Reputation Model in E-commerce: A systematic literature review

Marta Alexandra Guerra Magalhães Coelho

ISCAP, Politécnico do Porto

Maria José Angélico Gonçalves

CEOS.PP, ISCAP, Politécnico do Porto

Rui Humberto Pereira

CEOS.PP, ISCAP, Politécnico do Porto

15 de Junho, 2022

Abstract

The Digital Era is the present, and no one can deny that. With it came a digital transformation in several sectors of activity. E-commerce is not an exception, confronting us with new challenges such as the need of having confidence in new buyers, suppliers, customers, business partners, or investors, a crucial need, but not exactly easy to overcome. Thus, this study systematizes the knowledge generated by reputation models in E-commerce studies in Scopus, WoS databases, and Google Scholar.

A systematic approach was adopted in conducting the literature review. Results demonstrate that, in addition to identifying some indicators present in reputation models, we also conclude that these models could help provide some insurance to buyers and sellers, with a commitment to being a problem solver, being able to mitigate the known problems such as Collusion, Sybil attacks, laundering attacks, and preventing online fraud ranging from ballot stuffing and bad-mouthing.

These security and fraud issues are critical because users' trust is commonly based on reputation models, and many of these current models are not immune to them, thus, compromising the E-commerce growth.

Keywords: Ecommerce; Reputation Model; Security; Privacy

Introduction

E-commerce is an important part of our daily life. We have a huge number of platforms created with the sole intent to make our life easier. Online transactions have increased throughout the years thanks to platforms like Amazon, eBay, and others, that allow the buyer to find it all online, from technology to everyday essentials. Not only these platforms but also the arrival of cryptocurrency made it very necessary to establish a robust and impartial reputation model, that can assure security to sellers and buyers. The main reason is to know that we can create a long-term relationship with serious parts, both sellers and buyers.

One might think that the buyer is the one that needs to have more insurance since there's no physical place to complain, and the payment is in advance. For that reason, they rely on the reputation the seller and product have, and this information must be the most accurate possible. But it is also important for the seller to be assured that the buyer is an honest client and not a competitor that might leave a negative rate. Here enters the reputation model, which is used to grant confidence between all parties involved in the transaction, due to the increase in cybercrimes and perception of risks regarding online transactions. The need for a better knowledge of the seller, before deciding to transact, motivated the creation of a reputation model, that has a more relevant role in the present online transactions. Reputation models are programs or algorithms that allow the users of the platform to evaluate each other in order to gain trust. (Resnick, Z, et al., 2000).

It will be discussed, in this paper, several models that were suggested as problem solvers, it will be explained the results and limitations of these models.

It is important to acknowledge the relevance of such models on B2C and on C2C online transactions, this review will enlighten us about what has been done to overcome the difficulties of having a transparent reputation, and where we need to point the focus for future advances in this area.

The articles that were selected, and will be discussed in this article, for this review, approaches the main problems that online transactions faces, and through a very solid and in-depth reading, revealed to be very contextualized with the subject in hands, being very self-explanatory. They approach the existing reputation models and present solutions for the limitations of such models, even though, with the evolution of technology, further studies and adaptations are, always, required.

We intend to present the results of the purposed reputation models and the difficulties they faced during the development of such models.

This article will follow the next guidelines: an explication of the methodology used for the selection of the articles in review, the results of the review, and a brief discussion of the current models.

Related Work

The review showed similar reputation models, and they have in mind the same limitations and difficulties, most being the cost of a reservoir for data information and the preservation of privacy and anonymity.

Dennis & Owen (2015) state that removing human behavior and basing the reputation on a binary rating score of 0 (zero) and 1 (one) would be more efficient.

Ahn et al. (2019) state that human behavior and psychological factors based on an online payment system can be used to assure the trustworthiness of the review.

Joshi & Kumar (2020) also mention the importance of historic purchases to see if the reviewer is eligible to give an informed opinion.

Ramachandiran (2018) claims that buyers must be able to compare metrics, by a binary, stars or points rating system, across product category, title, and full description lengths, number of chances to edit a published review, media type, and size limit.

Liu et al. (2021) presented a reputation model based on three transactions, the normal transaction, purchase, a transaction that is based on the return of the item, and repurchase behavior.

Kugblenu & Vuorimaa (2020) brings light to a limitation of some models such as how to incentivize retailers to be part of the permissioned data information reservoir.

