HCIS Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) Open Access

Human-centric Computing and Information Sciences (2024) 14:42
DOI: https://doi.org/10.22967/HCIS.2024.14.042
Received: October 28, 2022; Accepted: February 15, 2023; Published: July 30, 2024

Testing and Substantiation of Zero Trust Devices with Blockchain Procedures for Secured Data Transfer Approach

Shitharth Selvarajan[1], Selvakumar Manickam[2,*], Hariprasath Manoharan[3], Shams Ul Arfeen Laghari[4], Mueen Uddin[5], Maha Abdelhaq[6], and Raed Alsaqour[7]

Abstract

The need for secured data transmission devices is growing in current generation networking meadows. It is very important to process all the transmitted data in a confidential way and maintain integrity by means of congesting other unauthorized users from entering the internal system. However some of the secured devices that are already present in the market cannot be trusted for a long period of time as non-repudiation factors are much higher. As such, in a data processing technique, a device needs to be verified in a complete manner before trusting it. Hence, the proposed method provides possible solutions of verifying a network device before transmitting data. In order to verify the data without difficulty, blockchain procedures are incorporated where no large segments of data are transmitted as fragmentation of data is being processed in the many circumstances. Moreover, the zero trust devices are verified for more time periods, and only if appropriate data processing routes are captured, only the devices are then allowed to transmit. To test further the accuracy of zero trust devices, real-time data outcomes are analyzed under five different scenarios and even congestion is highly reduced in the projected model. Thus, in the comparison case with existing method, the proposed outcome which is enacted with an analytical model proves to be much effective at more than 78%.

Keywords

Zero Trust Model, Blockchain, Congestion, Delay, Packet Rate

1. Introduction

The major scientific problem of security exists in most of the designed engineering and non-engineering sectors that are provided for data transfer function [1]. Whenever a system is designed for complete online mode of data transfer, there is then a need for high security features where entire data must be prevented from external system operations [2]. Even after examining most of the designed applications, it has been

***Corresponding Author:** Selvakumar Manickam (selva@usm.my)
[1]School of Built Environment, Engineering and Computing, Leeds Beckett University, Leeds, UK
[2]National Advanced IPv6 Centre, Universiti Sains Malaysia, Gelugor, Penang, Malaysia
[3]Department of Electronics & Communication Engineering, Panimalar Engineering College, Poonamallee, Tamil Nadu, India
[4]Department of Computer Science & Engineering, Seoul National University of Science & Technology (SeoulTech), Seoul, Korea
[5]College of Computing and Information Technology, University of Doha for Science and Technology, Doha, Qatar
[6]Department of Information Technology, College of Computer & Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia
[7]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

found that the speed of data transfer and other related characteristics are perfect in their own way [3]. But in existing data transfer case studies, evaluations have been made with control techniques based on speed measurements, inducing the entire system to operate under low security cases [4]. Therefore, the entire data network must be redesigned by maintaining other characteristics which are a very difficult task to achieve, so that authentication factors can be considered by adding some futuristic determinations [5]. Additionally some of the existing evaluations provide support to security features without any trust factors, resulting in low-effect causes, and it needs to be reduced [6]. It is an arduous effort to send data that only the recipient can grasp, even though it is necessary for most companies under all real-world conditions. Therefore, all apps must be accessed using conventional network edge technologies to provide a secure design of data processing networks. However, a majority of current network architectures are only designed with weak authentication, requiring the use of hybrid resources. Even hybrid solutions are susceptible to inadequate security measures, since data in the surviving state of a particular model can be taken by another user on the same network if the model is moved to a different state. Therefore, the proposed method connects to the blockchain protocol, which divides all data into individual blocks for simple transfer. The total congestion present throughout the data transmission phase is avoided, along with some random hazards analyzed in tandem through the suggested method. Additionally, the zero trust models are confirmed by including several security measures that offer a good chance of connecting a portion of the defined network's nodes. The proposed technique uses a delay reduction procedure at the early data transfer stage to prevent unwelcomed or unknown users from accessing the planned network.

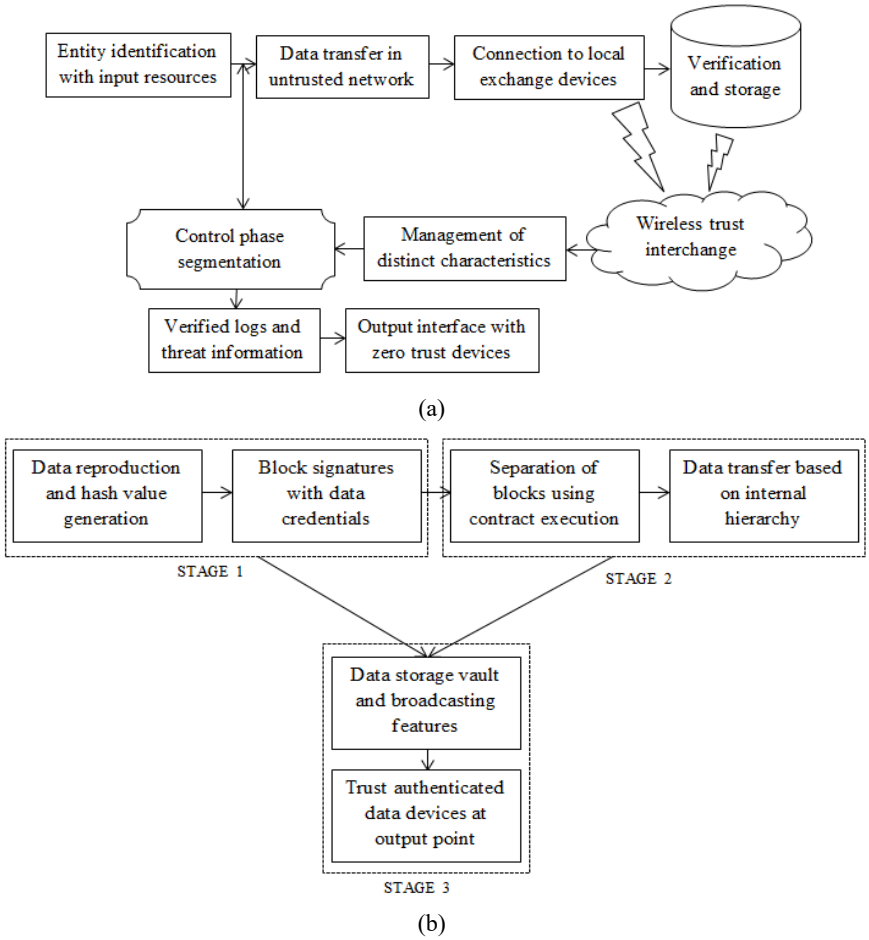

Fig. 1. (a) Block diagram of proposed verification model and (b) transaction execution hierarchy.

