IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 November 2022, accepted 12 December 2022, date of publication 20 December 2022,
date of current version 26 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3230944

RESEARCH ARTICLE

An Efficient Trust Management Technique Using ID3 Algorithm With Blockchain in Smart Buildings IoT

FATHE JERIBI[1], RASHID AMIN[2], MOHAMMED ALHAMEED[1], (Member, IEEE), AND ALI TAHIR[1]

[1]College of Computer Science and Information Technology, Jazan University, Jazan 45142, Saudi Arabia
[2]Department of Computer Science, University of Chakwal, Chakwal 48800, Pakistan

Corresponding author: Rashid Amin (rashid4nw@gmail.com)

This work was supported by the Deanship of Scientific Research at Jazan University, in 2021, under Project W43-077.

ABSTRACT Because of the rising population density, relationships are necessary to raise living standards through sending and receiving a wide range of services. Because of this, many means of object communication—regardless of their nature—are necessary to meet our daily needs. IoT is a network of physical things integrated with sensors, and software to communicate with each other. To establish a good connection, every object considered to be an associate of another object should meet certain requirements including scalability, interoperability, and trustworthiness. IoT security is a challenging task to protect the hardware and networks in the IoT system and a significant constraint to the deployment and realization of IoT. IoT security may include data confidentiality, authentication, access control, anonymity, and trust among services and products. Exchanging trust information is critical for assessing an entity's trustworthiness. Therefore, trust information must be shared and stored securely to ensure reliability, honesty, and safety. We propose a secure trust management scheme built on blockchain technologies to secure the entire system in transparency, traceability, and material integrity. We implement a blockchain-based trust management architecture for smart buildings that collect node trust proof. It assigns a trust score to each node, securely stores them in an array, then the threshold value is computed using the ID3 Algorithm. IoT threshold value is broadcasted into the blockchain network and stored in the trusted list. According to the findings, our approach encompasses security measures such as tamper-proofing, attack resistance, reliability, and low functionality for IoT in smart buildings.

INDEX TERMS IoT security, block chain, smart building, trust management.

I. INTRODUCTION

Iternet has become an important ingredient for people and companies to establish online enterprises such as banking, online education, and electronic commerce as a result of recent technical advancements and increasing digital adoption [1]. Humans' capacity to work and execute tasks (e.g., Transaction Banking (TB), healthcare support, and online education) at any time and from any location is increasing in this digital age [2]. The increasing reliance on the Internet comes with a slew of security and privacy concerns, including the theft of sensitive information and service interruption. The Internet of Things (IoT) in smart buildings plays a crucial role in everyday life and covers a variety of topics, including smart homes, cars, games, and organizational equipment [3]. IoT in smart buildings now includes smart grids and smart cities. In smart building networks, the Internet of Things (IoT) is linked to sensors, things, and smart equipment that may interact with one another; Kavin Ashton first proposed this idea in 1999. Every item is a component of the Internet of Things (IoT) in a smart building network, supporting compatibility with the present system [4]. Building Manage-

The associate editor coordinating the review of this manuscript and approving it for publication was Engang Tian.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

ment Systems (BMS) is made with efficeint underpinning control and networking infrastructure of smart devices like alarms, RFIDs, cameras, miles, and sensors [5], [6]. Mobile devices and networking infrastructure are both included in the Internet of Things (IoT in smart buildings). Many crucial building components, including the ventilation system, electricity, light, protection, and flame systems, are under the control of the building management system (BMS). It has the ability to exchange data with IoT cameras used in smart buildings [7]. IoT in smart buildings faces many challenges such as privacy, security, and access control. Additionally, every device connected/ deployed, and every single byte communicated in the IoT in the smart Building system, faces some security issues. In IoT in smart building, there can be compromise nodes as a part of the network [8]. The security issue is one of the most common issues in any IoT in a smart building network. The security of IoT in the smart building is concerned with cryptography and access control. The technologies that are part of the IoT in smart Building networks can share confidential Information with untrusted nodes. For the security of the devices, trust management systems are proposed by various researchers. The trust management models can maintain trust among nodes and decrease communication and information transfer risk with compromise nodes [9].

