Trinity University, Lagos, Nigeria
Harmarth Global Educational Services
FAIR Forward – Artificial Intelligence for All
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
Society for Multidisciplinary & Advanced Research Techniques (SMART)

32nd Accra Multidisciplinary Cross-Border Conference (AMCBC)

Eavesdropping Attack Prevention In E-Auction System Using Distributed Ledger Technology.

Ahubele, B.O. & Obahiagbon, K.
Department of Computer Science, University of Port-Harcourt, Rivers State, Nigeria
Department of Physical Sciences, Benson Idahosa University, Benin City, Nigeria.
E-mails: betty_ahubele@uniport.edu.ng, kobahiagbon@biu.edu.ng
Phone: +2348087473122; +2348131130870

ABSTRACT

Online auction is the most recent crazes on the internet where people can either offer junk, antiques or collects item for sale to anyone who is interested in bidding on them. People who do not have money or intention of buying an item for auction can indulge in fraudulent bids as well as clone artists selling their own fraudulent items. Despite the advantages of e-auction in e-commerce infrastructure, several in-auction threats and attacks may emerge which requires evolving technology such as blockchain-based cryptographic mechanism for end-to-end buyer-to-sellers verifiability in ensuring an attack free e-auction process. The biggest challenges with eavesdropping attacks is that they are very difficult to detect but preventive measures must be in place to keep the network safe from snoopers or sniffers. Amidst all, we proposed a model for combating eavesdropping attack between buyer and seller in an unsecure communication channel using the distributed ledger technology. The main aim of this research is to discuss emerging e-auction system using distributed technology and mitigation procedure in ensuring the CIA Triad (Confidentiality, Integrity and Availability) when transacting in e-commerce.

Keywords: E-auction, Distributed Ledger, Blockchain, Eavesdropping attack, Bidding, Digital Signature

Proceedings Citation Format
Ahubele, B.O. & Obahiagbon, K. (2022): Eavesdropping Attack Prevention In E-Auction System Using Distributed Ledger Technology. Proceedings of the 32nd Accra Multidisciplinary Cross-Border Conference. University of Ghana/Academic City University College, Ghana. 2th June-1st July, 2022. Pp 51-62
www.isteams.net/ghanabespoke2022.
dx.doi.org/10.22624/AIMS-/AMCBC2022P6

1. INTRODUCTION.

Recent technological advancements have brought a lot of transformation in e-commerce activities by providing an elaborate platform for customers and users to carry out their business transactions remotely and conveniently. One of the major pervasive transformations in e-commerce is the adoption of online auction system where users can purchase products online while increasing profits in a few years. E-Auction is an efficient e-commerce system which enable buyers and sellers to engage in online transactions through various e-platforms [7]. The distributed ledger technology through the implementation of smart contracts provides an online auction for secured, transparent and decentralized transactions. Various auction sites such as eBay, Amazon, eCrater and Copart have exhibited large profits for online auction systems. According to [1], eCrater exists as one of the easiest auction website with good quality that offers sales without exerting force on customers to register on the website. They showcase their products and provide steps that aid user in bidding to the end of the purchase once interest is indicated.

In online auction, exchange of products is done using various auction format such as English, Dutch, First-price Sealed Bid and second price sealed bid etc. Bidders in this market places faces the challenges of getting the best bidding strategies to win the auction, decision on which auction to participate in, when to bid (early or late), how much to bid etc. The need for automation in bidding becomes necessary to assist buyers with analyzing, selecting, making bids and monitoring development with the bidding. Besides online auction gaining immense popularity for fair exchange of goods and growing numbers of online vendors and buyers, it is also facing the challenge of fraud, since sellers and buyers alike can participate for their own benefit in auction fraud [3].

Online auction is more prone to fraud as large amount of money is being traded daily. In-auction frauds (like shill bidding and bid shielding) are most prominent due to its difficulty in detection with no apparent evidence of fraudulent act. Although, the emergence of decentralized-smart contract technology exists to revolutionizes the conventional e-auction system. It paved way for an immutable, transparent, auditable and secured e-auction process with better security. This paper proposed a framework with blockchain cryptographic technique for an efficient and secure in-auction bidding system.