The sequence in Fig. 1 usually starts with identification of the data set by which it is provided in the form of resource application. Once the resources are incorporated at the initial state, a control state is established to verify the user request. Then, a differentiation is made between authorized and unauthorized users as entire data is segmented into different parts, with only requested data being sent to the users. It is necessary that recognized data must be transmitted using a network which is not present in the trusted environment on account of trust authentication factors not being present. Therefore, at the next sequence, the connection will be transferred to local servers where verification of forward and reverse links takes place, following after data segmentation and verification storage of appropriate data takes place in a wireless environment with a high trust factor, leading in turn to the management stage. The last sequence of device verification model consists of verifying unique characteristics of devices where direct interface segments are provided. Because whole devices are tested and validated at high transfer packet rates, the proposed method is the only one capable of resolving the aforementioned obstructive circumstances. A block diagram of the proposed zero trust approach is shown in Fig. 1. With the help of input resources and identification of all entry devices in the system, the blocks of zero trust devices in Fig. 1 are discovered. All input devices must have a unique identity to enter the network, since it cannot be verified if any of the devices present lack identification. At first, every registered device will begin exchanging data exclusively across untrusted networks. That said, after connecting with a local device, the device will change to an authenticated mode, utilizing key encryption codes. After employing verification factors, all verified codes will be saved at a later stage with significantly less latency, launching the cloud storage approach for data exchange between all devices. Subsequently, all of the various device characteristics will be examined after the data has been exchanged, and if the traits are accurate, the control phase will be initiated. Also, all user logs will be checked, and once all zero trust devices have been controlled again, they will be linked to output units.

1.1 Literature Review

Understanding various devices introduced to convey data with minimal security measures is crucial for thoroughly understanding the zero trust concept. Thus, diverse information concerning outdated technology that is used solely for information transmission without any verification features is added in this part. To provide accurate comparison scenarios where it is implemented under one constraint, even some devices already equipped with security features are added. Zero trust architectures are used in [1] to create a thorough survey connecting two disparate data sets. That being said, in this architecture, a global time standard is adhered to for verification instances. The equipment only permits connecting a small number of users, since a universal time standard is observed. Hence, the verification case study fails in these kinds of circumstances. Even if a few users are permitted, the device's attributes cannot be modified at any time, causing it to run in standby mode for an extended time. To accommodate a more significant number of users, an extensive data analytics system using data management techniques is built [2]. A new platform-oriented solution with advanced tool functionalities that are not maintained in this operation must be given, because massive data is managed in this process. In contrast, with a dynamic system model being developed, an information-spreading mechanism is included in the system [3] with different security characteristics, which guarantees excellent efficacy. Many users still adopt state transformation states even after such system formulations, thus posing an unacceptable feature in various device settings.

With the help of sixth-generation networks, which examine vital factors such as device stability about collision detection, all industries have created zero trust devices to adapt to changing circumstances [4]. More issues will arise if the devices are not stabilized at a specific point, rendering the entire apparatus unusable for communication. The standardization of the whole device will also be impacted, so in addition to stability, there is a requirement for all users to review the universal constraint. All zero trust devices are subject to delay when the universal condition is checked, leading to the development of an aware optimization strategy [5]. The above analysis has revealed that the mathematically specified quality

of link control does not produce good predictability. It is crucial to create an appropriate mathematical model to provide an optimal route allocation strategy to all users in the network that requires the signal interference ratio to be minimized. As a result, a trust-based control technique combines a fuzzy logic control model, where all erroneous requests from various users are discovered and regulated [6]. Most trust values are far greater than anticipated since a different controlling mechanism is developed under the abovementioned model. However, the system's overall workload will become disorganized if regulating strategies are offered on other media. For this reason, data is not sent out regularly in a zero trust device. As such, the complete request must be validated, and the request must arrange the information because it is harder to find the lost segments if the data is not set in order.

A distinct health record is created that identifies massive data and stores it in dependable networks to organize it sequentially [7]. Since the zero trust model cannot provide excellent security for integrated networks in this scenario, the weight association will be extended to a greater level. Additionally, a fuzzy decision-making mechanism is added to the abovementioned process, offering equivalent answers for all zero-trust authentication models. Since identical answers are obtained, zero trust devices can look for more solutions using the blockchain as a model. To guarantee time-varying operations over the entire network, a peer storage optimization mechanism must be activated in the proposed device whenever a blockchain is used as a reference model [8]. As a result of high period variability, a swarm optimization approach is selected for all pre-defined networks. Swarm optimization can be turned on, but only for mechanisms that change over time. Swarm optimization can't be used if the whole control strategy does not change. The structure of the data establishment process must be examined using heterogeneity and resource-limiting constraints when a network is secured [9–13]. If all restrictions are met, the data transmission procedure will be much more transparent and thus more efficient than in typical situations. The entire system is quite resilient to modest changes in the device, even if one constraint in the zero device model fails. As a result, the network must immediately implement the aforementioned limits. To investigate the use of blockchain technology, a thorough review process is created where by a more significant number of standard procedures are examined and resolved [14–17]. All tested models follow the identity verification method, ensuring a high level of trust during the data transfer process. The data integrity method is also added to provide key setup process generation and administration. If more keys are generated, confusion matrices will be formed, precluding a standard configuration to be set up for storing various keys in the network. In this situation, storing and sharing must be made available with security features, and new strategies are introduced to store whole data as independent records [18–24]. Therefore, a system framework is developed with variables after reviewing all relevant studies for the zero trust model (Table 1). With this in mind, a better optimization technique is merged with the suggested formulations discussed in the following sections.