Methodological approach

In line with the aim of the study, which consists of a better understanding of the existing reputation models, it was determined to conduct a systematic literature review mapping following the guidelines of Petersen et al. (2015) and the suggestions of Kitchenham (2007). This methodology also enables the structuring of a solid scientific ground to stand in the analysis of the current state of art surrounding reputation models in E-commerce.

Research question

The initial group of research questions were

1. Which are the common kind of attacks and frauds on users' reputation on e-commerce platforms?

2. What are the main approaches and techniques to increase the users' trust in e-commerce transactions?

Search strategy and study selection process

The search string was constructed based on the key term content of the title of this study.

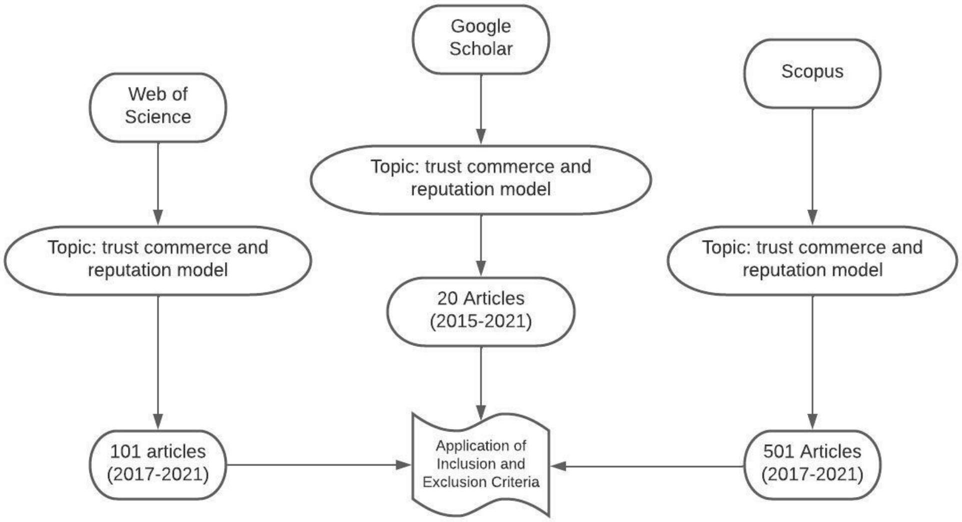
TOPIC: trust commerce and reputation model

The string terms were searched against the title, abstract, author keywords, and Keywords Plus of the articles. The primary search was developed during May 2021.

The research was conducted in the three main databases where the journals with the most significant impact factor in knowledge are located. The use of these databases makes the article more robust since it covers more journals, of greater academic importance, in this area of knowledge.

In Figure 1 we summarize the research layout and results that led to the final set of articles. As referred the search was conducted in May and the studies were analyzed between May, June, and July 2021. The number of articles retrieved from each database were: Web of Science: 101, Scopus: 501, and Google Scholar: 20.

Figure 1 - Sources and Structure of selection


Google Scholar
Web of Science
Scopus
Topic: trust commerce and reputation model
Topic: trust commerce and reputation model
Topic: trust commerce and reputation model
20 Articles (2015-2021)
101 articles (2017-2021)
Application of Inclusion and Exclusion Criteria
501 Articles (2017-2021)

The I/E (inclusion/Exclusion) criteria were applied to the title and abstract of the articles. Articles meeting the formula (E1 OR E2 OR E3 OR E4) were excluded and those meeting (I1 AND I2 AND I3 AND I4) were included, as presented in Table 1. Based on this search strategy and the selection process outlined above, duplicate articles were eliminated and the ones with a specific reputation model as a primary study were selected, the selection was between February and March 2022.

Table 1 - Include/Exclude Criteria

Inclusion criteria	Exclusion criteria
I1 - Selected research Databases	E1 - The paper is not available for viewing
I2 - Publication between 2015 and 2021	E2 - Duplicate papers
I3 - English papers	E3 - Articles that do not address reputational models
I4 - Articles that address specific reputation models that are applied to Ecommerce	

Paper quality evaluation

The evaluation of the quality of the studies was carried out to determine the level of detail of the articles, considering that: High value - the article clearly explains a tested reputation model applied to business; Medium value - the article explains a reputation model in a theoretical approach; and Low value - the article does not address a reputation model in sufficient detail.

