SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

# SURVEY PAPER ON THE VARIOUS SECURITY ALGORITHMS USED FOR E-COMMERCE SECURITY

**Polsani Jahnavi[1], Balla Manoj Kumar[2]**

[1]*School of Computer Science and Engineering , Vellore Institute of Technology, Vellore, 632014, Tamilnadu ,India,*

[2]*School of Computer Science and Engineering ,Vellore Institute of Technology, Vellore, 632014, Tamilnadu , India,*

**Article DOI: https://doi.org/10.36713/epra8839**
**DOI No: 10.36713/epra8839**

**ABSTRACT**

*Due to the growth of e-commerce, most of the banking transactions are made on the online platform and all these transactions are made on the websites provided by the merchant or the payable apps and because of this the vulnerability of attacks has increased and there are also chances of using fraudulent websites and apps by the attackers though there are many high-security algorithms are been used for safeguarding against vulnerabilities. The way of judging the relation of trust on the online platform has become a major issue, so a proper trust model also needs to be maintained. In this paper, we reviewed various security algorithms which involve cryptographic algorithms, machine learning, anonymization, and masking techniques, blockchain, distributed networks, and many more to provide integrity, privacy, reliability, authentication, security, and risk-less e-commerce platform.*

## 1. INTRODUCTION

From the previous decades the use of e-commerce has drastically increased and due to this the number of payment transactions made on online platforms has exponentially grown. E-commerce platforms are exposed to the attacks such as

- Financial fraud: Financial fraud generally occurs through stolen credit card private data, which is further used in purchasing services and products on e-commerce platforms. And, also occurs by false requests for credit returns through unauthorized transactions.
- Phishing attacks: The phishing attacks take place by creating a fake website which is similar to the original website through which the user's confidential data will be captured by attackers.
- Sql injection: In this attack the attackers will inject the code into the database to collect and modify the data.
- DoS attacks: Denial of service attacks will crash the website by producing a lot of requests and make the website unable for the user's.
- Brute Force Attacks: These attacks will crack the passwords by using all possible combinations of characters. Security of payment transactions , and user's private data has become a major concern.

Hence to avoid these attacks proper security protocols need to be followed and some of the security concerns of e-commerce are

- Confidentiality: Confidentiality helps to prevent unauthorised access to data. This protects the data involved in e-commerce transactions. The users with valid authorisation will only have the access to data with this data won't go into the wrong hands to misuse the data.
- Integrity: Integrity helps to prevent the damage to data from unauthorised modification. To obtain integrity we need to ensure that the users can only alter the information if they are authorised. This provides accuracy, trust and validity to the data. Integrity also protects data from

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

unintentional modification which causes damage to the system. In e-commerce with the help of integrity, transactions are made secure from tampering and the information of the customers remains unaltered.

- Availability: Availability helps to provide the information whenever and wherever it is required within a time limit. The information is available to the authorised users when it is needed. Disruption of e-commerce site availability even for a shorter time will cause consumer dissatisfaction and damage the reputation of the business.

In section 2 of the paper we have discussed about various security algorithms in order to provide the required security in e-commerce platform

## 2. SECURITY ALGORITHMS

### A. Algorithm for Providing Integrity

The author[1] tried to propose a mathematical model based on the third-party verification where it acquires two messages from the sender and the receiver and it tries to substantiate the integrity. The integrity of the ordered information and also the payment of the online transaction made is also substantiated with the proposed algorithm. This Payment integrity plays an important role in platforms like online payment where the dealer and merchant don't meet each other and trust needs to be established between them. Here before the confirmation of the product ordered and the payment made the payment authority needs to verify the agreement between the customer and the dealer. Because there are chances where the customer can claim for another order or the payment for the product which could result in a loss to the dealer or on the other side the dealer could also claim for another order or the payment for the product purchased which could result in a loss to the customer. Hence the payment authority which issues the payment plays an important role in the agreement between the customer and the dealer. The model which is proposed by the author[1] mainly concentrated on the payment and order integrity where it is simple to implement.