Table 1. Existing evaluations

Study	Issues	Expert solutions
Syed et al. [1]	Network connectivity with communication & session security features	Allocation of minimized resources using zero trust devices
Song et al. [3]	Operation of data transfer in dynamic environment	Changing the mode of transfer to information-spreading application
Kesarwani and Khilar [6]	Data transfer load & workplace	Separate the number of authorized & unauthorized users
Peng et al. [7]	Big data scheduling	Data segmentation using various time periods
Chen et al. [9]	Restriction on incoming data traffic	Dissuade number of forward links towards safety route

1.2 Research Gap and Motivation

Most of the existing works [25–27] are introduced for data transfer in several application functions with a segmented data set where security features are much reduced. Even an individual data set is transmitted with low security, given blockchain procedures not being introduced in any system description. But some of the security features are added for a total data set requiring the entire block of data to be transmitted for a requested user, posing much difficulty in all time periods. In addition, the existing works are completely based on automatic operations, and thus the design specifications must be provided before processing the data. If such data transfer specifications are delivered, then it is a highly complex task to define the structure of data if it is taken by unauthorized users.

Therefore, given the abovementioned drawbacks, the data transfer process is very difficult to determine with additional security features. Hence, the proposed method is introduced with forward and reverse link procedures using blockchain and zero trust authentication factors. In this type of process, highly congested networks are separated to allow only authorized users with appropriate request. Furthermore, the individual weight of each data is restrained to provide a differentiation between high and low weight factors. Consequently, an unique mathematical model is described to identify the verified devices as zero trust being assumed by each user before transmission cycle. Furthermore, additional blocks of data are added to provide enhanced security to each determined blocks at high efficiency.

1.3 Objectives

The major objective of preventing unauthorized users in data transfer process that is present at various applications must ensure that the following objectives are contented.

- To reduce the amount of congestion (duplicate packets) that is present in data transfer process even after segmentation that is caused by unauthorized users.
- To integrate blockchain and zero trust authentication factors, increasing the complete effectiveness of packet transfer in both forward and reverse modes.
- To maximize the number of zero trust authenticated devices by providing an appropriate request for the data transfer process, given the entire data present being in the form of distinct segments.

1.4 Paper Organization

The rest of the paper is organized as follows. Section 2 provides the design of proposed method with parametric evaluations using various notations, and Section 3 introduces an optimization algorithm with step-by-step integration procedures. In Section 4, the combined experimental outcomes are provided, and finally in Section 5, the paper's conclusion is made with a discussion on future works.

2. System Model

The procedure for confirming that each connected device offers the necessary data transmission technology must be planned with suitable characteristics. The device will spend more time in the listening period and have higher latency at specific moments, if more parameters are employed in the design process. Therefore, in the zero trust model, the quality factor that is formed using Equation (1) provides the strength of connectivity between two separate links.

$$S_{ZT}(t) = E_n(i) + C_{ZT}(i) - d_{ZT}(i). \tag{1}$$

According to Equation (1), the delay in zero trust devices needs to be decreased in order to boost the strength of node connectivity. If the delay is a little bit longer, Equation (2) can be used to figure out the following reverse transmission path:

$$I_{ZT}(i) = min \sum_{i=1}^{n} \frac{1}{\rho_{ZT}(i) * \tau_{ZT}(i)}. \tag{2}$$

Equation (2) shows how to reduce interference during packet transfer, and Equation (3) denotes how to reduce congestion between separate data packets in reverse mode.

$$cong_i = min \sum_{i=1}^{n} \frac{\delta_i + (P_s(i) + P_r(i))}{h_p(i)}. \quad (3)$$

Equation (3) is constructed using a hop count, where congestion minimization is guaranteed because the average latency decreases as the hop count increases. If the device needs to be checked, then Equation (4) must be used to calculate the number of requests:

$$R_{ZT}(i) = min \sum_{i=1}^{n} \frac{RB_i}{R_t(i)}. \quad (4)$$

Equation (4) denotes that the device will process the right requests over time, if the defined ratio is minimized. So, Equation (5) is used to keep track of each unknown user who shows up at the set time:

$$UA_{ZT}(i) = min \sum_{i=1}^{n} \frac{\beta_i + \vartheta_i}{rate_i}. \quad (5)$$

Equation (5) indicates that the system needs to be cleared of all illegal users. Even if there are unauthorized users on the network, the relevant authority devices can be used to figure out the entropy function, which can be written as Equation (6):

$$AD_{ZT}(i) = min \sum_{i=1}^{n} \omega_z + \omega_y + \omega_{dev}. \quad (6)$$

Equation (6) explains the various device functions that must be minimized for authorization. So, Equation (7) can be used to denote the following about the percentage of packet rate after minimization:

$$packet_i = \sum_{i=1}^{n} \frac{A_p(i) + l_p(i)}{total\ time}. \quad (7)$$

Table 2. Description of mathematical notations

Variable	Description
E_n	Probable energy of all nodes
C_{ZT}	Communication link count with zero trust factor
d_{ZT}	Delay of zero trust devices
ρ_{ZT}, τ_{ZT}	Ratios of packet transfer in both forward & reverse modes
δ_i	Average delay of the data transfer device
P_s, P_r	Verification of packet sending and receiving states
h_p	Hop count of trust devices
RB_i	Depraved device request rate
R_t	Total device requests
β_i, ϑ_i	Request rates of unauthorized and unidentified users
$rate_i$	Transmission rate
ω_z, ω_y, ω_{dev}	An authorized function of z, y & other verified devices
A_p, l_p	Accomplished and lost packets
eff_{old}	Effort to solve old data covers
N_b	Total number of blocks
T_a	Period of transmission
$weight_i$	Total weighting factor
∂_i	Score of each block
VR_i	Number of verified zero trust devices
NR_i	Total number of allocated resources to all devices

The mathematical equations for the proposed method are formulated in the following manner by using some parametric determination where individual variables are linked in the programming models. Hence, each equation has primary importance related to data transfer functionalities, which ensures high security with minimized risk factors. Equation (1) is implemented to determine the strength of data connectivity at all nodes given that trust factors are reduced at such connection points. Equation (2) is formulated to check the number of data that is transmitted with forward and reverse links where a limitation factor is provided in the projected design. Equation (3) identifies the number of congested points using number of hop counts as most of the data transfer process is completed using shortest route points. Equation (4) establishes a request point to identify the number of unauthorized users in the data transfer path, enabling original data points to be guaranteed. Equation (5) and (6) are used for preventing the device from duplicated data to ensure proper authorized functions even at a large distance transfer. Equation (7) calculates number of transmitted packets within the allocated time interval, with lost packets being found in this programming period. Equation (8) determines complete effectiveness of the integrated blockchain algorithm where data is processed in a sequential order and the score of each transferred data is restrained. All of the variables in Equations (1) through (7) are used to check the measurements of a device, and are combined with an optimization technique to ensure that trusted devices are as safe as possible (Table 2).