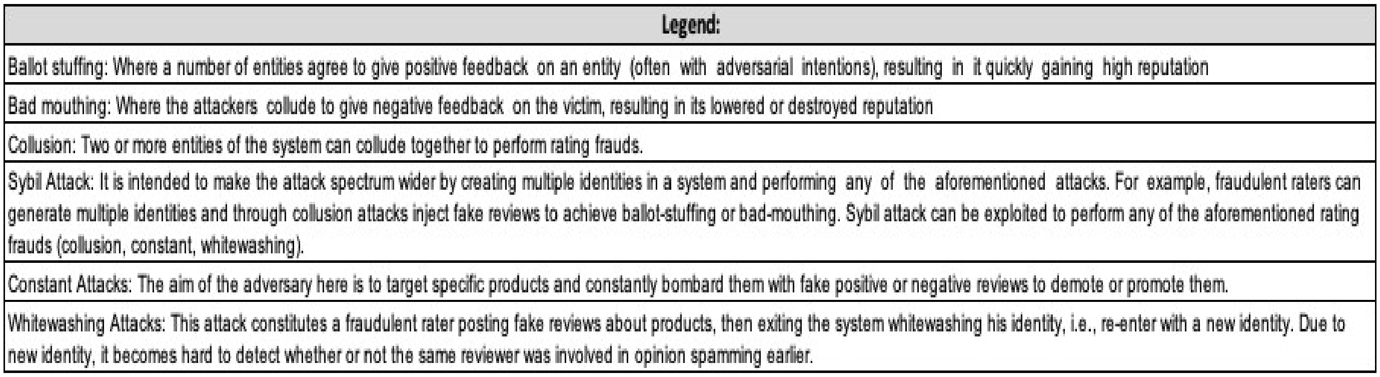
Results Analyses and Discussion

On a primary analysis, we were able to identify some of the known current attacks online platforms deal with daily. Acknowledging those attacks was step one, and then we started the search for literature where one can find more about what the technology and its science is doing to prevent or mitigate those attacks, which are mentioned in table 2.

Table 2 - Current attacks and meaning

Fraud	Attack
Ballot stuffing	Collusion
Bad mouthing	Sybil Attack
	Constant Attacks
	Whitewashing Attacks

Figure 2 - Legend of table 2



Legend:
Ballot stuffing: Where a number of entities agree to give positive feedback on an entity (often with adversarial intentions), resulting in it quickly gaining high reputation
Bad mouthing: Where the attackers collude to give negative feedback on the victim, resulting in its lowered or destroyed reputation
Collusion: Two or more entities of the system can collude together to perform rating frauds.
Sybil Attack: It is intended to make the attack spectrum wider by creating multiple identities in a system and performing any of the aforementioned attacks. For example, fraudulent raters can generate multiple identities and through collusion attacks inject fake reviews to achieve ballot-stuffing or bad-mouthing. Sybil attack can be exploited to perform any of the aforementioned rating frauds (collusion, constant, whitewashing).
Constant Attacks: The aim of the adversary here is to target specific products and constantly bombard them with fake positive or negative reviews to demote or promote them.
Whitewashing Attacks: This attack constitutes a fraudulent rater posting fake reviews about products, then exiting the system whitewashing his identity, i.e., re-enter with a new identity. Due to new identity, it becomes hard to detect whether or not the same reviewer was involved in opinion spamming earlier.

Source – Authors of the literature review

In these analyses, we will be getting into a more detailed discussion about the results presented by the prior authors mentioned.

Dennis & Owen (2015) state that removing human behavior and basing the reputation on a binary rating score of 0 (zero) and 1 (one) would be more efficient, meaning that every successful transaction gains a reputation score of 1 (one) and the reputation is the sum of the scores. In this model, the buyers send the info that the product was received, and the information is sent to miners ensuring that the transaction is real. On the other hand, Ahn et al. (2019) state that human behavior and psychological factors based on an online payment system can be used to assure the trustworthiness of the review, using the historic of purchase to analyze such behavior, this was reinforced by Joshi & Kumar (2020) that also mention the importance of historic purchase to see if the reviewer is eligible to give an informed opinion.

Another study conforming Dennis & Owen (2015) statement comes from Ramachandiran R., (2018) claiming that buyers must be able to compare metrics, by a binary, stars or points rating system, across product category, title, and full description lengths, number of chances to edit a published review, media type and size limit, also stating that all sellers must use existing product category codes with all these parameters built into them.