Whereas in the traditional online purchase system where the sender(customer) sends two messages which are signed PI and OI. Here the OI message is sent to the bank by the dealer who is selling his product. Whereas in the dual signature method the hash of the PI and the OI messages are linked together and this hash is encrypted with the senders(customers) private key. The customers also send the public key to the dealer so that he can compute the sent hash value of the PI and OI if the obtained values match each other the dealer can assume that manipulation has not been done by an attacker and hence it forwards the OI to the bank. In the bank the PI received is substantiated and the final transactions have been made. But the customer information redundancy is the limitation of this model. So the author[1] has proposed a model to address this issue where he mostly concentrated on the three main domains: the customer, dealer, and the authority who is responsible for payment of the transaction made by the customer. Here in this model after receiving the payment request the payment authority starts the whole process of transaction verification. In this model, the customer and the dealer are provided with an account and its linked digital certificates. When the customer makes his purchase of a product from the dealer's website, the digital signatures are sent from the customer to the dealer and these digital signatures are verified with the help of payment authority, where it checks for integrity between the order details and the sender's digital signature. When the payment authority sends an acknowledgement to the dealer he confirms the order. Two integer values are selected randomly by the payment authority and these integers are sent to the customer and the merchant. Now they compute with the formula given in the paper and exchange between themself to calculate the x and y values and send them to the central authority. By this, the central authority will be able to validate the agreement between the consumer and the dealer. This proposed model by the author[1] is more suitable for the transaction with a low payment or when three parties are making a deal with each other where the agreement stands as an evident between the three parties where anyone who tries to break the agreement can be caught easily. The protocol model mentioned in this paper which is used by the payment authority can be made more secure by the usage of a cryptographical algorithm. the only limitation of this proposed model is floating-point calculations are included.

### B. Algorithm to find Malevolent entities

The author[2] proposed an algorithm to find malevolent entities and to improve the security of the system efficiently. In e-commerce, finding malevolent entities is very important. In this paper author used distributed networks and dynamic algorithms in his implementation as centralized architectures are not that effective to provide security to the system because they have only one node that is the central node to calculate all the information so it takes a long time to execute and it is also cost-effective if that node fails then the whole network won't be working and it is also not that easy

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

to trust only one node whereas distributed networks will distribute the information to all the nodes equally as information is available to all the nodes this is a much trustable system.

Malevolent entities are the ones who give false information to the system and keep fake products and sell these products at unfair rates. There are two kinds of securities that are involved in e-commerce : hard security and soft security. Soft security provides trust to the system and hard security hides the information which is provided in the system with the help of cryptography algorithms. So, identifying malevolent entities is done by using soft security.

In a distributed network, the author[2] used a security graph. This graph is used to publish the information after verifying from all its neighbours. Here in the memory of each entity, the information of its neighbours is stored and for security, it will request to get information of its the neighbour entity through the network by using traversal algorithm and the results are accepted according to recommendations if it is in within threshold and with the help of directed weighted graph entities can have the track of entity network topology so it can pass their recommendations only to the trusted entities. With the help of this security graph, every node is included to identify the malevolent entities. A distributed network is very efficient to identify malevolent entities when they enter fake information. Hence, it provides good security.

The author[2] proposed a distributed algorithm to find the best seller or buyer and to find a secure product. This algorithm helps to give the best-secured products to the seller. This algorithm helps agents in calculating the security of the product, buyer, and seller by making recommendations and views from other entities. This is done in a distributed manner that provides a trusted and secured system. Updating the distributed network administrator plays an important role.

The author[2] used Java programming language to implement the proposed algorithm and he considered. Fluent NHibernate on SQL SERVER and web API is used to implement the database. He also evaluated the proposed algorithm by comparing it with other algorithms like genetic algorithms by considering the case study. In this case study, the author[2] considered the formula which is used in the stop and wait for an approach to calculate its efficiency. So, the author compared the accuracy percentage, optimization rate, execution time of the proposed algorithm, and genetic algorithm. With the help of these results, the author[2] concluded that the proposed algorithm is the best.