3. Optimization Algorithm

Blockchain technology must transmit data blocks at predetermined times to ensure high reliability in the integrated device. Although the process above is carried out in the event of regular operating instances, it is crucial to validate the blockchain process using a suitable system model if homogenous operational networks are formed. As a result, in this part, inspection processes are used to verify a block of data in addition to device verification. The main benefit of using blockchains as the optimization tool in the suggested method is attributed to the ease with which all decentralized data can be managed with minimal data duplication. Additionally, the entire system will fully avoid any data subjected to transformation content, and if any security flaws are found in the planned network, a blockchain can be used to isolate the entire network connection to enable the restriction of all devices. As was already indicated, if devices are constrained, transmission freedom in the network will be entirely prevented, and in this low-freedom case, only authorized users can broadcast [28–30]. As a result, in the case of inadequate security measures being in place, most data from unauthorized users is not transmitted. However, the proposed solution uses a blockchain with zero trust, which assures that a slight compromise can be made during data transmission and that even during the verification phase, if any discrepancies are discovered, the associated data can be ignored in the system. The following are the details of the mathematical model for the blockchain used in zero trust data transmission [31, 32]:

$$eff_{new} = min \sum_{i=1}^{n} \frac{eff_{old} * N_b * T_a(i)}{Total\ time}. \tag{8}$$

Equation (8) shows the minimization issue to check the quantity of challenges in developing a safeguarded transmission mechanism. So, Equation (9) is used to make a verification method that uses representations of the total weight.

$$VM_i = min \sum_{i=1}^{n} weight_i * \partial_i. \tag{9}$$

Equation (9) shows a minimization function that involves issuing a series of commands that are directly tied to weighting factors. To determine the weighting factors, each user must be aware of the source information, which is formulated using Equation (10) as denoted:

$$U_i = \sum_{i=1}^{n} \frac{VR_i}{NR_i}. \tag{10}$$

The flow chart in Fig. 2 provides an integrating network where the defined system model is combined with blockchain and zero trust authentication factors. The combined process is usually initiated with parametric values that are defined with maximum and minimum limits using energy, forward, reverse links and delay factors. After defining the limits of parametric segments, the number of packets to be transmitted in bidirectional ways are chosen and a complete ratio is defined with a low congestion rate. In the case of congestion of packets during data transfer state being higher, the objective function of the designed model is not contented, so the programming loop will be set at the initial stage for parametric description. In addition, other ways for reducing the congestion is also described using request rate by separating it into authorized and unauthorized users. At last stage the output function is achieved only if a request is made from authorized users, thus minimizing total loss in the network.

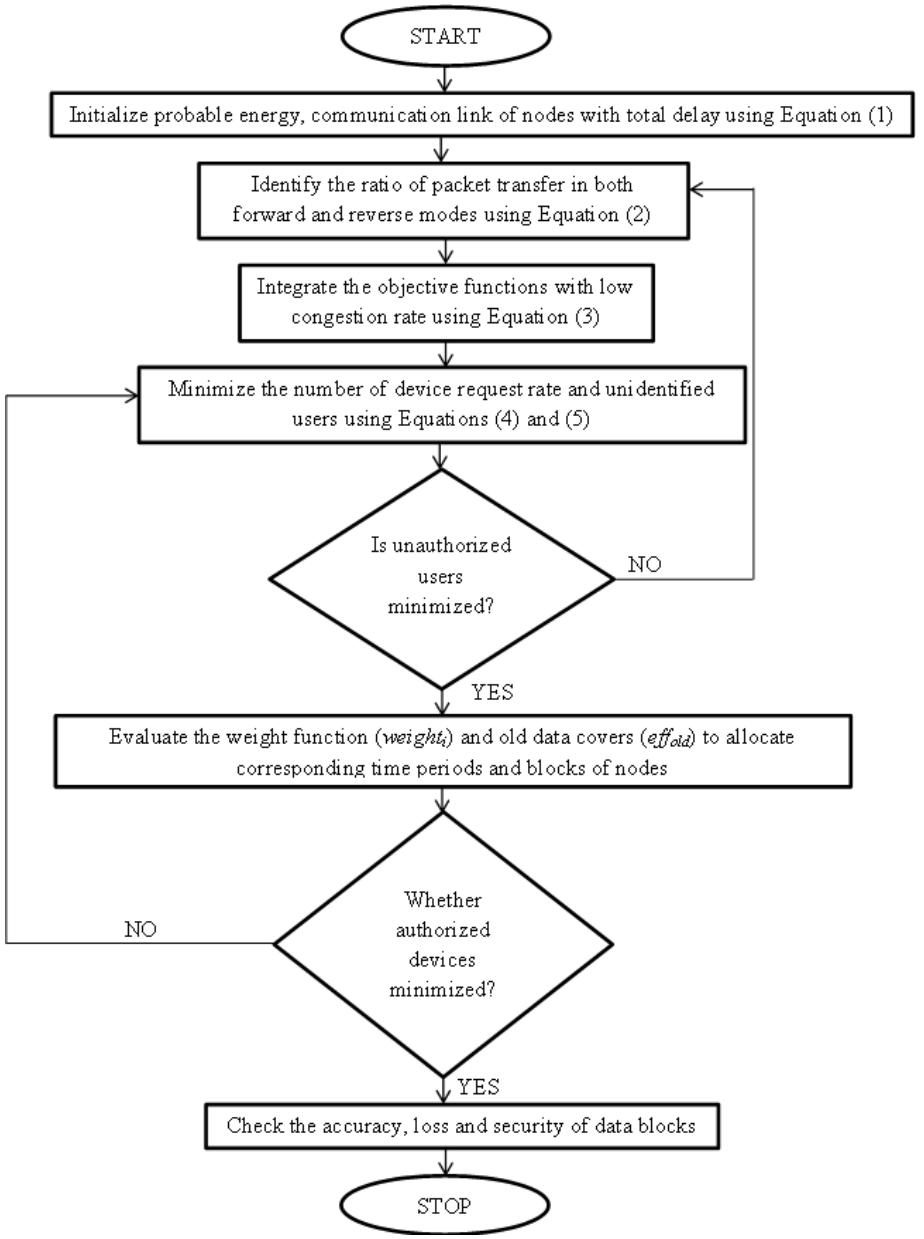

Fig. 2. Step-by-step implementation of zero trust model.