Still regarding the model of Dennis & Owen (2015) in order for the user to not be able to create several accounts is to link the indemnity creation to the IP address. To prevent collusion attacks, the reputation will be given on an average scale, so they can't trade between themselves to gain reputation. So, if two nodes are transacting together, the reputation score will be the same whether it is one transaction or a thousand. This requires a lot of data which is translated to a considerable space require storing the information and, in its turn, more costs.

However, this is only an idea, and more studies need to be made to prove the efficiency and reliability of this method.

Nonetheless, transactions have many forms, Liu et al., (2021) presented a reputation model based on three transactions, the normal transaction, purchase, and a transaction that is based on the return of the item (transaction with return in 7 days after delivery or 15 days after order of payment) and repurchase behavior (buying the same or other products from the same seller).

They present a mathematic equation to calculate the reputation of seller and buyer, proving the robustness of the model against unfair ratings, nevertheless, they intend to propose a model that can resist collusive attack.

A way to resist this attack is the sharing of reputation throughout platforms, Li et al., (2021), affirms that it is important that platforms collaborate in sharing suppliers' reputation. The model that they present, relies on a third party, besides the platform, buyers, and sellers, to assure the accuracy of the reputation. The security and privacy analysis validate that RepChain, the reputation model proposed, protects rating privacy, identity privacy, and unlikability. It also resists to multiple rating attacks and abnormal rating attacks. The experimental results show that the computational costs and communication overhead of RepChain are moderate compared to existing work.

This type of reputation model, based on sharing information across multiple platforms, normally uses Tokens, a sort of digital fingerprint of the user, that can be exchanged to buy or sell products. Dhakal, A., & Cui, X., (2019), brought attention, that this method, makes us face a possible raise of Sybil attacks because it makes it easier for the attackers to create a platform and assign a reputation to themselves. Their main goal is not to have the reputation data controlled by third parties, making the data transparent and impossible to manipulate. Besides the Sybil attack, a model that allows the sharing of information has other weaknesses such as increasing cost in transactions and only being suitable for e-commerce platforms. In the future, they intend to use artificial intelligence to validate the authenticity of reviews.

The Tokens, mentioned before to ensure privacy, ratings, and reviews of the same products sold on different platforms, are also included in a reputation model that guarantees anonymity because the product review is tied to a verified order and product, not identity. The limitation found by Kugblenu & Vuorimaa, (2020), is how to incentivize retailers to be part of the permissioned data information reservoir, and the malicious behavior some retailers might pursue executing some undefendable attacks such as collusion attacks. Customer orders in malicious retailers' systems could be faked to give the impression of proof of purchase. However, the overall impact will be low.

We must have in mind that reputation has both sides, this was said by Sun et al., (2020), referring that it is important because it is the basis of a mutual judgment, and that the integration of the reputation mechanism into a consensus can promote normal operation making the model more secure. The analysis shows that this model can resist the most attacks. The consensus consists in uploading the information that will be verified by a selected group of members that will validate the data and confirm its accuracy. Through the consensus protocol, buyers leave a numeric ratio score for the seller, and the seller can sell products establishing a reputation from buyers' feedback, sellers also act as stakeholders and collaboratively maintain a public ledger. Each buyer will obtain an anonymous identity credential. This model, proposed by Liu et al., (2019), provides high privacy guarantees for buyers, and it has been proven feasible.

The biggest limitation is still the fear of retaliation once negative feedback has been given, this stops users from sending this feedback. Schaub et al., (2016), aimed to achieve trustlessness, to be suitable for e-commerce, be decentralized and robust and assure the preservation of anonymity. The robustness of the model will prevent attacks such as Bad-mouthing, ballot-stuffing, whitewashing, and Sybil attacks. The way to guarantee that these attacks are prevented is through anonymity, and the anonymity comes from the Tokens that are given to users as a code, the already mentioned digital fingerprints. One problem with the model presented by Schaub et al., (2016), is the money needed to produce enough tokens while limiting ballot-stuffing attacks. Also, a definite way to prevent the leakage of information must be considered, nonetheless, they are assertive saying that this would be a valuable model because the risk that the privacy of the users could be breached is minimal.

Another way to try to convince users to leave feedback is an award method, one gives feedback and receives points or discounts, many platforms use this type of reward-attracting method, but one must be able to guarantee the veracity of the feedback.

Conclusion

It seems to be a consensus on the variables that a reputation model needs, one must have a rating score, and human behavior has a word on it, whether in the absence or as a modus operandi of the user and the information of the users is the most relevant variable. Also, the information must be private, and anonymity must be assured.

