© 2017 IJSRST | Volume 3 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Scienceand Technology

The Analysis of Security Issues and Threat Prevention Model in E-Commerce

Dr. Sharad Gangele[1], Deepika Pathak[2] and Dr. Dhanraj Verma[3]
[1,2]Department of Computer Science & Application, RKDF University, Bhopal, MP, India
sharadgangele@gmail.com
[3]Department of Computer Science & Engineering, Dr. APJ Abdul Kalam, Indore, MP, India

ABSTRACT

Large online retailers are trying to establish secure transaction technologies to reduce the rate of fraudulent transactions. The rapid development of communication technologies and standardizations have created possible growth in e-commerce. Reduction in the operation cost, enhancement in the transactions speed and easy availability to customers became the reasons for the popularity of e-commerce. This paper examines the issues related to the security and threat prevention of the assets and transactions in the e-commerce components and activities. In ecommerce transactions, large amount of public money is involved, so role of information security and privacy is important in this type of business. E-commerce security is analyzed as an engineering management task and a life cycle approach is introduced. Finally, an exploratory survey of various e-commerce security framework and models are analyzed and security collaboration and model is presented.

Keywords: E-Commerce, Security Framework, Threat Prevention, Vulnerability.

I. INTRODUCTION

E-Commerce is the buying and selling of products and services, transaction of amount, over an electronic network as Internet. These business transactions occur either as business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. These are four main categories and subfields as [1]:

1) **Business-To-Business (B2B):** It is electronic trading between companies with for improving their supply chain management processes [2].
2) **Business-To-Consumer (B2C):** It is electronic trading between a company and its consumers (most prominent example for it is Amazon [3]).
3) **Consumer-To-Consumer (C2C):** It is electronic trading between consumers (most publicly known example for that is eBay [4]).
4) **Consumer-To-Business (C2B):** It is electronic trading between consumers and businesses (most notable example for this is Task Rabbit [5]).

E-commerce includes shopping for commerce merchandise over internet and various business processes inside individual organizations that support the goal. Like e-commerce, e-business also adds wide range of features definitions and it is applied in variety of various contexts [6]. E-commerce has been taking experience of evolution through the adoption of Internet capabilities to increase customer participation and achieve high economic value. In addition, there is more research on social commerce and some significant research devoted to the social commerce platforms design. This study offers exploratory survey to justify the concept of social commerce, covers its state-of-the-art, and discusses related design features as they relate to the E-commerce [7]. We propose a new resource utilization framework and a set of unified guiding for social commerce design. The performance of e-commerce depends on the wide availability of goods and services for the consumer, the speed of access, easy accessibility and international access. Its comprehended downsides including sometimes-limited customer service, consumers unable to see or touch a product prior to buy, and requires wait time for product shipping.

In a E-commerce framework, the merchant offers a catalog of available products or services on the website which is available and accessible for the general public and global reach [8][9]. The merchant execute the e-commerce shop software on their servers and outsource this additional sales channel to a 3rd party web

hosting company using Cloud Service Provider (CSP). Moreover, the E-commerce shop software itself can be developed by the merchant on the market [10]. For business accounting purposes, the merchant also runs a bank account with an acquirer (see Figure 1).