3.2 Program Execution Event

```
%function added = add_mined_block(obj, block)
assert(isa(block, 'bc.Block'));
valid = bc.Blockchain.validate_block(block, obj.blockchain(end));
if valid
obj.blockchain(end+1) = block;
added = true;
else
added = false;
%function rv = replace_blockchain(obj, new_blockchain)
valid = bc.Blockchain.validate_chain(new_blockchain);
if ~valid
rv = p2p.MessageType.DO_NOTHING;
return;
end
if numel(new_blockchain) > numel(obj.blockchain)
obj.blockchain = new_blockchain;
rv = p2p.MessageType.BROADCAST_LATEST;
end
end
%function rv = handle_blockchain_response(obj, mess)
% Convert incoming message of strcut or array of struct
% to array of blocks
received_blockchain = bc.Block(mess(1));
if numel(mess) > 1
for idx = 2:numel(mess)
received_blockchain(end+1) = bc.Block(mess(idx));
end
end
latest_block_received = received_blockchain(end);
latest_block_held = obj.blockchain(end);
rv = p2p.MessageType.DO_NOTHING;
% If received latest block is not later than the local, do
% nothing.
if latest_block_received.index > latest_block_held.index
if latest_block_held.hash == latest_block_received.previous_hash
% We can append the received block to our chain
% FIXME validate block
valid = bc.Blockchain.validate_block(latest_block_received, latest_block_held);
if valid
obj.blockchain(end+1) = latest_block_received;
rv = p2p.MessageType.BROADCAST_LATEST;
end
elseif numel(received_blockchain) == 1
% We have to query the chain from our peer
rv = p2p.MessageType.QUERY_ALL;
else
% Received blockchain is longer than current blockchain
rv = obj.replace_blockchain(received_blockchain);
end
% Above only works if only one block or entire chain is
```

```
% sent, which should be the case.
end
end
end
```

4. Results and Discussions

In this section, simulation settings offered for zero trust devices are used to discuss the results and compare the obtained results with those obtained using existing methodologies. Since only simulation records may be used to witness all defined outcomes in this verification procedure, it is necessary to specify the kind of simulation tool integrated with the hardware configuration. As a result, the network blockchain tool is employed in the suggested method with an initial address transfer, and all parametric assessments are completed in MATLAB. The intended zero trust device is compatible with blockchain tools, because every created block is subject to examination at every level. Most devices will have their proper data transfer functionality checked during the analysis step, with only the chosen devices being used for wireless operations. That being said, all unsuccessful zero trust devices are permitted for re-verification by implementing the necessary blockchain features. Additionally, zero trust devices work in all supported situations with low robustness, but the loss ratio for the intended devices will be significantly higher if greater robustness is seen. Hence, in testing how well the suggested approach works, the system model is broken up into five main scenarios. A loop-based route score is built into the system model, which is used to implement all of the above scenarios. The zero trust devices will be checked once more using new route design elements, if the score of each scenario falls below a certain threshold. Therefore, it is crucial first to determine how many resources are available for validating the device simulation factors. Additionally, if the resources allocated are significantly higher, they can be used in the subsequent verification phases. However, suppose a user chooses to avoid giving the same amount of resources to each device in a specific network. In that case, prior notice must be provided to all newly generated blocks. If the information about the resource is not provided, the whole block will have security problems again, and in the end, the produced blocks won't get all of the data to the destination.

4.1 Scenario 1

The communication link factor analyzes the total latency, validating all of the network's devices. Information resources must be appropriately allocated to decrease the time it takes to verify zero trust devices. Additionally, all delay times of the zero trust device must be kept to a minimum, creating an inverse ratio in the suggested method for all verification processes. Furthermore, a user can transmit the data block on zero trust devices in both forward and reverse modes, while using this delay minimization approach. When a user uses both transfer modes, the proper precautions are taken to verify the network's devices, due to risk of the reverse transfer resulting in severe congestion issues. This decreases the time required to validate a zero trust device by measuring the reproduction rate of the reverse transmission line and providing the inverse product at output stages. The simulated output is evaluated for the delay representation factor as shown in Table 3.

The analysis of the delay characteristics of zero trust devices is provided with five probable alternative energies, as shown in Table 3. Accordingly, the observed proportion of packets transported in both forward and reverse modes for allotted potential energies, such as 1.5, 2, 2.5, 3, and 3.5 kW, is 34%, 37%, 41%, 45%, and 48%, respectively. The proposed approach is substantially faster than the current way of checking all transmitted packets in a zero trust device during this type of packet transfer procedure [6]. This may be confirmed by utilizing a mid-probabilistic energy rate of 2.5 kW, where 41% of packets are transmitted with a verification stage delay of 2.2 seconds for the previous technique and 1.01 seconds

for the suggested method. Additionally, even though the proportion of transmitted packets is raised, the verification latency is shortened. By sending the data in blocks, the overall time is cut by more than a second. Thus, this example demonstrates how the suggested method can enable zero trust devices to employ reverse transmission modes.

Table 3. Comparison of data delay

Probable energy (kW)	Percentage of packet transfer	Delay time (s)			
		Kesarwani and Khilar [6]	Kumari et al. [25]	Rahman et al. [26]	Proposed
1.5	34	2.36	2.31	2.29	1.13
2	37	2.24	2.19	2.17	1.07
2.5	41	2.2	2.11	2.04	1.01
3	45	2.16	2.05	1.76	0.8
3.5	48	2.1	1.96	1.52	0.5

4.2 Scenario 2

Every time data is carried across wireless networks, there is an issue with data congestion that can only be fixed if a device continues to be confirmed in the system. As a result, rather than using total delay representations, this scenario looks at average delay times to analyze the congestion condition. Since it is necessary to determine the hop count, also known as the distance of transfer, average values are preferred in these situations for verifying data in a zero-trust paradigm. That being said, a user can also check a zero trust device using total delay values, with extra waiting time to be assigned during verification at the transmission and reception times. As a result, the verification device must spend time listening to a particular set of data representing the average delay values. The entire distance of the device, which is simulated and shown in Table 4, will be used to separate all the summed values.