Blockchain was introduced in October 2008 by Nakamoto; it sets top of the Internet because BlockChain is a peer-to-peer network. Initially, it was a part of the Bitcoin virtual currency system. A bitcoin currency system has authority for issuing currency, ownership transforming and transactions confirming, etc. Bitcoin is the first application that depends on BlockChain. BlockChain and TCP/IP protocol works in parallel. Blockchain, like TCP/IP, is a network that is accessible, distributed, and sharing. The TCP/IP protocols lowering the cost of links, and Blockchain reduced the expense of operations as much as possible that is being used in different platforms such as automobiles, business organizations, homes, and financial organizations. Now a day's [10], cyber-attacks have become more advanced complex. An intrusion detection system (IDS) helps to identify these cyber attacks. IDS is categorized into two forms. One is (HIDS), and the other is (NIDS). BlockChain works with IDS and identifies and resolves these cyber attacks more accurately. There are several challenges to adopt blockchain in IoT framework some of them are as follows:

- In the PoW system, a miner must do some prescribed labor, often a difficult-to-calculate but simple-to-verify mathematical problem or challenge. In order to validate each block, a PoW is required. The time required to verify a block and the computing power of the miners may be used to adjust the mathematical challenge's difficulty level.
- Due to the network layer's sensitivity and need for legitimate, temper-proof data delivery, a difficult task, more attack opportunities exist.
- The authorization process regulates who has access to the IoT services. Although connecting particular services to specific devices is exceedingly difficult, maintaining confidence is necessary. Unlike conventional database management systems, queries in an IoT situation are processed instantly.
- IoT variety necessitates interoperability for proper operation, yet the diverse environment created by this diversity gives rise to several security concerns. Different interoperability postures, such as heterogeneous devices, networks, platforms, and protocols, are possible.

Blockchain is an open ledger and is saved by each node in the network. Blockchain is an open ledger and peer-to-peer network that means there is no need for decentralized or third-party involvements to resolve or detect any cyber attacks. BlockChain treated a constantly expanding catalogue of documents, and this index of fields is called blocks. Blocks are interconnected with each other using a cryptographic hash. Blockchain is transparent and provides integrity-protected data storage. Once data is recorded in Blockchain, it cannot be changed until all subsequent Blocks of data cannot be changed. Each block contains Information on previous nodes. The attacker can attack by using malicious nodes in the network; these nodes should not communicate with other nodes until verification. BlockChain [11] provides possibilities to make a more secure M2M (Machine-to-Machine) environment without third-party involvement. Blockchain guarantees the tamper-proof (Transparent) storage of approved transactions among trusted nodes. Blockchain components include (unique code of block), cryptography, digital signatures (rules), P2P, and proof of work.

The proposed solution incorporated blockchain technology to compute the trust of IoT devices in smart buildings. We use the ID 3 algorithm to find the threshold value and compare the trust value of each node with the threshold value. Then we use the blockchain server, i.e., miner, to broadcast the threshold value into the whole network. We use the concept of a trusted list for storing the information of trusted devices. Moreover, the proposed model is time-driven and event-driven. It recomputes the trust scores, threshold values, broadcasts them when a new event occurs or after the specified time.

A. TRUST OBJECTIVES

Several cyber-physical social relations exist in smart building model layers on the IoT. These relations for human beings explored advanced services. For example, trust management is concerned with gathering data to judge a relationship of trust, trust relationship conditions, managing and reassessing trust. Following goals can be achieved by using trust management IoT in a smart building.

1) Trust Relation and Determination (TRD): Trust management offers a way for IoT in smart Building devices to evaluate the trust relationship and assist IoT in smart

Building devices to communicate and collaborate with a wise decision. TRD is concerned with all IoT layers in the smart Building system and plays a vital role in smart and automatic trust management [12].