### C. Algorithm for Providing Authorization

The author[3] proposed a system that uses machine learning algorithms to analyze the integrity of the site. The proposed system helps in e-commerce transactions like payment gateways by providing authentication. For a secure payment system, it is much necessary to check if the websites are secured or not because attackers can hack the bank accounts with the database. There are many credit card frauds like skimming, forging signatures, hacking bank accounts…etc. To predict credit card fraud the author[3] mentioned three techniques which are Support Vector Machines ( SVM algorithm), Naive Bayes algorithm, and K- Nearest neighbour algorithm.

By using three machine learning algorithms the author[3] implemented a secured payment gateway which is a decision tree used in classification and regression problems it is a supervised machine learning algorithm it has two phases processing state and detection phase, artificial neural networks based on predictions it may be unsupervised and supervised ML algorithm and AES algorithm which is used to encrypt and decrypt the data. As there are multiple algorithms used in the system it provides the best security in financial transactions by which no fraud can take place. This system provides confidentiality, authentication, and integrity in the payment gateway.

### D. Algorithm for Providing Privacy

The author[4] proposed a model for encrypting the personal data which are acquired from e-commerce, to provide security and privacy for the personal data. As the count on the usage of e-commerce is increasing exponentially, due to this more and more amount of data is being produced, while considering the security issues by the governmental organizations and also the banking organizations personal data is being captured from the users of the e-commerce. To protect this personal data of the users many masking and anonymising techniques are been used and this Anonymised personal data which is been acquired in the name of analysis is been misused by using various corporations by using various methods such as disclosure analysis and also the e-commerce platform could retrieve the user's data very easily, such as for making a transaction on the e-commerce the personal info is required like the account number of the user's bank, the address of the user to deliver a product or mailing him a post, his e-mail id for acknowledgement of the transactions and tracking of the order and also much other personal data is been acquired on the e-commerce platform like sex, age etc which are based on the product the customer

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

ordered. Hence this personal data needs to be masked or encrypted to achieve privacy and security. In this paper, the author[4] analysed personal data usage in e-commerce and some methods which are used for securing personal data security on the database level. In section three of the paper, the homo-morphism safety interview model is explained where the customer service is prioritized by operating directly on the secret content by a mathematical transformation through a safe technique the customer's private information is transferred to it. In section four of this paper, the query algorithm is explained where the encryption is done on the master document and the query field is present for the establishment of the clear statement. The non-sensitive information is used for the query condition to reduce information to reveal. a query is required after all the secret content is decrypted for a customer.

In this paper the author[4] tried to apply the query algorithm on a test statistical data containing the details of customers and he assumed to mask the age of the customers and he applied this algorithm and the results were shown. for the encryption purpose he used the c=E(c)=(c+e*p)mode*q where the numbers p and q are the prime numbers where the homo-morphism is carried on with the c and for the decryption part D(c)=cmodp here the adverse transformation is done on the c's to the original value in the example shown in the paper the number 20 is encrypted to 12993550 which makes a huge difference and turns hard for the attacker to retrieve the data. Hence the huge amount of data which has been produced on the e-commerce platform needs to be secured and stored, to maintain the customer data confidentiality and also it doesn't turn into a source for attackers to perform illegal activities. Hence by using the model proposed by the author[4] in this paper the information which is to be considered as a piece of private information for the customers or the information which could be an advantage for the hackers, can be securely maintained on the databases by encrypting them.