Table 4. Percentage of data congestion

Hop count	Number of verified packets	Percentage of congestion			
		Kesarwani and Khilar [6]	Kumari et al. [25]	Nartey et al. [27]	Proposed
1	1,005	43	40	38	27
2	1,678	41	34	32	22
3	2,013	40	30	27	16
4	2,279	37	25	21	13
5	2,568	34	22	16	10

According to Table 4, there is less congestion of zero trust devices during the packet transfer stage than with the current method [6]. The one-step factor is used to vary the number of hop counts between various zero-trust nodes in the network to investigate the congestion issue. More packets are verified using the step-above factor, including 1,005, 1,678, 2,013, 2,279, and 2,568. The congestion percentage is quickly determined despite the higher number of verified packets in zero trust devices. As a result, for verified packets, the congestion percentage for the existing technique is 43%, 41%, 40%, 37%, and 34%, whereas for the suggested method, it is equivalent to 27%, 22%, 16%, 13%, and 10%. The proposed method transmits all data blocks at low congestion rates to verify the zero trust device at low data traffic rates. Furthermore, because of low congestion levels, correct device requests can be detected and verified for just that device.

4.3 Scenario 3

The quantity of packet rate in the system must be checked after making the appropriate request to the other user, which has been done in this case. Most users will authorize a higher request rate to other users in various locations during the evaluation stage. Due to the increased requests, each device will allow a certain amount of time for the reply message before verifying. A zero trust device may very well send corrupted packets into the system during the waiting period, a possibility that should be prevented. However, the entire number of original packets can be considered in this situation, which gives a technique to locate the correct network users. As a result, the system uses transmission rates to add and differentiate between approved and unknown users. The certified device will cover more data points throughout this separation procedure, but the total number of communicated blocks must be less. A comparison of the considerable pack rate for the existing [6] and suggested methods is shown in Table 5.

Table 5. Rate of data packets

Percentage of accomplished packets	Percentage of lost packets	Packet rate (Mbps)			
		Kesarwani and Khilar [6]	Rahman et al. [26]	Nartey et al. [27]	Proposed
84	16	2.5	2.2	3.4	1.2
89	11	2.9	3.1	3.7	1.4
93	7	3.4	3.6	4.2	1.6
99	1	3.7	3.9	4.4	1.6
100	0	4.6	5.1	4.8	1.6

Table 5 denotes that measuring both accomplished and lost packets is practical, and the system gives percentages of measurements of 84%, 89%, 93%, 99%, and 100%, respectively. Given that there are fewer lost packets due to the high percentage of achieved packages, permitted functions are automatically increased. At this controlling stage, zero trust devices are allowed to receive a packet request rate from other network devices, when the initially lost packets are regulated. As more transmission rates are required for more significant amounts of the packet transfer, the existing method allows up to 4.6 Mbps, in contrast to the projected model's 1.6 Mbps. With the packet rate demonstrating this in a comparison case, the devices will be tested at higher transmission rates, even for growing data segments, and the rate of 1.6 Mbps will only change if the suggested method is used.

4.4 Scenario 4

In this case, the effectiveness of device verification, as indicated by specific factors is measured. The zero device models will verify all previously communicated data, also known as "old cover terms," to make accurate measurements. The effectiveness of zero trust devices will rise significantly if the gadget offers a higher accuracy rate for solving outdated data. However, a device can use the entire period for testing purposes without needing to constantly rely on old data covers. Thus, the complete number of blocks is duplicated with a maximum number of periodic representations. Furthermore, all zero trust devices in this type of efficiency determination mechanism must have their resources properly allocated, or else efficiency will suffer. As a result, a more significant number of zero trust devices continue to operate without any constraints. The efficiency of the suggested and existing methods is shown in Table 6.

Table 6 shows how effective the suggested method is at proving the zero trust model utilizing the newly added blocks in contrast to previous cases. The resolved old data representation with percentage factors of 40%, 50%, 60%, 70%, and 80% can be used to verify this. In this example, the number of newly inserted blocks equals 6, 8, 10, 12, and 14, respectively. The suggested verification technique is not altered due to the newly inserted blocks, so no additional vibrations are discovered in the system. The efficiency of the proposed approach has grown above 80% due to the newly included blocks, but the efficiency of the present method does not reach such a percentage factor. This can be seen using the 60-

year-old data factor and the six newly added blocks, where the efficiency percentages for predicted and existing models are 87% and 70%, respectively. Because of these efficiency improvements, it's easy to send blocks of data, even when the transmission of brand-new blocks with significant efficiency improvements is acknowledged.

Table 6. Effective data transfer points

Percentage of old covers	Number of new blocks	Efficiency (%)			
		Kesarwani and Khilar [6]	Rahman et al. [26]	Nartey et al. [27]	Proposed
40	6	67	71	68	79
50	8	69	74	72	85
60	10	70	79	75	87
70	12	73	83	79	89
80	14	74	85	81	93

4.5 Scenario 5

For all zero trust devices, the weight representation process is evaluated by counting the number of sent blocks that must not contain significant weighting factors. The total score of all verified zero trust devices will significantly increase if a block's weight is higher. Therefore, in the system that is directly reproduced using the score of individual factors, the weight of each block must be decreased. Information about each transmitted block must be known during this score-based measurement. If information is not known in a prior medium, confusion metrics will result, which must be avoided. The score above will mitigate all challenges associated with designing and validating a specific zero trust device. That being said, if congestion is more significant, the score of each block will be impacted. Simply put, each block's weight must be less than 20% of the sent data [7]. Table 7 provides individual scores of transmitted blocks with total weight factor representations.