2) Data View Trust: In the IoT in smart Building systems, data sensing and data gathering should be trustworthy. Trust management provides trust properties on a physical layer such as sensor awareness, precision, protection, trustworthiness and determination, data gathering, and competence [13]. The proposed solution incorporates blockchain technology to compute the trust of IoT devices in smart buildings. We use the ID3 algorithm to find the threshold value and compare the trust value of each node with the threshold value. Then we use the blockchain server, i.e., miner, to broadcast the threshold value into the whole network. We use the concept of a trusted list for storing the information of trusted devices. Moreover, the proposed model is time-driven and event-driven. It recomputes the trust scores, threshold values, broadcasts them when a new event occurs or after the specified time.
3) Data Combination and Extracting Trust: Large quantities of data in IoT in the smart building should be managed efficiently regarding trustworthiness, 3-D data process, confidentiality preservation, and precision. DCET is concerned with the network layer [14].
4) Data Communication and Interaction Trust: Data must be shared strongly. The authorized entity cannot access the data of any other entity during communication [15].
5) The excellence of IoT in smart Building services: The Internet of Things (IoT) in smart building facilities should be provided to the proper authorities at the appropriate time and place. QIoT in smart Buildings concerned with the application layer. But is required to support other layers similar to the application layer [16].
6) System Protection and Robustness (SPR): Trust management ought to contain cyberattacks to give IoT to smart building users [14].
7) Human-Computer Trust Interface (HCTI): Trust management offers a handsome level of usability. HCTI is concerned with application layers [17].
8) Individuality Trust (IT): The identifiers are well managed in the IoT in smart Building systems. It relates to all three layers and concerns with identity and privacy of data [18].

B. RESEARCH CONTRIBUTION

Cryptography and access control are widely used methods for the security of IoT in smart buildings. But these techniques have many limitations, e.g. fraudulent information, system high jacking. These methods are complex and non-homogeneous that can compromise the nodes. It can authenticate bogus information by utilizing valid cryptography. Access control is also used to secure the distributed systems by denying them access to unauthorized users. For IoT security, trust computation can be used instead of cryptography and access control. Trust management solves the problems mentioned above in IoT. In this system, devices shares trust among neighboring devices for communication. Following are the research objectives.

- The proposed system uses reputation and trust-related information for making a tamper-proof network. As a result, credibility and trust-related information are collected and distributed across the Blockchain network. Furthermore, implementation of a Blockchain-based trust architecture is done to maintain adequate security.
- Every node needs membership authentication for communication in the proposed scheme. Every device can communicate if it has the authenticity, rationality, and reliability of trust files and detail about each transaction.
- interactions and purchases are recorded in a hybrid (Time and Event) manner to collect trust-related information. Then, a trust manager is used to aggregate and compute the final trust score and accumulate the degree of trustworthiness.

The Rest of the paper is organized into different sections. section II describe the Related Work, Section III represent the Proposed System. The section IV describe the Performance and Evaluation of the model, section IV-I represent Discussion and section V represent Conclusion of the study.

TABLE 1. List of abbreviations.

Acronyms	Abbreviation
IoT	Internet of Things
IDS	Intrusion Detection System
HIDS	Host Based Intrusion Detection System
NIDS	Network Intrusion Detection System
P2P	Peer to Peer
M2M	Machine to Machine
TRD	Trust Relationship and Decision
DPT	Data Perception trust
DFMT	Data Fusion and Mining Trust
DTCT	Data Transmission and communication trust
QIoT	Quality internet of things services
SSR	System Security and Robustness
HCTI	Human Computer Trust interaction
IT	Identity Trust
BIM	Building Information Modeling
LCA	Life Cycle Assessment
HVAC	Heating Ventilation and Air conditioning
KNN	K-Nearest Neighbor
BLE	Bluetooth Low Energy
NLM	Novel Localization Method
POW	Proof of work
POS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
RR	Round Robin

II. RELATED WORK

Panteli et al. [19] discuss the various stages of Building Information Modeling (BIM) in smart building applications. They talk about how BIM is used throughout the design, construction, and post-construction phases. In the first level

of their study, they prioritize BIM implementations during the pre-construction period, focusing on BIM during the design phase. They performed a list of the best activities used in 4, 5, and 6D architecture. The second phase of their study focuses on power assessment, pollution measurement, planning, and management of human comfort and waste. Finally, the scientific advances in construction architecture, optimization, and environmental evaluation of building design are explored using LCA and BIM. The post-construction applications of BIM are also discussed in this study. In the post-construction phase, they discuss the integration of IoT in smart buildings with BIM. A case study was used in this article to give an overview of BIM in reconstruction projects. Various challenges related to BIM integration models, data interoperability, energy performance of building information modelling simulation are also discussed in this article.