### E. Algorithm for certifying Software

The author[5] tried to propose an algorithm to certify the software used for e-commerce purposes. The corporate home living and the board rooms have been taken hold by the web and internet communication purposes used for e-commerce. As internet growth took place its applications like e-commerce also took place in a wide range which made it easy for an expansion of business and also for marketing purposes. Due to this, the demand for security is increasing because a large amount of data that is sensitive or confidential is exchanged and a leak of this sensitive information could lead to a major loss to a business. Though there are many protocols such as the S_HTTP, S/MIME, secure socket layer etc they are restricted only for the transaction level security but the attacks near the user level. For proper security and maturity for the entire process in e-commerce, secure software needs to be developed while building the commerce applications. Certification is a process where the software is analysed to determine whether the risks are on an acceptable scale or not. This type of certification can also be used on the business side, where for a given application the vendors get third-party approval for using the vendor's software. And the workers could also get certified on the platform for process generation and also work on the hardware and software platforms in companies. This process of certification is required for assuring and providing a productive and high-quality service to the end-users or the customers. The author[5] in this paper provided an algorithm to perform the analysis and for checking whether any security policy is violated and finally, the certificate is issued or else the software which is sent for the analysis is denied. In this algorithm various analysis techniques are applied and are represented by the notation "Ai" and each portion of the analysis (ECi) exists and proves that the analysis is passed and can be sent to the next step, An if condition is used whether this particular software is following all the security policies and then finally the software is sent to the if condition with an and operator so that all the "ECi" are set to true. Until the software has gained the acceptable range and the confidence for risk-free it's not been certified. A set of analyses that have been performed during the certification process and the security policies that software needs to follow are defined by the software template. The software security policies follow on the assurances the software follows like its resistance to DOS attacks, robustness, no malicious logic on the program code of the project etc. most of the security breaches all around the world are because of no assurance of certification on the software used and also the flaws in that particular software. and the other major problem is due to malicious software or codes which have been added to the software so that the system privileges are exploited. the public based software is turning into a commonplace for most of the cyber attacks like hijacking the software distributions with the help of trap doors, trojan horses etc.

The dynamic analysis is used to check the security policies and the vulnerability for the occurrence of the risks on software and this has been concluded from the statistical analysis which is used to reduce the cause of the problem. In the

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

certification process, the functionality of the program is not checked but the vulnerability to the risks is only checked. Hence in this paper, the author[5] has proposed an algorithm for certifying the software which is based on the applications of e-commerce to provide security, so that the security is provided before that soft is deployed and made use to the end-users where it software goes through various assurance rounds and finally they are been certified.

**F. Algorithm for Providing Trust**

The author[6] has proposed a trust model by using the fuzzy theory for e-commerce. As the transactions made on the network entities mostly get restricted due to trust issues in e-commerce, the trust of the dealer (seller)entities has turned into a serious problem for businesses. By having the base on the fuzzy theory a design and trust model the algorithm of the author[6] is designed. With the growth of the internet the usage of its applications like e-commerce has also increased over the past decade and due to this the transactions which are made on the internet platform has also increased and a huge amount of personal and bank related information is shared in these transactions. And also there is an uncertainty that the trust needs to be made between the two parties where there are chances that they can fake their identity and due to this it is difficult to ensure an interaction that they are honest and trustworthy. Though many cryptographic algorithms could provide trust, there are problems for ensuring trust between the two entities. In section 2 of this paper, the author[6] has explained the trust model which is based on the security policies and credentials of the secure key operations and also the other model which used the fuzzy protocol based method which could measure the metric and the trust system which uses the encryption system to ensure privacy.

In the third section of this paper, the author[6] has explained his proposed model FBTEM, the author has included modules such as the Entity information collection module where it gathers the feedback of the transactions along with the information which is been registered and if there are any malicious behaviour which are further been forwarded to the analysis module, the entity information analysis module where it checks whether a new entity is added in the network and through the analysis it classifies the information, Trust evaluation and algorithm module where it is considered as a core module of FBTEM where it contains an algorithm of trust and the fuzzy comprehensive evaluation. The trust algorithm has comprehensive, initial, update, punishment trust modules. Various sets such as entity trust evaluation, evaluation level test etc are used in this algorithm. The fuzziness is the only true relationship between the transaction entities, due to this various levels are made from A1 to A5 which is based on the ladder-type membership function. The initial truth value is always set to zero. Some of the factors which affect the trust are certification, security services. In the second step, the trust model needs to be updated so when a trade happens between the two entities we can get the trust value where the buyer evaluates the seller which is called update trust. In punishment trash when two entities are having a mutual transaction, and if the transaction fails then it means it's having malicious behaviour, so the malicious entities are punished. In section 4 of this paper, the author[6] performed a comprehensive evaluation by considering two entities A and B with two different fuzzy sets. and a small transaction is conducted assuming that trust has been established with a level 0.2and for this situation he used the FBTEM evaluation model. Hence by using the author[6] model the fuzziness between the entities on e-commerce is reduced, and also the algorithm has enhanced the experiments which are conducted by the author to show that it can upstand the malicious behaviour more effectively.