1.1 Types of E-Auction System

Online auction system is gaining popularity daily due to its ease of bidding, selling or buying of products and services. It afford users the uninterrupted opportunity to utilize the web and register for e-commerce transactions.

In [20] e-auction is broadly classified into different categories:

a) English Auction: This is also called forward auction where the bids are thrown in ascending order i.e. the lowest bid price is mentioned at first and then the bid amount increases till the highest bid where no other person can bid beyond that price and the product is sold at that highest price.

b) Dutch auctions: unlike the forward auctions where the bids are thrown in descending order starting with the highest price, then the price is systematically lowered until a buyer accepts the last reduced price and won the bid.
c) First-price sealed-bid: This describes scenario where a single bid is classified as all bidding parties and the single highest bidder wins, and pays what they bid. The main difference between this and English auctions is that bids are not open to the public.
d) Vickrey auction: Also called the second-price sealed-bid auction with similar operations as the first-price sealed bid. Although, the winner which is the highest bidder and winner will only pay what the second highest bidder had bidded [21].
e) Reverse auction: In this type of e-auction bid, the roles of buyer and seller are interchanged. While multiple sellers compete to obtain the buyer's business, the prices decrease over time as new offers are made. The typical auction format where the buyer can see all the offers and may choose which they would prefer is not considered.

2. RELATED LITERATURES.

Recently, many researchers have focused on the need for integrating blockchain in diverse industries such as healthcare, education, supply chain, e-voting, e-governance and e-auction to provide enhanced security, integrity and authentication of products during and after bidding. Previous researches in distributed ledger technology had created an elaborate platform for secure and transparent business processes with immense benefits [6]. The research by [22], proposed a formal verification model for security vulnerability in non-fungible tokens. The study was able to implement a smart contract model to eliminate any vulnerability for any threat or launch of an attack on non-fungible tokens. The authors [22] also discussed the unique transformation of the distributed ledger technology in the area on non-fungibility.

In [4] a protocol for running sealed-bid auctions on Ethereum decentralized platform was presented. This protocol provided features such as verifiability, privacy of bids and fairness to the e-auction system. In another study by [13], the authors described a prototype for secure blockchain-based e-auction system that could lower the uncertainties of far-distance complex trade in an online auction system. The study also demonstrated the important security requirements using smart contract. The implemented smart contract encoded information such as auctioneer data, start time, current winner data, current highest price and time-limit of auction. Although, the study further discussed the security issues of the proposed smart auction but failed to implement the possibility for coalition large bidders. This could result in big discrepancies among the offers. The study intended to implemented fuzzy approximation function while the bidding phase is running in order to provide advanced security level.

Similarly, the research carried out in [14], presented a novel electronic english auction system using symmetric encryption and Elliptic Curve Cryptography (ECC) operations. The proposed model provided an improved and secured e-auction system as well as reduces the cost. The study was able to fulfill the verifiability of all messages published on the agent centre and utilized BAN logic to prove mutual authentication of their protocol. Besides, their protocols implemented more security properties, which makes it more efficient for implementation in comparison with recent works in same domain.

A further research in [12] was able to describe how interaction in a company can be improved using digital signature technology. The authors modeled the AS-IS and TO-BE process of business process for analysis and implementation. According to the study, the general requirements for the digital signature, the possibility of introducing the module into existing e-document management system and the necessity of implementing the technology were considered. Alternatively, [15] introduced a novel and secured e-auction management system using group cryptography and remote supervision. The authors discussed the advantages and exploitation of online auctioning system by both buyers and sellers. The issues and challenges involved in maintaining security of e-auctioning system were analyzed. The improved model security was controlled through group communication based on public key infrastructure (PKI) but could not implement protocols for detecting malicious entries in the system and preventing frauds in e-auctioning system.

In the same vein, [17] presented a 'Hawk' framework for creating a smart-contract on the ethereum ledger platform. Although 'Hawk' was modeled to utilize a zero knowledge proof (ZKP) to prove the honesty of the manager but it took a long time to produce the proof and deploying the ZKP in a smart contract was seen to be complex. Another study in [18] demonstrated that bidder's privacy in a decentralized-based e-auction protocol remains a huge challenge since every single transaction within the blockchain system is made public which can be inspected and analyzed to reveal real identities. In a nut shell, this paper presented a distributed platform using smart codes for prevention of eavesdropping attack using digital signature algorithm with hash functions and public key cryptography to enhance the bidders' privacy in an online auction.