Siountri et al. [20] talk about how Blockchain, BIM, and IoT are being used to design smart buildings. The use of cutting-edge technologies like BIM, IoT in smart buildings, and blockchain for the construction industry is the main topic of this study. This study examined how Blockchain, IoT, and Building Information Modeling (BIM) technologies may work together as complimentary innovations to improve IoT in smart Building services and secure data processing and storage for building operations. They explore the interconnection and interoperability of these technologies on a proposed building (museum) network infrastructure. The proposed building used efficient storage and security mechanism, maintenance, and surveillance. These factors are seen as essential to the unhindered functioning of this host organization in this article.

Carli et al. [21] study on the use of IoT in smart buildings. HVAC (heating, ventilation, and air conditioning) system analytical management using a model for smart buildings. In order to predictably regulate HVAC systems, this study proposes an interior thermal comfort and energy use optimization architecture. The HVAC control method is seen as an overall framework for a real-time environment. In this system, on the one side, to comprehend HVAC automated control in a specific network, they offer an IoT in innovative Building-based general structure. The MPC optimization problem for efficient HVAC management, on the other hand, has been established. IoT in a smart building network consists of various parts like sensors and devices, a firewall, a DBMS server, a monitoring panel, and an internet protocol control panel.

The measurement and control details are maintained and retrieved from devices, control units, and dashboards from/to the database server. Because of dashboards, any user can customize the comfort and control the system's various modes. Their suggested MPC process was dependent on an indoor and linear variant of the thermal comfort index of the tractable dynamic thermal model. The optimization problem posed here, in particular, offers sufficient control acts to maximize thermal environment, energy consumption, and controller vector angle variance all at the same time, resulting in a modular non - linear quadratic equation. Their achieved results indicate that the method is simple to use, and the underlying control algorithm is efficient. Furthermore, indoor comfort is ensured, and significant energy reductions are gained compared to conventional control methods utilizing traditional thermostats because of numerous disruptions. The limitation of this study is that ''there are no-cost analyzes of both power and deployment of the emerging IoT in smart Building-based control platform for HVAC systems.''

Casado-Vara et al. [22] presented IoT in smart building network network slicing on virtual homogeneous data layers for smart buildings. This study examined the imprecision of IoT in smart Building network algorithms by utilizing heterogeneous data. This study uses clustering methods and complex networks; the heterogeneous data is virtualized into comparable data. This step optimizes the performance of the algorithm. Furthermore, the algorithms ensure optimum efficiency for the different topology areas of the IoT in smart Building networks utilizing the virtual segmentation technique given by the latest system. Finally, the efficiency of the proposed IoT in the smart Building slicing process is demonstrated by a case study in this article.

Sadowski et al. [23] proposed memoryless and wireless techniques for internal localization. They evaluate and compare K-nearest and Naïve Bayes techniques. In this article, they discuss The use of Trilateration in an indoor localization system. The various experiment has been done in three multiple rooms with differing levels of interference. The performance of models was compared based on accuracy, precision, and recall. They did various experiments with three technologies, i.e., BLE, Zigbee, and Wi-Fi, to verify results. The results of this article show that KNN outperformed other models when k=4. KNN and Naïve models have high running time with O(mn) complexity. Trilateration seems to be the worst technique in this study, having the time complexity of O(2), taking relatively a brief period to measure a location. The findings of this study can be used in smart buildings as an indicator for choosing a suitable technique for indoor localization.

Akkaya et al. [24] surveyed on current IoT in smart building related design strategies for intelligent, energy-efficient structures. This paper discussed various existing techniques used for occupancy monitoring in smart buildings for energy efficiency purposes. In addition, they identify multiple problems in existing processes related to people's occupancy. Finally, with smartphones, motion sensors, and Wi-Fi APs, they investigated the current efforts where IoT in the smart building comes into the picture. The current technologies revealed a trend towards the use of existing IoT in smart Buildings inside the buildings. Intending to use minimum hardware/software expenses, future smart buildings have enormous potential to save energy through innovative control strategies on HVAC.