**G. Algorithm for C-2-C E-commerce**

The author[7] analyzed the credit evaluation system for C2C e-commerce and about issues in it and then implemented the best credit evaluation model by proposing a new algorithm. By using synthetic data this system is validated.C2C electronic commerce websites provide a credit evaluation system for safe transactions. It is very useful for the development of electronic commerce.

The author[7] mentioned the functions of the credit evaluation system in which the transaction that is conducted between two parties verifies each other after validating the information the user's credit is conveyed. This system provides trust which makes transactions insecure.

The author redesigned the credit rating scale and updating scales to avoid drawbacks of the old credit evaluation system like old credit evaluation system has a 3-point rating scale ( negative, positive and neutral) corresponding to -1,+1,0 respectively which are not distinguished much, it considers only the number of transaction and not the amount and there will be no update in feedback for latest transactions. The model which the author[7] proposed has considered the number of transactions along with the number of transactions and feedback is also upgraded for the latest transactions. This model has a 5-point rating scale (bad, poor, neutral, good, very good) corresponding to -2,-1,0,1,2 respectively to have a good difference which can give the best feedback.

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

To improve the credit-evaluation model the author[7] used a new weighted rating algorithm. In transactions, the rating of feedback is weighted; this gives feedback importance. The algorithm has three parts. In the 1st part the credit weight is calculated with the help of the provider's credit so that the feedback is more trustable if credit weight is higher which has more providers credit. In the second part, the amount-weight is calculated with the help of the number of transactions here. The feedback is very important if the amount-weight is more which has more transactions. In the third part weighted score of feedback is calculated by calculating the average weight of occurred feedback. The author[7] proposed a new credit updating algorithm for better evaluation-receiver improvement and by considering a case study the author validated his proposed improved credit evaluation model.

**H. JS-Security Algorithm for transaction Security**

The author[8] proposed a secure payment system by considering the rules of SET protocol. Encryption algorithms are used to provide good security to payment systems. The proposed algorithm by the author gives a larger length of ciphertext without increasing the executing time and throughput compared to traditional algorithms. The algorithm used is the Jumbling Salting encryption algorithm.

Many protocols and encryption algorithms are used to have security in the transaction between payer and payee. Cryptography plays an important role to maintain security. The Jumbling Salting encryption algorithm (JS algorithm) used by the author[8] is a symmetric algorithm that uses a single key that is kept secret between sender and receiver.

In online transactions, the payment gateway is necessary for secured transactions. The author[8] mentioned the protocols used in payment gateway and their limitations. The mentioned protocols are SET and MSET protocols which stand for the secured electronic transaction and modified secure electronic transactions. Digital signature and digital certificates are used in the SET protocol to give security in payments. The limitations of the SET protocol are its performance is slow and adaption of the SET protocol is not easy and the modified set that is MSET is also similar to SET improvements are not made much.

JS algorithms contain two-block jumbling and salting blocks and a jumbling block contains three more blocks: addition block, selection block and reverse block. These three blocks of jumbling block have three functions which and by adding salt block helps to provide more security and then cypher text is obtained this obtained ciphertext is encrypted one more time to give strong security. The author[8] used python language for implementing the JS algorithm and proposed a JSSecure payment gateway by using the JS algorithm. And also used the client system, merchant system and bank's server to propose the model.The main focus of the author[8] is on throughput in encryption and decryption, encryption time, decryption time and length of the ciphertext. The size of ciphertext is more compared to plain text this gives more security by making attackers tough to attack the data. And encryption time, decryption and throughput are also limited.

**I. For detecting phishing websites**

The author[9] created various machine learning models to detect whether the website is legitimate or not and performed it on the dataset from the UCI machine learning repository. The algorithms used are logistic model tree, naive Bayes, J48 and random forest and the author compared the accuracy of these algorithms by using the data mining tool WEKA. After looking at the results we can tell the random forest algorithm is best with an accuracy of 89.87%. For predicting whether the website performs phishing attacks or not, a random forest algorithm is used on any e-commerce website before making payment.