Another consensus is that the costs might have a say when it is time to decide if the model is suitable or not, the more information we have, the more storage we need, and to grant that anonymity we will have to give the users a unique digital identity, and that also cost money.

Also, the granting of rewards will affect the seller's profit and might influence the buyer. It is safe to say people react to prizes, and no matter how small, they are always welcomed. The price discounts might grant customer loyalty to the seller, but it is not a way to guarantee that the seller is a good seller, it might give him a good reputation percentage, but it also might be because the prices are low.

On the other hand, the return policy can be used as one key point to develop a model that can be more trustworthy. The more returns, the less reliable the products are, e.g., the seller. It’s certain that the more information we have, the more we can assure a more trustworthy reputation model. However, the security of those data is not very explicit and there’s a lack of information on how they will prevent the breaching of data.

Some reputation models intended to solve the collusion problems of reputation models by allowing the seller to calculate the reputation score based on parameters set by them. This type of model alone would not be able to solve all problems since there will not be an impartial party, if the seller sets the parameters, the seller controls the outcome.

Creating a reputation model which is to store reputation from completed transactions seems to be a good way to increase the reputation and being able to be implemented into any network is a plus.

Nevertheless, it is important to pay attention to psychological factors to increase the reliability of a reputation model but associated with other information. However, emotions, sociocultural factors, inborn or acquires factors and the friend-to-friend information are important, we trust the people we know and the people that have a similar background, but that alone is not enough.

All of this must be held into account when discussing a reputation model. More analysis shall be conducted, so it will be possible to present a more robust, assertive, and reliable reputation model as well as a reservoir that assures the privacy and protection of the information of the users on online platforms.

References

Ahn, J., Park, M., & Paek, J. (2018). Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System. At 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE. https://doi.org/10.1109/ictc.2018.8539641

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583. https://doi.org/10.1016/j.jss.2006.07.009

Dennis, R., & Owen, G. (2015). Rep on the block: A next generation reputation model based on the blockchain. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE. https://doi.org/10.1109/icitst.2015.7412073

Dennis, R., & Owen, G. (2015). Rep on the block: A next generation reputation model based on the blockchain. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE. https://doi.org/10.1109/icitst.2015.7412073

Dhakal, A., & Cui, X., (2019). DTrust: A Decentralized Reputation model for E-commerce Marketplaces.

Joshi, P., & Kumar, A. (2020). A Novel Framework for Decentralized C2C E-commerce using Smart Contract. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE. https://doi.org/10.1109/icccnt49239.2020.9225377

Kugblenu, C., & Vuorimaa, P. (2020). Decentralized Reputation model on a Permissioned Blockchain for E-Commerce Reviews. In Advances in Intelligent Systems and Computing (pp. 177–182). Springer International Publishing. https://doi.org/10.1007/978-3-030-43020-7_24

Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M., & Alazab, M. (2021). Anonymous and Verifiable Reputation model for E-commerce Platforms based on Blockchain. IEEE Transactions on Network and Service Management, 1. https://doi.org/10.1109/tnsm.2021.3098439

Liu, D., Alahmadi, A., Ni, J., Lin, X., & Shen, X. (2019). Anonymous Reputation model for IIoT-Enabled Retail Marketing Atop PoS Blockchain. IEEE Transactions on Industrial Informatics, 15(6), 3527–3537. https://doi.org/10.1109/tii.2019.2898900

Liu, Y., Zhou, X., & Yu, H. (2021). 3R model: A post-purchase context-aware reputation model to mitigate unfair ratings in e-commerce. Knowledge-Based Systems, 231, 107441. https://doi.org/10.1016/j.knosys.2021.107441

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, *64*, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007

Ramachandiran, R., (2018). Using Blockchain Technology to Improve Trust In eCommerce Reviews. 10.13140/RG.2.2.29324.00646.

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation models. Communications of the ACM, 43(12), 45–48. https://doi.org/10.1145/355112.355122

Schaub, A., Bazin, R., Hasan, O., & Brunie, L. (2016). A Trustless Privacy-Preserving Reputation model. In ICT Systems Security and Privacy Protection (pp. 398–411). Springer International Publishing. https://doi.org/10.1007/978-3-319-33630-5_27

Sun, Y., Zhang, R., Xue, R., Su, Q., & Li, P. (2020). A Reputation Based Hybrid Consensus for E-Commerce Blockchain. In Web Services – ICWS 2020 (pp. 1–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-59618-7_1