II. LITERATURES REVIEW

The study of Sen *et al.* started with an introduction of e-commerce and specifies possible categories of it. It further represents the profits of e-commerce with its limitations also. Here they observed security issues of the system and the communication protocols used in transactions. In this work they listed the related stakeholders of an e-commerce transaction and identify the credit card payment procedure in detail. They concluded with an study of the security features of a online shop and presents that those are not limited to technical aspects, but always consider the consumers behaviors on the Internet [1]. Sobko's presented the non-cash transactions and it began with a categorization of non-cash payments including online banking, credit and debit cards which are handed out to individuals by financial institutions. They observed possible 56 ways to lead on an individual with the objective to get access to credit card information such as skimming and phishing. He explained that once a transaction has been successfully executed using a stolen credit card, the information about it will be sold on the black market to other fraudsters, who will then use the same credit card to make additional purchases. Moreover, this research discussed the impact of fraudulent transactions for the merchants and credit card owners, as well as presents technological advances and regulations which have been developed to protect against non-cash fraud transactions [11].The research of Rana *et al.* proposed the actual frauds in e-commerce and how they can be noticed with current fraud prevention systems. They explained different implementations of fraud and threat detection algorithms, which range from a simple rule-based filtering to score-based solutions using fuzzy logic. They concluded that existing systems can cover up to 80% of fraudulent transactions at manageable efforts and costs. More coverage can be accomplished by combining existing solutions with information of the profile of card owner, which would introduce credit card usages patterns into this analysis. Still this analysis is very expensive to implement and operate [12]. Carvalho *et al.* presented a view point formulation on investigation procedure with the help of banking frauds as an example. It presents that the investigation of them is a very complex work that requires further collaboration between experts. However, by sharing the information will not be adequate as a common understanding of the different characteristic and terms is needed. Therefore they present that finding a common language to exchange information is very crucial for the success of the research. They also developed a model to describe the domain of online banking fraud investigation. It explains on the objects and their relations in detail and presents that reusing concepts and terms from present vocabularies can be helpful when designing a model. They found semantic technologies which can have an optimistic impact on the crime investigation as they also proved primary reasoning capabilities on the data sets, as well as offering support for the aggregation of information coming from several sources. Finally they analysed semantic technology to be very crucial in future cyber-crime investigations [13].

The basic concepts, approaches and technologies for contribution of data on the Web presents how a "Resource Description Framework" (RDF) data set should be applied to publish organized data on the Web, and prepare rules for these resources. Additionally, it discusses the commonly used vocabularies available on the Web, and explains ways how to link together various resources on the Internet. After describing different kinds of applications that are possible with the technologies shown, it gives an outlook of future research, which also states the aspects of schema mapping and data fusion as possible challenges. Other issues in the area of Linked data are related to privacy violations that become possible when information from different sources is combined. As conclusion the authors consider the Linked data approach as intermediate step to a Semantic Web, because it follows the same established Web standards like RDF, RDFS and SPARQL, but uses a more pragmatic approach by getting rid of all the complexities involved when having to create, maintain and use elaborate ontologies in OWL [14]. Different ways to publish semantic data on the Web have been analysed by Laurens Rietveld *et al.* They show that current approaches range from simple data dumps of complete RDF data sets to publicly available query endpoints

using the SPARQL protocol and query language. As a conclusion they state that the more flexible approach of SPARQL endpoints is generally not working on the Internet, but is instead more suitable for internal data collection and analysis. This is due to the enormous overhead of a SPARQL server both in memory and CPU consumption if it has to deal with a large RDF data set and a huge number of concurrent users. The former provides subsets of a RDF data set optimized for specific subjects or objects and allow focused querying of a RDF data set. As a result of the work new approaches have been proposed for offering RDF data sets on the Web, which are optimized for querying and processing large scale RDF data sets, and make better use of the processing capabilities of clients [15].

The need for a RDF vocabulary to express products and offerings on the Internet was first mentioned and described by Martin Hepp. The author was also the founder of the GoodRelations vocabulary, which he explains in detail in his work. After showing possible use case scenarios for such ontology on the Web the author elaborates the available entities and their meanings. Interestingly, the author states that he has restricted usage of more expressive OWL axioms in the GoodRelations vocabulary due to the limited availability of full-featured OWL reasoners. By focusing on RDFS constraints only less advanced functionality is required for the processing engine of the RDF data sets. The research work closes with examples of using the vocabulary in the ecommerce scenario and its possible future development for B2B service integrations [16].

III. TECHNICAL ASPECTS OF E-COMMERCE

When placing an order with a merchant online, the consumers normally use a credit card for finalizing the transaction. These credit cards have originally been handed out to the consumers by the issuers [17]. Additionally, in some online shops it is mandatory for the consumers to create a user account with them, while in others it is not. The former is the preferred way when consumers are repetitively buying from that merchant, whereas the latter might be used for onetime or irregular shopping trips online. To be able to connect to the Internet the consumers also rely on a service offered by an Internet Service Provider (ISP) [18][19]. The whole initial setup for participating in E-commerce activities is found in Figure 1. When a consumer places an order online, the merchant receives at least a list of products or services from the current shopping cart of the consumer, the identification of the consumer, as well as the delivery address to ship thephysical items to. If the transaction is going to be finalized with a credit card, the consumer will have to provide additional information such as the billing address and the credit card details including the number, the expiry date and the security code of the card.

