International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 10, December- 2012

Secure Decision Making Algorithm In B2B Scenario

C. Phani Ramesh[1], Prof. M. Padmavathamma[2]
(Department of Computer Science, Sri Venkateswara University, Tirupati, A.P., India.)

Abstract

The fast improvement of information technologies and widespread diffusion of communication networks through the Internet have being changed our daily lives in a drastic and electronic way. E-commerce is the business process of selling and buying the products, goods and services by on-line communications. It can be highly beneficial in reducing business costs and in creating opportunities for new or improved Distributor services. It is widely recognized that Security will plays a crucial role in modern times for business purposes and it will be transacted over the Internet through E-Commerce. In this paper, we propose Secure Decision making Algorithm for selecting the best Distributors among the existing Distributors in B2B Scenario.

Keywords: E-Commerce, Cryptosystem, M-Prime RSA, Key Generation, Data Mining.

1. Introduction.

The Rapid expansion of the Global Market, the explosive growth of information and Communication Technologies, aggressive competition and the changing Economic and social conditions have triggered tremendous opportunity to conduct Business in a collaborative way [1]. The business processes of different organizations need to be integrated to adapt the dynamic conditions and to remain competitive in the global Market. But, in a loosely coupled collaborative environment, several crucial aspects such as privacy and security do not get sufficient support.

In the emerging Global Economy, E-commerce and E-business have increasingly become a necessary component of business strategy and a strong catalyst for economic development. The security of Internet electronic transactions is one of the key factors needed for further E-business development. Online Commerce processes demonstrate particularly to security problems.

Development of Internet local networks have brought about an increase in security risks that may jeopardize supply and demand, especially in electronic transactions. Hence, Manufacturers and Distributors are often preoccupied with the problem of electronic transactions in exchange of information. To overcome these issues, Cryptographic techniques have to be adopted, in addition to physical, technical and organizational protection measures. By skillfully combining available cryptographic systems and mechanisms it is possible to build an adequate cryptographic architecture and offer several basic security services: Confidentiality (Privacy), Authentication, check on the integrity and non-repudiation of the Electronic Transactions.

In this paper, the proposed research focuses on the development of new Algorithm for secure classification, verification and development of decision tree to the Manufacturer for selecting the Best Distributor among the available Distributors by using M-prime RSA Cryptosystem in B2B Scenario.

2. Related Work.

E-commerce is transforming the global marketplace and its impact being felt across the full range of business and government. E-commerce requires an open, predictable and transparent trading environment, which operates across territorial borders and jurisdictions. To foster such an environment and to realize its full economic potential necessitates international co-operation, which will be instrumental in developing the enabling conditions for its growth. As online E-commerce continues to grow in all areas, customer expectations particularly in B2B e-commerce are changing rapidly. Companies serving business to the buyers are realizing that the conventional ways of doing the business are no longer sufficient. B2B companies are wishing to grow and become more profitable to adopt e-commerce. [2]

2.1 Business-to-Business (B2B)

B2B consists of largest form of Ecommerce. This model defines that Buyer and seller are two different entities. It is similar to manufacturer issuing goods to the retailer or wholesaler. The development and usage of B2B e-Commerce enabling technology has caused profound changes in the e-Business environment. The B2B e-Marketplace can significantly improve the way companies deal with their customers and suppliers. Furthermore, the initial proliferation of B2B e-Marketplaces that proved to be sustainable for buyers/sellers and play an important role in B2B e-Commerce [3].

B2B e-commerce makes it easier for companies to implement streamlined purchasing, payment, and inventory processes while providing unique product assortment, pricing, and business flows. A B2B e-commerce platform can also dramatically improve and the user experience by allowing vendors to provide rich pages, targeted dynamic content and sophisticated search capabilities.

2.2 Cryptosystems

Privacy is becoming an important issue in many data mining applications. This has led to the development of privacy preserving data mining. Cryptosystems is one of the technique emerged for privacy preserving Data Mining.

There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption.) [4]

2.2.1. Symmetric Encryption. Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, and that, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all the messages.