Table 7. Data weights

Total weighting factor	Score of blocks	Total weight (g)			
		Kesarwani and Khilar [6]	Rahman et al. [26]	Nartey et al. [27]	Proposed
0.5	78	0.9	0.95	0.92	0.04
0.8	85	1.7	1.9	1.8	0.19
0.9	91	2.4	2.5	2.4	1
1	95	2.9	3.2	3.1	1.2
1.2	97	3.1	3.4	3	1.5

From Table 7, it is evident that weighting factors are varied in small step sizes of 0.5, 0.8, 0.9, 1, and 1.2, respectively. For each change in the block weighting factor, an individual score is measured as 78, 85, 91, 95, and 97, respectively, where both values are reproduced. During the reproduction stage, the total number of verified devices is counted, and weighting factors for verified devices are not considered. The aforementioned instance is applied to the proposed and existing approach [6], and the total weight is measured. Based on comparison results, the total weight of blocks allotted using the predicted technique is significantly less and culminates at 1.5 g. However, the weight factor in the current technique has been raised to 3.1 g, which is substantially larger for a single block of data. This can be accurately maintained with an individual score of 78 and a total weighting factor of 0.5. The total weight, in this case, is 0.9 g for the existing methods and 0.04 g for the proposed ones.

5. Conclusion

In today's networks, which work well in a variety of situations, the method of data transmission involving an intermediary node is strongly advocated. When intermediate nodes are preferred in the system, the device requires more configuration changes made by outside users. Such configurations make it impossible to guarantee that every connected device in the network is completely secure. In most circumstances, a device cannot completely authenticate all data packets and associated intermediary nodes within the same network. Therefore, it is essential to verify the device by sending the data in discrete blocks, which are then examined and decoded in the suggested model. It is also necessary to develop a separate analytical formulation where packets are permitted to transmit in both forward and reverse modes, enabling a device to be trusted during the data transmission process. The zero trust device experiences some latency during the transmission period due to reverse motion transmission, which is eliminated by using a corrupted device request. Data will only be delivered in secure mode for specific requests, given that zero trust devices cannot be requested frequently. Similarly, blockchain technology also offers a secure method of transfer because each user transmits small data blocks that are incomprehensible to machines.

Additionally, each block's weight was decreased during the transmission process, enabling each packet to be transferred at a rapid pace. The efficiency of the data transfer phase was increased with the total amount of time spent on representations. The analysis was done at each stage to identify potential approaches to looking at historical data stored in the system. As a result, the security of the zero trust model was improved because all unknown and unauthorized users were prevented during device verification. In testing the effectiveness of the zero trust model, five scenarios were examined on average, with each scenario outperforming the current method by 78% on average fields.

5.1 Future Works

The proposed work on zero trust authentications can be extended with large parametric identification by considering more number of requested users towards forward link cases. In additional the zero trust factors can be elaborated with immediate mode changing characteristics where complete assurance can be provided for safety routes. Moreover automated enabling features can also be provided towards incoming data traffic using intelligent optimization techniques such as deep and machine learning.

Author’s Contributions

Conceptualization, SS, HM; Funding acquisition, SM; Investigation and methodology, SS, HM; Project administration, MU; Resources, SUAL, MA, RA; Supervision, SM, MU; Writing of the original draft, SS, HM; Writing of the review and editing, SS, HM; Software, SUAL, MA, RA; Validation, SUAL, MA, RA; Formal analysis, SM, MU; Data curation, SM, MU; Visualization, SUAL, MA, RA.

Funding

This research was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project (No. PNURSP2023R97), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Competing Interests

The authors declare that they have no competing interests.

References

[1] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): a comprehensive survey," *IEEE Access*, vol. 10, pp. 57143-57179, 2022. https://doi.org/10.1109/ACCESS.2022.3174679

[2] P. Colombo and E. Ferrari, "Access control technologies for big data management systems: literature review and future trends," *Cybersecurity*, vol. 2, article no. 3, 2019. https://doi.org/10.1186/s42400-018-0020-9

[3] G. Song, Y. Wang, and Y. Li, "Dynamic mathematical model of information spreading on news platform," *Wireless Communications and Mobile Computing*, vol. 2021, article no. 2174190, 2021. https://doi.org/10.1155/2021/2174190

[4] S. Li, M. Iqbal, and N. Saxena, "Future industry Internet of Things with zero-trust security," *Information Systems Frontiers*, 2022. https://doi.org/10.1007/s10796-021-10199-5

[5] G. R. Elangovan and T. Kumanan, "Energy efficient and delay aware optimization reverse routing strategy for forecasting link quality in wireless sensor networks," *Wireless Personal Communications*, vol. 128, pp. 923-942, 2023. https://doi.org/10.1007/s11277-022-09982-7

[6] A. Kesarwani and P. M. Khilar, "Development of trust based access control models using fuzzy logic in cloud computing," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 5, pp. 1958-1967, 2022. https://doi.org/10.1016/j.jksuci.2019.11.001

[7] H. Peng, Z. Tian, X. Li, W. Wang, G. Nauryzbayev, K. Rabie, and T. R. Gadekallu, "Covert communication for cooperative NOMA with two phases detection," *Alexandria Engineering Journal*, vol. 67, pp. 39-49, 2023. https://doi.org/10.1016/j.aej.2022.10.031

[8] M. U. Aftab, Y. Munir, A. Oluwasanmi, Z. Qin, M. H. Aziz, and N. T. Son, "A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles," *IEEE Access*, vol. 8, pp. 24196-24208, 2020. https://doi.org/10.1109/ACCESS.2020.2969715

[9] A. Chen, G. Lu, H. Xing, Y. Xie, and S. Yuan, "Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments," *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, article no. 1550147720921778, 2020. https://doi.org/10.1177/1550147720921778

[10] N. Papakonstantinou, D. L. Van Bossuyt, J. Linnosmaa, B. Hale, and B. O'Halloran, "A zero trust hybrid security and safety risk analysis method," *Journal of Computing and Information Science in Engineering*, vol. 21, no. 5, article no. 050907, 2021. https://doi.org/10.1115/1.4050685

[11] S. Mandal, D. A. Khan, and S. Jain, "Cloud-based zero trust access control policy: an approach to support work-from-home driven by COVID-19 pandemic," *New Generation Computing*, vol. 39, pp. 599-622, 2021. https://doi.org/10.1007/s00354-021-00130-6

[12] T. W. Chiang, D. L. Chiang, T. S. Chen, F. Y. S. Lin, V. R. Shen, and M. C. Wang, "Novel Lagrange interpolation polynomials for dynamic access control in a healthcare cloud system," *Mathematical Biosciences and Engineering*, vol. 19, no. 9, pp. 9200-9219, 2022. https://doi.org/10.3934/mbe.2022427