2.1 E-Auction and Distributed Ledger Technology

With the advent of the transformative technology called blockchain, new e-auction schemes have been proposed with smart contract implementation to provide more coherent, fair, open, transparent, tamper-proof, high-trust, traceable and secure bidding platform for buyers. The distributed ledger technology in collaboration with Cryptographic mechanism helps to create contract codes for encryption and storage of bidding information on the chain in order to ensure assurance in the integrity of online bidding information. Several permissioned and permissionless distributed platforms for e-auction implementation exist. Ethereum blockchain is a major permissionless smart contract platform proposed by Vitalics Buterin in 2014 for decentralized applications other than financial transaction without a middle trust-based party. Similarly, a study by [4] presented a verifiable sealed-bid auction on the ethereum platform for the bidders to submit homomorphic commitments to their sealed-bids on the contract. The bidders utilized a public key cryptographic scheme to reveal their commitments secretly to the auctioneer without the attacker having a knowledge of the information communicated.

The study in [4] also provided an interactive zero-knowledge proof attributes such as bid privacy, posterior privacy, public verifiable, correctness, financial fairness and non-interactivity using a set of cryptographic primitives. Consequently, the rapid growth of e-auction promotes work efficiency but incur some new and distinctive limitations such as data privacy, low-robustness and lack of trust. To tackle the above limitations, researchers have proposed various auction designs in various academic and industrial sources. However, most of these designs failed in achieving decentralization, bids privacy, secure communication, free and collision resistance.

Consequently, in [5] an effective smart contract platform was designed using blockchain technology to implement a verifiable privacy-preserving sealed-bid reverse auction scheme. The study also provided a robust and privacy protection of losing bids even in the face of overwhelming collusion, without the need for trusted third parties. In Figure 1, a typical blockchain distributed ledger system was described showing how various transactions are linked with their cryptographic hashes and private keys.

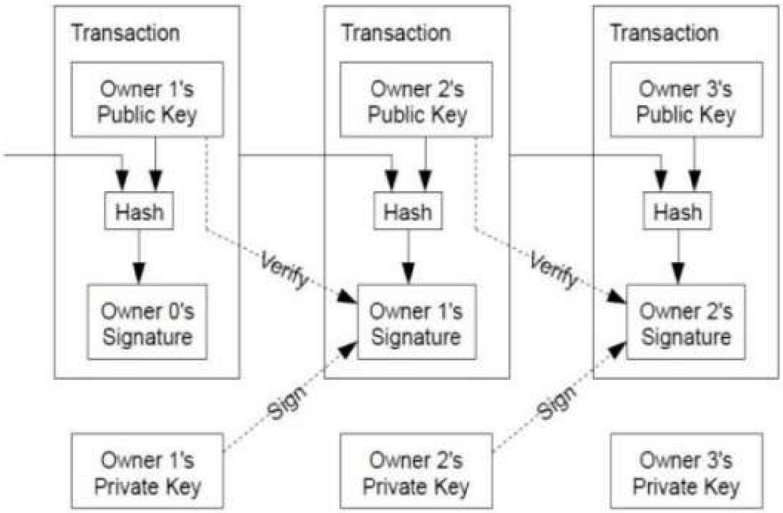

Figure 1: Blockchain Technology [6]

2.2 In-Auction Attacks

As the world continue to experience new technological innovations with evolving technologies, the number of sellers and buyers attracted by e-auction kept increasing in a spontaneous fashion, creating enormous challenges in the e-commerce domain. E-auction fraud has become prevalent, depriving participants in trusting the online platform for successful e-commerce transactions [16]. As a result, sellers and buyers can expound the online auction perpetrating different fraudulent activities for their own benefits.

E-auction fraud can occur in diverse ways, thus; Product misrepresentation for sale, refusal to deliver merchandise or services sold, triangulation which entails eavesdropper purchase items using a stolen credit card, sales of items to uninitiated buyers, thereby retaining the cash and transferring the risk of seizure to the end recipient; fee stacking i.e charging extra money after an auction is over; selling black market goods, multiple bidding (buyers inflate prices using aliases, which frustrates competitors, then at the last moment the high bids are withdrawn to secure a low bid), and finally shill bidding (a situation where sellers or their associates place bids on their own auctions to perpetuate fraud). In-auction frauds are categorized into shill bidding, bill shielding, false bidding, multiple bidding etc.