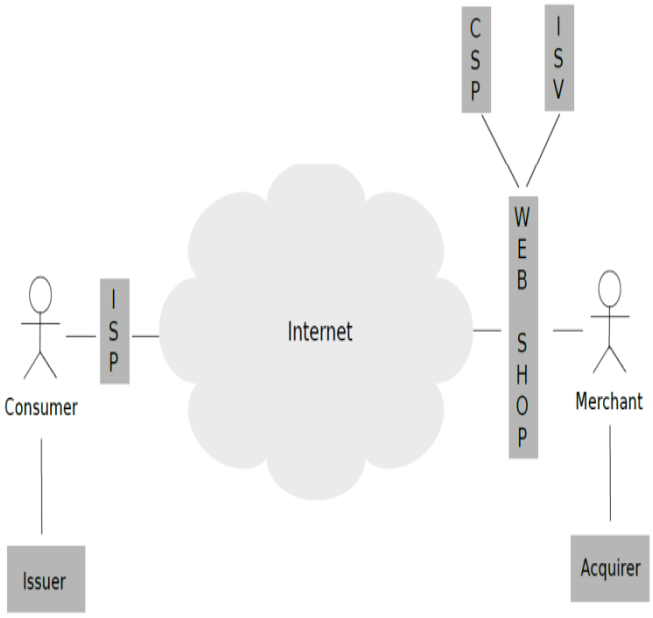

Figure 1. E-Commerce Fundamentals

The merchant receives the status of the authorization as well as a unique payment token in return. If the authorization has been successful, the merchant collects the items and sends out a shipping request to one of the available Logistic Service Providers (LSP), which are capable of delivering the order. They pickup the items at the merchant's facility and ship them to the delivery address stated by the consumer.

Usually at about the same time the merchant informs the acquirer about the order, amount due as well as the payment token received from the PSP. The acquirer is in charge to withdraw the amount of the order from the consumer's bank account either via the PSP or directly from the issuer, depending on who of them has authorized the initial payment request - a process called clearing [20]. The sequence of activities within an e-commerce checkout process is visualized in Figure 2.

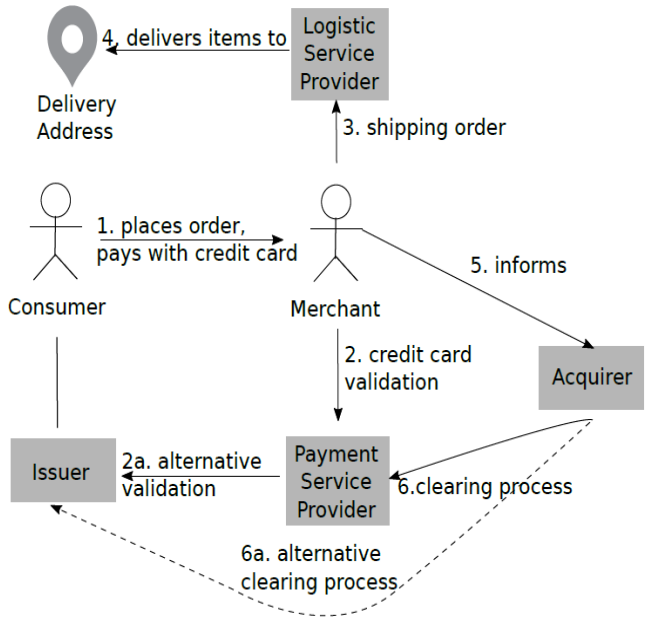

Figure 2. E-Commerce Checkout Process in Detail

IV. EXISTING SYSTEM

Based on the analysis, and especially the scope definition for the collaborative system for investigating e-commerce fraud incidents has to answer the central question:

> *Is this transaction really a valid e-commerce transaction?*

Looking into the stakeholders, who can provide useful information to decide it, one will come up with:

1) **Merchants,** who can provide additional information of each e-commerce transaction in question.
2) **PSPs/issuers,** who have information about the credit card usage patterns and the original credit card owners.
3) **LSPs,** who can offer information about whether an order has already been shipped or not, and in the former case to whom it has been handed over.