**J. For detecting online credit/debit card transaction fraud**

The author[10] developed integrated online shopping for the user. First, the user needs to register with their fingerprints for security purposes and the one-way hash function is applied to these fingerprints then unique hash code value is generated and stored in the database, next few security questions should be answered by the user and these are stored in the database while shopping check out these security questions will be asked for verification, then for authentication, there is an OTP verification. At last, the large amount of data from this real database which is developed by the author is used for detecting the fraud and the Support vector machine model is used to improve the accuracy of fraud detection. If the transaction is fraud then the user gets a notification through email else the transaction is completed and is stored in the database.

**K. Multi-Agent System**

The author[11] designed a blockchain-based multi-agent electronic commerce system that uses a consensus algorithm and dual SHA256 where the RSA algorithm is combined with a hash function to provide security, authentication, riskless, safe, reliable, and tamper-proof system. The author[18] verified the proposed system which resulted in

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

secured e-commerce. There are also few security issues in blockchain to avoid this the RAFT consensus algorithm was used which contains the mechanism of message signature verification and uses the non-Byzantine algorithm. The smart contracts are used with the help of blockchain by which there won't be any third party involvement; this gives a tamper-proof system. The smart contracts are sent to products and after verifying it the product is shipped.

The blockchain is a decentralized network that makes it nearly impossible to change or manipulate the data. By this, the blockchain assures us to overcome issues like tampering, security, and privacy. Blockchain is an immutable chain so that no one can alter the data and this provides integrity. Blockchain has high availability as it is decentralized as it has consensus it is highly verifiable. The distributed consensus protocol like Pos, Pow, distributed algorithms and Dpos helps in identifying who can add new transactions to the ledger. Cryptography plays an important role to achieve security in blockchain.

**Table1.1**

| S.No | Authors | Year | Title of the paper | Proposed Method |
|---|---|---|---|---|
| 1 | S. Raghuwanshi, R. K. Pateria, and R. P. Singh | 2009 | A new protocol model for verification of payment order information integrity in online E payment system | Algorithm for providing integrity |
| 2 | F. Fouladfar | 2016 | Proposing a distributed algorithm to finding malevolent entities and improving security in e-commerce environments | Algorithm to find Malevolent entities |
| 3 | S. J. Pon, S. S. Ramya, A. V. Christal, and K. Mythili | 2020 | Secured payment gateway for authorizing E-commerce websites and transactions using Machine Learning Algorithm | Algorithm for providing authorisation |
| 4 | C. Yin, R. Sun, and S. Xue | 2009 | A modified query algorithm for private data security facing E-commerce | Algorithm for providing privacy |
| 5 | A. K. Ghosh | 1999 | Certifying E-commerce software for security | Algorithm for certifying software |
| 6 | Y. Han and W. Jiang | 2012 | Trust evaluation model and algorithm based on fuzzy theory for e-commerce | Algorithm for providing trust |
| 7 | P. Chunhui, A. Jing, and F. Meiqi | 2007 | Study on credit evaluation model and algorithm for C2C E-commerce | Algorithm for C2C E-Commerce |
| 8 | M. Neelansh Prasad, M. Ramakrishna Oruganti, M. Saurabh Shah, M. Yohan Pavri, and P. Churi | 2018 | Improvised E-commerce Transaction Security using JSSecure Algorithm | JS-Security algorithm for transaction security |
| 9 | Latif, R. M. A., Umer, M., Tariq, T., Farhan, M., Rizwan, O., & Ali, G | 2019 | A smart methodology for analyzing secure e-banking and e-commerce websites. | Algorithm for detecting phishing websites |
| 10 | Mary, I. M., & Priyadharsini, M. | 2021 | Online Transaction Fraud Detection System | Algorithm for detecting online credit/debit card transaction fraud |
| 11 | H. Xu, X. H. Shi, and D. Yi | 2018 | Multi-Agent System for E-commerce Security Transaction with Block Chain Technology | Multi agent system |