Besides frauds prevalent in online auction, possible attacks include wormhole, Denial-of-Service (DoS), eavesdropping etc. Eavesdropping occurs when there are weak connections between seller and buyers, outdated devices or software, malware etc. Hackers intercept data packets traversing the network by exploiting these weak connections in an online auction system. In this paper, we expound the eavesdropping attack as a major attack possible on an e-auction system. Eavesdropping or sniffing attack is described as an unauthorized and illegal interception of a private communication [9]. These attacks are difficult to detect because they utilized an unsecured network communication to access data with no evidence to prove that it has occurred. For instance, a bidder sending his/her bid to the seller, an attacker can quietly introduce and place some software through which he can eavesdrop in the network and capture all the relevant information.

2.3 Eavesdropping Attacks

Eavesdropping involves listening in on conversations across components such as platforms, servers, mobile phones, computers and connected devices for possible interruption or launch an adversary. Hackers could look for weak connections, install sniffer programs or launch illegitimate apps to monitor distributed communication in a distributed platform [21]. Eavesdropping attacks could be passive or active. In passive attacks such as VoIP (Voice over IP), a hacker may use a compromised VoIP device such as switch, cable or internet to infiltrate the network. This type of attack may be impossible to detect and prevent as they do not cause any disruption or manipulations. On the other hand, active attack occur when hackers masquerade themselves in the e-auction network as legitimate sellers/bidders.

They can inject, modify or hijack packets data and interfere in the bidding process. With the blockchain-based e-auction system, the man-in-the-middle may be a malicious miner whose intent is to validate and verify blocks of information to his credit in launching an attack. The malicious miner may validate a malicious hacker as the legitimate seller, they could attempt group attack and utilize the buyer's information, steal the bidder's credit card and perpetrate threat. A secure communication could be implemented by encrypting bidder's details and ensuring all conversations are digitally signed for non-repudiation and confidentiality. Blockchain cryptographic mechanisms with digital signature algorithms could be implemented as a potential counter measure against eavesdropping attack in the distributed-based e-auction platform.

3. METHODOLOGY.

Digital signatures have been in use for quite a while to authenticate various e-commerce transactions. The digital signature is a cryptographic scheme used to authenticate a message and identify the sender of the message, thereby preserving the integrity and avoiding non-repudiation. Today, the processes of creating and verifying a digital signature provide a high level of assurance to the involved parties that the e-signature is genuinely the signer's and that the electronic document is not manipulated [11]. This system utilized Digital Signature for encrypting buyer's information against in-auction electronic fraud. In an e-auction system, the bidder places his bid on a particular product displayed by the seller. The possibility of seller-buyer communication theft by a fraudulent hacker could be detected.

The hacker may have installed on the communication line or connected a device to the communication between the seller and the buyer. The fraudulent eavesdropper can also use the information he/she was able to access over the conversation to impose as a genuine bidder and places a bid as well, while also presenting fake credit card to another bidder for payment. Attacks are prominent in online auction as a result of prevailing technologies despite efforts by researchers to curb possible in-auction fraudulent activities.

The study demonstrated by [19] revealed the feasibility of data integrity and authenticity by employing the concept of Digital Signature. Digital signature is a public key infrastructure (PKI) that ensures the integrity and authenticity of a message. A hash function is applied to the message to be signed, in order to yield a hash code of fixed length. The sender's private key is used to encrypt the hash code to form a signature. Finally, the signature and the message are encrypted and transmitted. The receiver gets the message and decrypt with the sender's public key. The receiver also generates a hash code from the message received. However, if the calculated hash code matches the decrypted signature, the signature is said to be valid.

This is possible because only the sender knows the private key, and thus only the sender could have produced a valid signature. In Figure 2, the study reveal how the digital signature works. In a simple e-auction system, a digital signature is formed by encrypting the entire message or the hash code of the message with the buyer or bidder's private key. Confidentiality can be provided by further encrypting the entire message plus signature with either the seller's public key encryption or the shared secret key, which is also conventional encryption.