Ideally, each of those participants would make parts of their internal databases available for the others to access and query for information in a shared information space. That would allow those stakeholders, who have to authorize or validate a suspicious credit card transaction, to analyse all available information as depicted in the Figure 3.

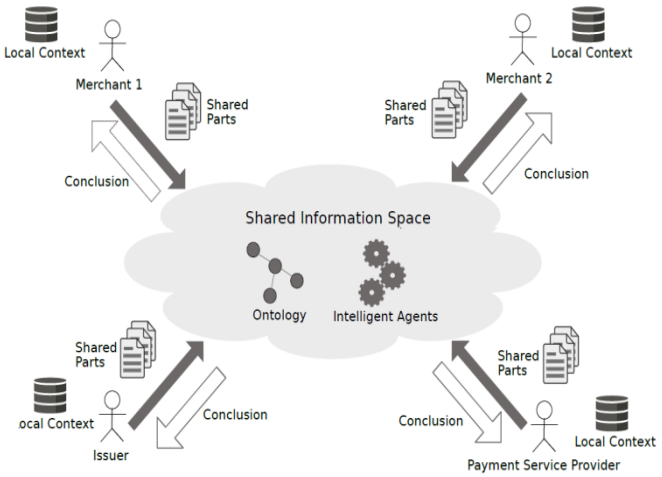

Figure 3. Existing E-Commerce Transaction System

In this figure one can see, how the relevant parties provide access to parts of their internal local context information within a shared information space. The collaborative system should allow participants to communicate and collaborate on the e-commerce fraud incidents from different places at the same time. Due to the fact that data from various sources have to be combined into a shared understanding of the e-commerce activities of a consumer, there is a need to harmonize and transform the information from each participant into a common data model to be able to analyse the combined data set. Based on the shared understanding of the e-commerce activities that have been done with a credit card recently, a set of intelligent agents (aka analysis tools) can assess them and present their findings, which can be valuable to any of the participants of the collaborative system.

V. PROPOSED METHOD

The proposed security framework of e-commerce system is presented in Figure 4, in which the linked data set will initially 58 collect and cluster the information from each merchant based on this list. In case there are already suspicious information in one of these clusters, an issuer can ask for further details and enrich that specific cluster with additional order information for this consumer and that merchant. In the final step the system has to do the mapping and linking of the order detail information between each merchant to allow subsequent analyzing and clustering of the transaction details based on various criteria.

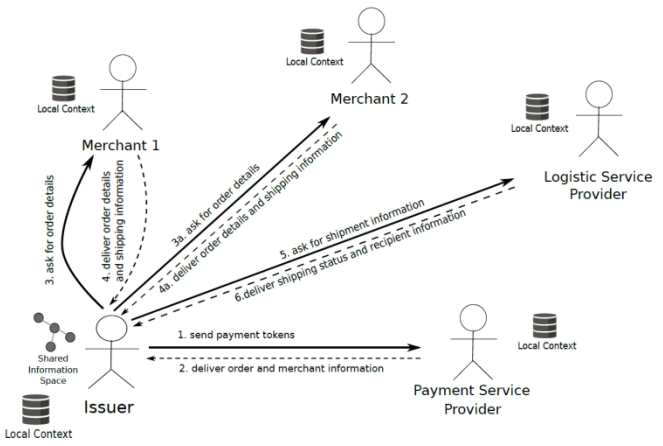

Figure 4. Information Flow in the Proposed Collaborative System

VI. CONCLUSION

In this paper, exploratory survey of different e-commerce security framework and models has been analyzed. It is found that the demand for real-time security services is increasing in e-commerce applications. This analysis has shown that the technical issues, which lead to insecure and threatful transactions in the e-commerce scenario, can be solved partially by introducing new security procedures, but require a security collaboration and framework of different experts on the edge cases. This collaboration and framework can become more efficient and effective, if a shared information space is used, which combine and link together the information from the relevant stakeholders in e-commerce system.