## 3. CONCLUSION

In this paper, we have reviewed some of the e-commerce security algorithms and have studied various methods for securing the transaction data and the user data. As e-commerce is growing over the past decade and is been expected to have a high rate of growth in the future more and more amount of data that is personal and also confidential is been deployed into this platform and this data needs to be

SJIF Impact Factor 2021: 8.013| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 6 | Issue: 11 | November 2021 - Peer Reviewed Journal

handled properly in a secure manner because it has turned into a hot-spot for many of the attackers, where the data can be used for their benefits which could lead to a huge loss for the users hence a proper security need to be provided to secure this information.

## REFRENCES

1. *S. Raghuwanshi, R. K. Pateria, and R. P. Singh, "A new protocol model for verification of payment order information integrity in online E payment system," 2009 World Congr. Nat. Biol. Inspired Comput. NABIC 2009 - Proc., pp. 1665–1668, 2009, doi: 10.1109/NABIC.2009.5393641.*
2. *F. Fouladfar, "Proposing a distributed algorithm to finding malevolent entities and improving security in e-commerce environments," 10th Int. Conf. e-Commerce Dev. Ctries. With Focus e-Tourism, ECDC 2016, pp. 1–6, 2016, doi: 10.1109/ECDC.2016.7492977.*
3. *S. J. Pon, S. S. Ramya, A. V. Christal, and K. Mythili, "Secured payment gateway for authorizing E-commerce websites and transactions using Machine Learning Algorithm," 2020 Int. Conf. Comput. Commun. Informatics, ICCCI 2020, pp. 20–24, 2020, doi: 10.1109/ICCCI48352.2020.9104140.*
4. *C. Yin, R. Sun, and S. Xue, "A modified query algorithm for private data security facing E-commerce," Proc. 2009 Pacific-Asia Conf. Circuits, Commun. Syst. PACCS 2009, pp. 585–587, 2009, doi: 10.1109/PACCS.2009.47.*
5. *A. K. Ghosh, "Certifying E-commerce software for security," Proc. - Int. Work. Adv. Issues E-Commerce Web-Based Inf. Syst. WECWIS 1999, pp. 64–67, 1999, doi: 10.1109/WECWIS.1999.788187.*
6. *Y. Han and W. Jiang, "Trust evaluation model and algorithm based on fuzzy theory for e-commerce," Proc. - 2012 4th Int. Conf. Multimed. Secur. MINES 2012, pp. 95–98, 2012, doi: 10.1109/MINES.2012.243.*
7. *P. Chunhui, A. Jing, and F. Meiqi, "Study on credit evaluation model and algorithm for C2C E-commerce," Proc. - ICEBE 2007 IEEE Int. Conf. E-bus. Eng. - Work. SOAIC 2007; SOSE 2007; SOKM 2007, pp. 392–395, 2007, doi: 10.1109/ICEBE.2007.77.*
8. *M. Neelansh Prasad, M. Ramakrishna Oruganti, M. Saurabh Shah, M. Yohan Pavri, and P. Churi, "Improvised E-commerce Transaction Security using JSSecure Algorithm," 2018 IEEE Int. Conf. Syst. Comput. Autom. Networking, ICSCA 2018, 2018, doi: 10.1109/ICSCAN.2018.8541188.*
9. *Latif, R. M. A., Umer, M., Tariq, T., Farhan, M., Rizwan, O., & Ali, G. (2019, January). A smart methodology for analyzing secure e-banking and e-commerce websites. In 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST) (pp. 589-596). IEEE.*
10. *Mary, I. M., & Priyadharsini, M. (2021, March). Online Transaction Fraud Detection System. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 14-16). IEEE.*
11. *H. Xu, X. H. Shi, and D. Yi, "Multi-Agent System for E-commerce Security Transaction with Block Chain Technology," 2018 Int. Symp. Sens. Instrum. IoT Era, ISSI 2018, vol. 123, pp. 1–6, 2018, doi: 10.1109/ISSI.2018.8538253.*