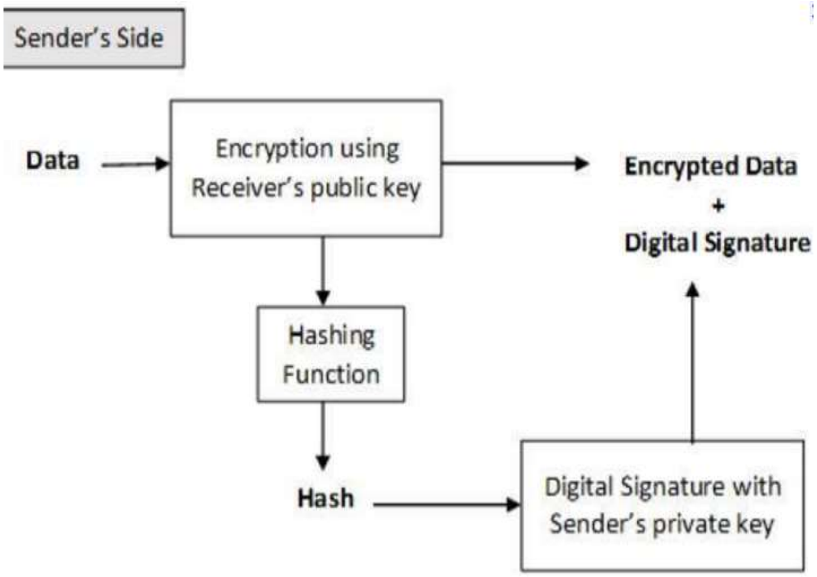
Sender's Side
Data
Encryption using Receiver's public key
Encrypted Data + Digital Signature
Hashing Function
Hash
Digital Signature with Sender's private key

Figure 2: How Digital Signature Works.

A. The Proposed System

The proposed system is based on blockchain cryptography using hash function and digital signature. The system provides support for a secured communication between auctioneer/bidder and seller in an online auction system against eavesdropping attack. In this paper, we presented a blockchain-based hash function and digital signature algorithm to provide data integrity and authentication in the e-auction communication channel between bidders and sellers. This is relevant to avoid tampering, digital modification and forgery during information transmission in the bidding process.

Hash function converts arbitrary length of input string to a fixed output string. The output is irreversible, which means it cannot yield same result as the input string. Digital Signature is a public key cryptography which can also be called 'virtual fingerprint'. The digital signature is created using DSA (Digital Signature Algorithm) or RSA (Rivest Shamir Adleman). Then we encrypt the signature using the private key and decrypted using the public key. Decoding with public key verifies signature provenance since it was encrypted with its corresponding private key. The encrypted hash together with the hashing algorithm forms the digital signature.

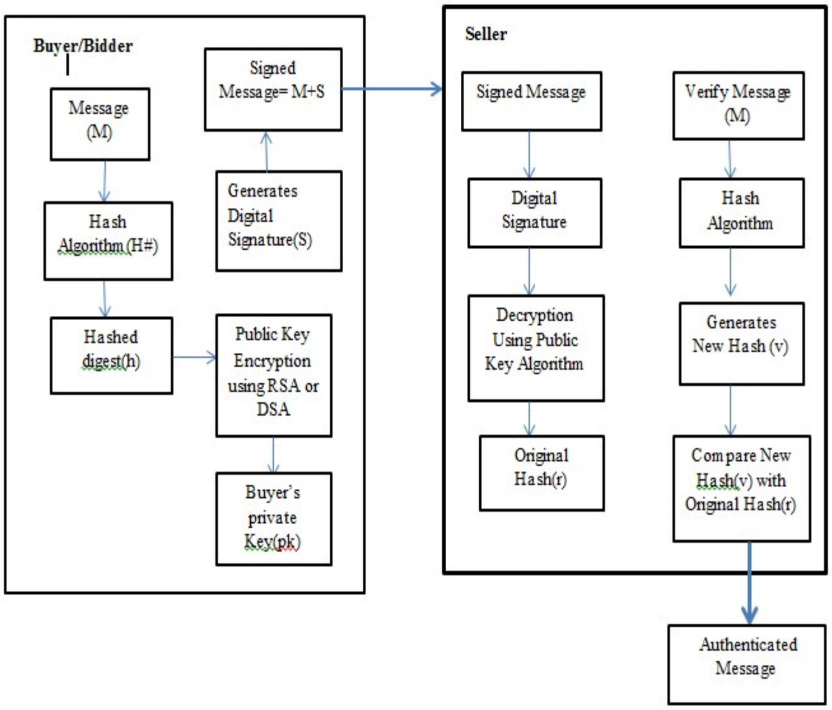

Figure 3: Block diagram of e-auction system using Digital Signature

B. The Proposed System Architecture

The proposed blockchain-based e-auction platform is made up of three phases: The registration phase of the bidder, bidding phase and the winner's phase. The aforementioned e-auction phases are analyzed below:

1. Bidder's Registration Phase

Bidder U_i (1≤ i ≤m) secretly sends (ID_i, y_i) to all the RM_j 's (1≤ j ≤n) for the registration. Upon receiving the registration request, each RM_j chooses a random integer k_{ij} such that gcd(k_{ij} , q)=1, where p and q are large prime numbers, and another random integer RN_{ij} for each U_i, and computes the certificate for the bidder as follows:

$r_{ij} = yi \times k_{ij} - x_{RM} \bmod q,$
$s_{ij} = yi^{kij} \bmod p$

2. Bidding Phase

Assuming the bidder U_i, with identity ID_i wants to participate in the online auction, then he/she will send his/her random number RN_i and identify the goods kept for auction as specified by the seller.

3. Winner's Identification Phase

After the bidding process, the AM, IM and RM will cooperate to find and publish the identity of the winner.

C. Digital Signature Algorithms

The proposed system utilized the digital signature algorithms as stated below:

i. Key Generation Algorithm: utilizes the concept of modular exponentiation for private and public keys (x,y) generation such that 0<x<q and y =gx mod p such that keys Pri, Pub(x,y) = private key pairs (p,q,g,x); Public key pairs (p,q,g,y).

ii. Signature Generation Algorithm: This entails a hashing algorithm which generates a message digest as an input to create two-variable outputs (r,s). Then select a random integer (k) such that 0<k<q. Calculate r given r=(gk mod p) mod q. To calculate the output variable, s, given s=[k-1(h+x .R) mod q]. Receiver gets (M,r,s) as the signatures where M is the plaintext.

iii. Signature Verification Algorithm: Here, the hashing function is used to output the digest and incorporates variable, s, with other parameters to produce verification output of v.

The verification algorithm, thus:

a. Input digest(h) with hash function(H#)
b. create digest(h) through (Ver.func), v
c. calculate w, given s*w mod q=1
d. calculate u_1 from u_1=h*w mod q
e. calculate u_2; u_2=r*w mod q
f. compute ver.output, v, given v=[((gu1 . yu2) mod p) mod q]
g. The Value v is compared with the generated value, r
h. Sig(Ver) is complete if matches obtained.

D. Advantages of the Proposed System

The advantages derivable from the proposed design are listed below:

i. it protects the integrity of information sent and received between bidder and seller and ensure that the information has not been modified in any capacity at any stage of communication.

ii it verifies the identity of the people involved in the e-auction transactions, such a way that bidders as well as sellers can confirm that the other is indeed who he/she claims to be.

iii sellers need to get signatures of the bidders on these products to ensure that the bidders agrees and comply with the products terms and conditions, bidding agreements etc.

The proposed system is a digital signature scheme that ensures the information between seller and bidder is kept private and confidential. Hence, the bidding data is only available for view to the relevant people involved in the online auction transaction.

4. CONCLUSION.

Online auction is becoming a popular domain in electronic commerce and hence the system must increase its quality and security. Security and trust in e-commerce can be achieved by providing authentication, non-repudiation and confidentiality of transactions. Techniques such as public key cryptography could be implemented to achieve an efficient e-auction system. Our proposed model utilizes a digital signature algorithm (DSA) for a secure communication between seller and buyer when transacting online.

The buyer’s/bidder’s information is encrypted with its private key, both the message digest is signed and sent on the blockchain. The seller decrypts the digitally signed message with its corresponding public key. However, both the sellers and buyers details are validated and recorded on the blockchain. The DSA is available for generating, updating, recovering, signing and verifying e-commerce transactions. Eavesdropper may listen to the communication but the content of the communication is kept secret. The researchers also discussed the need to prevent eavesdropper in intruding in the e-auction process to avoid possible occurrence of impersonation and financial theft.