2.2.2. Asymmetric Encryption. The problem with secret keys is, to exchange the secret key over the Internet or a large network. Anyone who knows the secret key can decrypt the message. In Asymmetric Encryption, there are two related keys-- a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret**.**

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key, any message that is encrypted by using the private key can only be decrypted by using the matching public key.

3. Decision trees.

A decision tree is a tree in which each branch node represents a choice between a number of alternatives, and each leaf node represents a decision.

Decision tree is commonly used for gaining information for the purpose of decision -making. Decision tree starts with a root node on which it is for users to take actions. From this node, users split each node recursively according to decision tree learning algorithm. The final result is a decision tree in which each branch represents a possible scenario of decision and its outcome. [5]

ID3 is a decision tree induction algorithm that uses information gaining as the quality function for choosing attributes.[6] Information gain is defined as the difference of entropy of data set T before and after it is spitted with attributed A.

Information Gain (A) E(T) – E(T/A)

If there are categories Ci….C_l

TC is the set of records where class = ci,

and (T) is cardinality of the set, then there entropy E(T) is defined as

$$E(T) = \sum_{i=1}^{l} \left(-\frac{|T_{Ci}|}{|T|} . \log \frac{|T_{ci}|}{|T|} \right)$$

To make classification mark the leaf node with the class that has the highest number of instances. This method of inducing decision tree can be easily extended to distributed data mining process

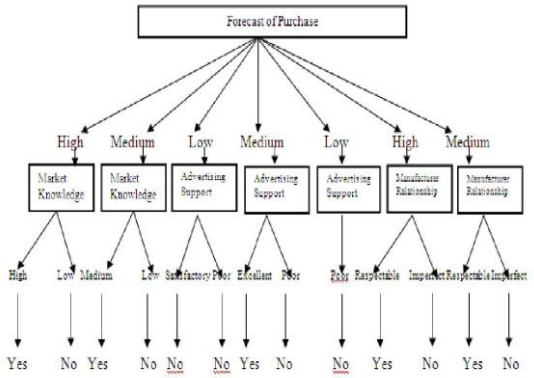
The Symbolic Attribute Description.

Attributes	Possible Values
Forecast of Purchase (Fp)	High, Low, Medium
Marketing Knowledge (Mk)	Good, Minimal, Low
Manufacturer Relationship (Mr)	Respectable, Imperfect
Advertising support(As)	Excellent, Satisfactory, poor
Decision	Yes, No

The Learning set to select the Best Distributor example.

Distributors	Marketing Knowledge (Mk)	Manufacturer Relationships (MR)	Advertising support(As)	Forecast of Purchases (FP)	Decision
1	Good	Respectable	Excellent	High	Yes
2	Good	Respectable	Satisfactory	Medium	Yes
3	Good	Imperfect	Poor	Low	No
4	Medium	Imperfect	Satisfactory	Medium	No
5	Medium	Respectable	Excellent	High	No
6	Medium	Respectable	Excellent	High	Yes
7	Low	Respectable	Satisfactory	High	Yes
8	Low	Respectable	Poor	Low	No
9	Low	Imperfect	Satisfactory	Low	No