[13] M. Liyanage, Q. V. Pham, K. Dev, S. Bhattacharya, P. K. R. Maddikunta, T. R. Gadekallu, and G. Yenduri, "A survey on Zero touch network and Service Management (ZSM) for 5G and beyond networks," *Journal of Network and Computer Applications*, vol. 203, article no. 103362, 2022. https://doi.org/10.1016/j.jnca.2022.103362

[14] W. Wang, H. Huang, Z. Yin, T. R. Gadekallu, M. Alazab, and C. Su, "Smart contract token-based privacy-preserving access control system for industrial Internet of Things," *Digital Communications and Networks*, vol. 9, no. 2, pp. 337-346, 2023. https://doi.org/10.1016/j.dcan.2022.10.005

[15] P. Zhang, C. Tian, T. Shang, L. Liu, L. Li, W. Wang, and Y. Zhao, "Dynamic access control technology based on zero-trust light verification network model," in *Proceedings of 2021 International Conference on Communications, Information System and Computer Engineering (CISCE)*, Beijing, China, 2021, pp. 712-715. https://doi.org/10.1109/CISCE52179.2021.9445896

[16] H. F. Atlam, M. A. Azad, M. O. Alassafi, A. A. Alshdadi, and A. Alenezi, "Risk-based access control model: a systematic literature review," *Future Internet*, vol. 12, no. 6, article no. 103, 2020. https://doi.org/10.3390/fi12060103

[17] T. Zhong, J. Chang, P. Shi, L. Li, and F. Gao, "Dyacon: Jointcloud dynamic access control model of data security based on verifiable credentials," in *Proceedings of 2021 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*,

New York, NY, USA, 2021, pp. 336-343. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00054

[18] V. Gayoso Martinez, L. Hernandez-Alvarez, and L. Hernandez Encinas, "Analysis of the cryptographic tools for blockchain and bitcoin," *Mathematics*, vol. 8, no. 1, article no. 131, 2020. https://doi.org/10.3390/math8010131

[19] S. Dhar and I. Bose, "Securing IoT devices using zero trust and blockchain," *Journal of Organizational Computing and Electronic Commerce*, vol. 31, no. 1, pp. 18-34, 2021. https://doi.org/10.1080/10919392.2020.1831870

[20] M. Waleed, R. Latif, B. M. Yakubu, M. I. Khan, and S. Latif, "T-smart: trust model for blockchain based smart marketplace," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 16, no. 6, pp. 2405-2423, 2021. https://doi.org/10.3390/jtaer16060132

[21] S. Ali, G. Wang, S. Riaz, and T. Rafique, "Preserving the privacy of dependent tuples using enhanced differential privacy," *Human-Centric Computing and Information Sciences*, vol. 12, article no. 43, 2022. https://doi.org/10.22967/HCIS.2022.12.043

[22] A. Hussain, B. Shah, T. Hussain, F. Ali, and D. Kwak, "Co-DLSA: cooperative delay and link stability aware with relay strategy routing protocol for flying ad-hoc network," *Human-Centric Computing and Information Sciences*, vol. 12, article no. 34, 2022. https://doi.org/10.22967/HCIS.2022.12.034

[23] E. Shin, H. Yu, S. Bae, and H. B. Chang, "The impact of enterprise security performance on business performance in industrial convergence environment," *Human-centric Computing and Information Sciences*, vol. 12, no. 33, 2022. https://doi.org/10.22967/HCIS.2022.12.033

[24] M. Y. Hong, J. S. Yoo, and J. W. Yoon, "Homomorphic model selection for data analysis in an encrypted domain," *Applied Sciences*, vol. 10, no. 18, article no. 6174, 2020. https://doi.org/10.3390/app10186174

[25] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and AI amalgamation for energy cloud management: challenges, solutions, and future directions," *Journal of Parallel and Distributed Computing*, vol. 143, pp. 148-166, 2020. https://doi.org/10.1016/j.jpdc.2020.05.004

[26] Z. Rahman, X. Yi, and I. Khalil, "Blockchain-based AI-enabled Industry 4.0 cps protection against advanced persistent threat," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6769-6778, 2023. https://doi.org/10.1109/JIOT.2022.3147186

[27] C. Nartey, E. T. Tchao, J. D. Gadze, E. Keelson, G. S. Klogo, B. Kommey, and K. Diawuo, "On blockchain and IoT integration platforms: current implementation challenges and future perspectives," *Wireless Communications and Mobile Computing*, vol. 2021, article no. 6672482, 2021. https://doi.org/10.1155/2021/6672482

[28] W. Abu-Ulbeh, M. Altalhi, L. Abualigah, A. A. Almazroi, P. Sumari, and A. H. Gandomi, "Cyberstalking victimization model using criminological theory: a systematic literature review, taxonomies, applications, tools, and validations," *Electronics*, vol. 10, no. 14, article no. 167, 2021. https://doi.org/10.3390/electronics10141670

[29] A. Mughaid, S. Al-Zu'bi, A. Al Arjan, R. Al-Amrat, R. Alajmi, R. A. Zitar, and L. Abualigah, "An intelligent cybersecurity system for detecting fake news in social media websites," *Soft Computing*, vol. 26, pp. 5577-5591, 2022. https://doi.org/10.1007/s00500-022-07080-1

[30] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging trends in blockchain technology and applications: a review and outlook," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6719-6742, 2022. https://doi.org/10.1016/j.jksuci.2022.03.007

[31] H. Manoharan, S. Shitharth, K. Sangeetha, B. P. Kumar, and M. Hedabou, "Detection of superfluous in channels using data fusion with wireless sensors and fuzzy interface algorithm," *Measurement: Sensors*, vol. 23, article no. 100405, 2022. https://doi.org/10.1016/j.measen.2022.100405

[32] A. O. Khadidos, S. Shitharth, H. Manoharan, A. Yafoz, A. O. Khadidos, and K. H. Alyoubi, "An intelligent security framework based on collaborative mutual authentication model for smart city networks," *IEEE Access*, vol. 10, pp. 85289-85304, 2022. https://doi.org/10.1109/ACCESS.2022.3197672