6. FUTURE SCOPE

The advent of quantum computer will render present cryptographic techniques useless and vulnerable to attacks. Existing distributed ledger technologies including blockchain utilizes public key cryptography and digital signatures which are prone to attacks by the speculated quantum computers. Therefore, we recommend that post-quantum cryptographic mechanisms be employed in order to enhance the security of the distributed systems against quantum attacks.

REFERENCES

1. Al-Baddaci, H.H. and M. Sadiq (2021). Design and Implementation of an online Auction in Al-Somhan Showroom with IT and Information System Strategy. Journal of student Reseach. ISSN 2167-1907.
2. Madhuri et al (2020). Analysis, Design and Implementation of a secure online Auction System using Detaining Technique. International Research Journal of Engineering and Technology (IRJET). 2285-2288.
3. Singh, P and S.C. Jat (2020). A survey to detect financial fraud using deep learning approaches. International journal of Sceintific and Technology Research (IJSTR). 9(3). 16-20.
4. Galal, H.S. and A.M. Youssef(2018). Verifiable Sealed-bid Auction on the Ethereum Blockchain. 1-14. Retrieved 18/03/2022. https://github.com/HSG88/AuctionContract.
5. Chen, B, Li, X. T. Xiang and P. Wang (2022) SBRAC: Blockchain based Sealed-bid Auction with Bidding price privacy and public verifiability. Journal of Information Security and Applications. 65(2022). https://doi.org//10.1016/j.jisa.2021.103082.
6. Pillai, R, R. Ankalkote, M. Tamboli, S. Prakash and P.G. Narang (2021). E-Auction Website using Blockchain Technology. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE). 10(5). 90-93.
7. Sambare, S.S, N. Khandelwal, M. Nathwani, P. Munot and S. Patil (2022). A survey of E-bidding system using Blockchain. 4th International Conference on Smart Systems and Inventive Technology (ICSSIT).
8. Shea, S.(2020). How to prevent network eavesdropping attacks. https://www.techtarget.com
9. Sehgal, U and A.P.K Singh(2018). Eavesdropping attack problem threat in cyber security and wireless sensor network.
10. Yegui, C, G. Omyee, G.U. Yuan and C-H Lung (2020). Threats to online advertising and counter measures. A Technical Survey. Digit. Threat res. Pract. 1(2). https://doi.org/10.1145/3374136.
11. Ketan,P(2021).Digital Signature in India. https://www.networkinmagazineindia.com/200610/coverstory03.shtml. Retrieved 24/03/2022.
12. Khrykova, A, M. Bolsunovskaya, S.Shirokova and A. Novopashenny (2021). Implementation of digital Signature Technology to improve the interaction in Company. E3S Web of Conference 244.12023(2021). https://doi.org/10.1051/e3sconf/202124412023.
13. Qusa, H, J. Tarazi and V. Akre (2020). Secure E-auction system using Blockchain: UAE Case Study. Advances in Science and Engineering Technology International Conference (ASET). 1-5.
14. Zhong, H, S. Li, T-F, Cheng and C. Chang (2016). An Efficient Electronic English Auction System with a secure on-shelf mechanism and privacy preserving. Innovations in Communications Security.

15. Priya, J.P and J.P. Prathap (2012). Security boosted online auctions using Gnew Cryptography. International Journal of Applied Engineering & Research. 12(16). 6257-6266.

17. Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. IEEE Symposium on Security and Privacy (SP). San Jose, USA. 839–858.

18. Lafourcade, P., Nopere, M., Picot, J., Pizzuti, D. and Roudeix, E. (2019). Security analysis of auctionity: A blockchain based e-auction. International Symposium on Foundations & Practice of Security. FPS 19, Toulouse, France. 290–307.

21. Shea, S. How to prevent network eavesdropping attacks. 2020. https://www.techtarget.com/searchsecurity/answer/How-to-prevent-network-sniffing-and-eavesdropping

22. Ahubele, B.O and Okolai, B.D (2022). A Formal Verification Model for Security Vulnerability in Non-fungible Tokens (NFTs) Platform. Journal of Advances in Mathematical and Computational Sciences. 9(2). 61-74.