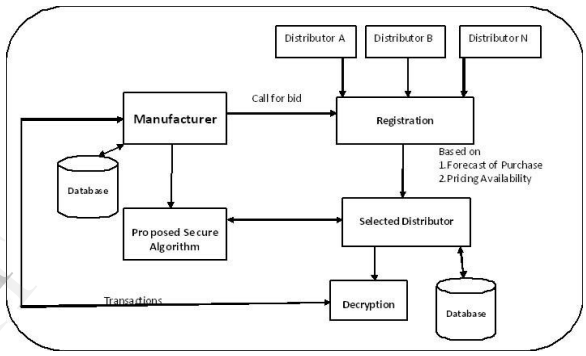
3.1 Distributor Decision Tree



Distributors

- Forecast of purchase: High
  - Market knowledge: High
    - Decision: Yes
  - Market knowledge: Low
    - Decision: No
- Forecast of purchase: Medium
  - Market knowledge: Medium
    - Decision: Yes
  - Market knowledge: Low
    - Decision: No
- Forecast of purchase: Low
  - Advertising support: Satisfactory
    - Decision: No
  - Advertising support: Poor
    - Decision: No
- Forecast of purchase: Medium
  - Adverting Support: Excellent
    - Decision: Yes
  - Adverting Support: Poor
    - Decision: No
- Forecast of purchase: Low
  - Adverting Support: Poor
    - Decision: No
- Forecast of purchase: High
  - Manufacturer Relation: Respectable
    - Decision: Yes
  - Manufacturer Relation: Imperfect
    - Decision: No
- Forecast of purchase: Medium
    - Manufacturer Relation: Respectable
    - Decision: Yes
  - Manufacturer Relation: Imperfect
    - Decision: No

4. System Model.



5. Methodology.

From the above System Model, the Manufacturer is responsible for the effective promotion of Business Products. This requires a thorough knowledge of the products being promoted, as well as the ability to solicit orders from outside Distributors, the manufacturer calls for bid from the Distributors. The Distributors will make registrations here. There are n distributors (=d1,d2,d3,…..dn) and Manufacturer (M_B).The role of Manufacturer is to organize each auction, run and announces the bid result based on the attributes Forecast of Purchase (FP), Marketing Knowledge (Mk), Manufacturer Relationships (MR) and Advertising Support (As) and announces the selected distributor among the registered distributors using decision trees [7]. The channels between Manufacturer and Distributor are to secure and reliable. For selecting the best distributors, we proposed a secure decision making algorithm to select efficient distributor.

5.1 M – Prime RSA Cryptosystem.

Multi prime RSA Cryptosystem was introduced by Collins who modified. The RSA modulus so that it consists of r primes p_1, p_2 .....p_r instead of traditional prime's p and q. [8]

5.2 Key Generation.

The key generation algorithm services as parameter the integer r, indicates the number of primes to be used. [9] The key prime is generated as follows:

1. Choose r primes $p_1, p_2.....$

$$n = \sum_{i=1}^{r} p_i = p_1.p_2.....p_r$$

2. Compute E and D such that d = e^{-1}

$(\mathrm{mod}\,\phi(n))$ Where gCd $(p, \phi(n)) = 1$

Where $\phi(n) = \sum_{i=1}^{r}(p_i - 1)$

$= (p_1 - 1)(p_2 - 1).....(p_r - 1)$

3. For $i \le i \le r$ compute $d_i = d \pmod{p_1 - 1}$

public key = (n, e)
Public key = (n, e)
Private key = (n, d1, d2……d_r)
Encryption: Given a public key (n, e)

$M \in Z_n$

Encrypt M exactly as in the original RSA, then

$C \equiv M^e (\mathrm{mod}\, n)$

Decryption: The decryption in an extension of quisquarter couvreur method. To decrypt a ciphertext C,

Calculate $M_i \equiv c^d (\mathrm{mod}\ p_i)$ for each i= 1,2……r

Apply the Chinese remainder theorem to the M is to get

$M \equiv C^d (\mathrm{mod}\, n)$

M – prime $J_2 - RSA$ cryptosystem with one public key and two private keys

By replacing $\phi(n)$ *by* $J_2(n)$ with the we can generate new variant cryptosystem.

Threshold key generation encryption and decryption are given below.

Key generation: 1. Choose r distinct primes

$p_1, p_2.....p_r$

$$n = \sum_{i=1}^{r} p_i = p_1, p_2.....p_r$$

2. Compute E and D such that D

$E^{-1} (\mathrm{mod}\ J_2(n))$ *i.e.*, $ED \equiv 1 (\mathrm{mod}\ J_2(n))$

Where $\gcd(E_2 J_2(n)) = 1$ *and*

$J_2(n) = n^k \prod_{p/k} (1 - p^{-k})$

$= (p_1^k - 1)(p_2^k - 1).....(p_r^k - 1)$

$= \pi_{i=1}(p_i^k - 1)$

3. for $1 \le i \le r$ compute

$d_i \equiv d \bmod (p_i^k - 1)$

Public key = (2, E, n)
Private key = (2, D,n)
Encryption: Given a public key (2, E., n) and a message $M \in Z_n$, encrypt M.
M exactly as in the original RSA.