REFERENCES

[1]. P. Sen, R. A. Ahmed, and M. R. Islam, "A study on e-commerce security issues and solutions," 2015.

[2]. C. Lin, Y.-A. Huang, and J. Burn, "Realising b2b e-commerce benefits: the link with it maturity, evaluation practices, and b2bec adoption readiness," European Journal of Information Systems, vol. 16, no. 6, pp. 806-819, Dec 2007.

[3]. I. Adaji and J. Vassileva, Perceived Effectiveness, Credibility and Continuance Intention in E-commerce: A Study of Amazon. Cham: Springer International Publishing, 2017, pp. 293-306.

[4]. K. Le-Nguyen and Y. Guo, "Choosing e-commerce strategies: a case study of ebay.vn partnership," Journal of Information Technology Teaching Cases, vol. 6, no. 1, pp. 1-14, May 2016.

[5]. M. Iguchi, M. Terada, Y. Nakamura, and K. Fujimura, A Voucher-Integrated Trading Model for C2B and C2C ECommerce System Development. Boston, MA: Springer US, 2003, pp. 415-429.

[6]. H. Xu, D. Liu, H. Wang, and A. Stavrou, "An empirical investigation of ecommerce-reputation-escalation-as-a-service," ACM Trans. Web, vol. 11, no. 2, pp. 13:1-13:35, May 2017.

[7]. E. ehirli and lhami M. Orak, "E-commerce according to hobby," Procedia - Social and Behavioral Sciences, vol. 143, no. Supplement C, pp. 1144 - 1147, 2014, 3rd Cyprus International Conference on Educational Research, CY-ICER 2014, 30 January-1 February 2014, Lefkosa, North Cyprus.

[8]. E. Ofuonye, P. Beatty, I. Reay, S. Dick, and J. Miller, "How do we build trust into e-commerce web sites?" IEEE Software, vol. 25, no. 5, pp. 7-9, Sept 2008.

[9]. M. Hecker, T. S. Dillon, and E. Chang, "Privacy ontology support for e-commerce," IEEE Internet Computing, vol. 12, no. 2, pp. 54-61, March 2008.

[10]. K. J. Lin, "E-commerce technology: Back to a prominent future," IEEE Internet Computing, vol. 12, no. 1, pp. 60-65, Jan 2008.

[11]. O. V. Sobko, "Fraud in non-cash transactions: Methods, tendencies and threats," World Applied Sciences Journal, vol. 29, no. 6, pp. 774-778, 2014.

[12]. P. J. Rana and J. Baria, "A survey on fraud detection techniques in ecommerce," International Journal of Computer Applications, vol. 113, no. 14, 2015.

[13]. R. Carvalho, M. Goldsmith, S. Creese, and B. F. Police, "Applying semantic technologies to fight online banking fraud."

[14]. C. Bizer, T. Heath, and T. Berners-Lee, "Linked data-the story so far," Semantic Services, Interoperability and Web Applications: Emerging Concepts, pp. 205-227, 2009.

[15]. L. Rietveld, R. Verborgh, W. Beek, M. Vander Sande, and S. Schlobach, "Linked data-as-a-service: the semantic web redeployed," in European Semantic Web Conference. Springer, 2015, pp. 471-487.

[16]. M. Hepp, "Goodrelations: An ontology for describing products and services offers on the web," in Knowledge Engineering: Practice and Patterns. Springer, 2008, pp. 329-346.
[17]. Y. Zou, Q. Zhang, and X. Zhao, "Improving the usability of e-commerce applications using business processes," IEEE Transactions on Software Engineering, vol. 33, no. 12, pp. 837-855, Dec 2007.
[18]. C. C. Albrecht, D. L. Dean, and J. V. Hansen, "An ontological approach to evaluating standards in e-commerce platforms," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 37, no. 5, pp. 846-859, Sept 2007.
[19]. K. L. Roche, "How to succeed in e-commerce," IEEE Review, vol. 52, no. 3, pp. 49-49, March 2006.
[20]. P. Giorgini, F. Massacci, and J. Mylopoulos, Requirement Engineering Meets Security: A Case Study on Modelling Secure Electronic Transactions by VISA and Mastercard. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 263-276.