning and Gärtner Felix C, "Modular fair exchange protocols for electronic commerce", *Proc. of the 15th Annual Computer Security Applications Conference*, 1999, pp 3-11.

[5] Vogt Holger, Pagnia Henning and Gärtner Felix.C, "Using smart cards for fair exchange", *Electronic Commerce–WELCOM 2001*, Lecture Notes in Computer Science, Vol. 2232, 2001, pp. 101-113.

[6] Vogt Holger, Pagia Henning, and Gartner Felix C, "Supporting Fair Exchange in Mobile Environments", *Mobile Networks and Applications*, 2003, pp 127-136.

[7] Ray Indrakshi and Ray Indrajit, "An Optimistic "Fair Exchange E-commerce Protocol with Automated Dispute Resolution", *EC-Web 2003*, pp 84-93.

[8] Zhou J, and Gollmann D, "An efficient non-repudiation protocol", *Proceedings of the 10th IEEE ComputerSecurity Foundations Workshop,* 1997, pp. 126-132.

[9] (NYSE: HIT) Introduction: "*Supply Chain Technology Adoption*", A Knowledge-Driven Consulting® White Paper © 2006 Hitachi Consulting Corporation

[10] William Stallings," Cryptography and Network Security" *Principles and Practices, PrinticeHall, New Jersey 2000, pp:* 401.

[11] IEEE Paper "*Secure E-Commerce Protocol for Purchase of e-Goods - Using Smart Card*" pp:9