$C \equiv M^E \pmod{n}$

Decryption: The decryption is an extension of the quisquater courier method. To decrypt a cipher text C, calculate $M_1 \equiv c^d (\mathrm{mod}\ p_i)$ for each apply choose remainder theorem Mi's to get $M \equiv C^D (\mathrm{mod}\, n)$.

6. Proposed Secure Decision making Algorithm to Select Efficient Distributor.

1. Set of Distributors d=(d1,d2,d3,…….dr}
2. Generate the attributes respective to the Distributors

$N = \{n_1, n_2.....n_r\}$

Where n1= Marketing Knowledge (Mk)
n2= Forecast of Purchases (FP)
n3=Manufacturer Relationships (MR)
n4= Advertising Support (AS)

3. Generate primes such that

$n_i = pi_1, pi_2, pi_3.....pi_k, \forall\, i = 1, 2, 3.....r$

say $i = 1$

$N_1 = \{P_{i1}, P_{i2}, P_{i3},,..... P_{ik}\}$

$n_i = \overset{k}{\pi}_{k=1}\ pi_k \qquad i = 1, 2, ...r$

4(a) Compute E_i and D_i g.c.d of $(E_i, J_2(n_i)) = 1$
$\rightarrow D_i = E_i^{-1} (\text{mod } J_2(n_i))$
$D = D_{i1}, D_{i2}, \ldots, D_{ir}$
$\rightarrow D_i = E_i^{-1} (\text{mod } J_2(n_i))$
(b) $D_{ik} = D$ [mod $(p_i^k - 1)$], $k=1,2,\quad i=1,2,\ldots r$

Public Key (K, E, n_i)
Private Key (K, D, n_i)

Classification Phase:

- If all Distributors in d have the same category di then
- Return a leaf node whose category is set of di
- End if
- Determine the attribute A that best classifies the Distributors in "d" and assign it as the test attribute for the current tree node
- Create a new node for every possible value ai (A) and recursively call this method on it with R^1 □ (R □ {A}) *and* d^1 □ d (ai)

7. Conclusion.

In this paper, we proposed a new Algorithm for secure classification, verification and development of decision tree to the Manufacturer for selecting the Best Distributor among the available Distributors by using M-prime RSA Cryptosystem in B2B Scenario.

8. References.

[1] Sumit Chakraborthy, Asim Kumar Pal , "Privacy preserving Collaborative Business Process Management", Business Process Management Workshops 2007, Springer 2008, 24-09-2007, pp.306-315

[2] "Reinventing the Web Channel to Maximize B2B Sales and Customer Satisfaction – January 2011"

[3] H. Saini, D. Saini and N. Gupta, " E-Business system development: review on methods, design factors, techniques and tools with an extensive case study for secure online retail selling industry", International Journal of Science and Technology, Vol 2. No.5 (May 2009), pp.82-90

[4] Lalanthika Vasudevan , S. E. Deepa Sukanya , N. Aarthi, "Privacy Preserving Data Mining Using Cryptographic Role Based Access Control Approach", Proceedings of the International MultiConference of Engineers and Computer Scientists 2008, Vol IIMECS 2008, Hong Kong, 19-21 March, 2008.

[5] Leonard A.Breslow and David W. Aha, "Simplified Decision Trees: A survey", The Knowledge Engineering Review, Vol.12:1, 1997, pp.1-40.

[6] Quinlan, J.R. "Induction of decision trees", Machine Learning", vol.1, No.1, 1986, pp. 81-106.

[7] C. Phani Ramesh, Prof. M. Padmavathamma, "Threshold Secure B2B Model", IOSR Journal of Computer Engineering, Vol.5, No.6, Sep-Oct, 2012, pp.11-14.

[8] Ueli Maurer, "Secure Multi-party computation made simple", Security in Communication Networks, Vol.2576, 2003, pp.14-28.

[9] E.Madhusudhan Reddy, B.H. Nagarajasri, A.B. Rajesh Kumar, Prof. M. Padmavathamma , "New Variant MJ2 – RSA Cryptosystem", Software Engineering and Service Science, July 2011, pp.142-145.