Lin et al. [11] proposed a novel technique called LNM. This method uses in smart buildings; the NR signal fingerprint and Markov chain are used to localize. They utilized a neighbor's relationship method for their suggested fingerprint radio construction and localization systems. Their suggested solution offers stable and accurate localization accuracy in the face of interface heterogeneity and dynamic environmental factors. During the study, they perform various experiments by using different smartphones. The experiment results show that LNM is feasible and reliable. The proposed LNM can produce optimal localization accuracy with an average error of around 1.5 m. The LNM outperforms other existing technologies like RADAR, Zee, and WILL. Since LNM can identify in actual time with high correctness, it has achieved a sophistication point that allows for the practical application of IoT in smart Building localization applications and services. Moreover, it has the ability for wide-scale implementation in IoT scenarios such as smart buildings.

A. CONSENSUS OF BLOCKCHAIN

A consensus algorithm is a process that enables all Blockchain network peers to consent to the status of the public ledger. In a distributed computing system, consensus algorithms improve network stability, and foster trust between unknown peers [25]. Indeed, according to the consensus procedure, each new block introduced to the network is the first and only iteration of the version on which all Blockchain nodes accept [26].

In the blockchain, some consensuses are being used for the security and performance of the blockchain environment. Therefore, various techniques are implemented in previously extended agreements among them.

1) Proof of Work (POW)
   The POW is used for transactions and creating new chain blocks in the Bitcoin network and other cryptocurrencies. POW miners compete against one another to solve complex programming problems and are rewarded for their efforts [27].
2) Proof of Stack (POS)
   We can use POS instead of POW for environments where we have less CPU power. For the time being, they store as many currency forgers as possible to have the best chance of making the next brick [28].
3) Practical Byzantine Fault Tolerance (PBFT)
   The principle of this consensus is to repeat the process to accept complex failures. Every entity transaction attempt to double expenses if it considers the transaction. The definitive decision is made by a majority vote and take into account up to three dishonest Byzantine replicas [29].
4) Round Robin (RR)
   Another one is the round-robin consensus technique. This allows organizations to create suitable blockchain by building blocks in a circular pattern. More precisely, the amount of blocks that one item in a time frame may create is limited and is determined by a network parameter called mining diversity, which also controls how many blocks must pass before a miner can try again [30].

III. PROPOSED SYSTEM

Figure 1 represents the conceptual framework that indicates that these should be the minimum requirements for developing trustworthy and dependable trust models in the IoT setting. An IoT trust model aims to identify, evaluate, and transfer trust across diverse connected devices. In order to build trustworthy and accurate trust models, IoT configurations must meet some minimal design criteria. Figure 6 depicts the structural design of the study for an IoT trust model. Two or more trust entities must be represented as trustor and trustee nodes in a trust model. There are trustors—entities that create trust—and trustees—entities that create trust. In order to establish trust and/or share information with other entities about their trust experiences with a node, other entities, such as observers and/or recommenders, may watch a node's behaviour. Direct or indirect data collecting might be used to create a trust. For trust calculations, the direct method solicits data and recommendations from other nodes functioning as observers or recommenders. In contrast, the indirect approach uses additional nodes that function as observers or recommenders for trust calculations to gather information and ideas. One of two kinds of nodes may exist in an IoT system. Type "A" nodes are able to determine trust independently, but type "B" nodes are unable to do so because of resource limitations and must rely on other nodes.

The trust model deployment might be decentralised or centralised. In a centralised system, a central node in charge of all trust generation, creation, and propagation activities is given the job of trust calculation. In contrast, each node on the network manages its own trust generation and dissemination processes in a decentralised configuration. A decision-making or evaluation technique may be used to develop trust models in unique situations. As trust must be renewed over time since it is constantly dynamic. This trust update might be event-driven, time-driven, or continuous, depending on the model or environment in question as well as its context and level of complexity. The trust model recognises three different forms of trust: single trust, distinct multitrust, and combined multitrust. It demonstrates the breadth of trust-building techniques used to a particular organisation. To determine trust, one trust assesses only one trust characteristic. While combined multi-trust employs a weighted aggregation of trust characteristics to calculate trust, distinct multi-trust uses trust features and metrics with their associated trust thresholds. Trust properties are the characteristics or traits of a trustor or trustee node that are presumptively used to create trust. Honesty, cooperation, benevolence, expectancies, and belief are examples of subjective properties, while reliability, competence, assessments, and standards are examples of objective attributes. Because trust is mostly dependent on the context or circumstances in which it is formulated, context is regarded as

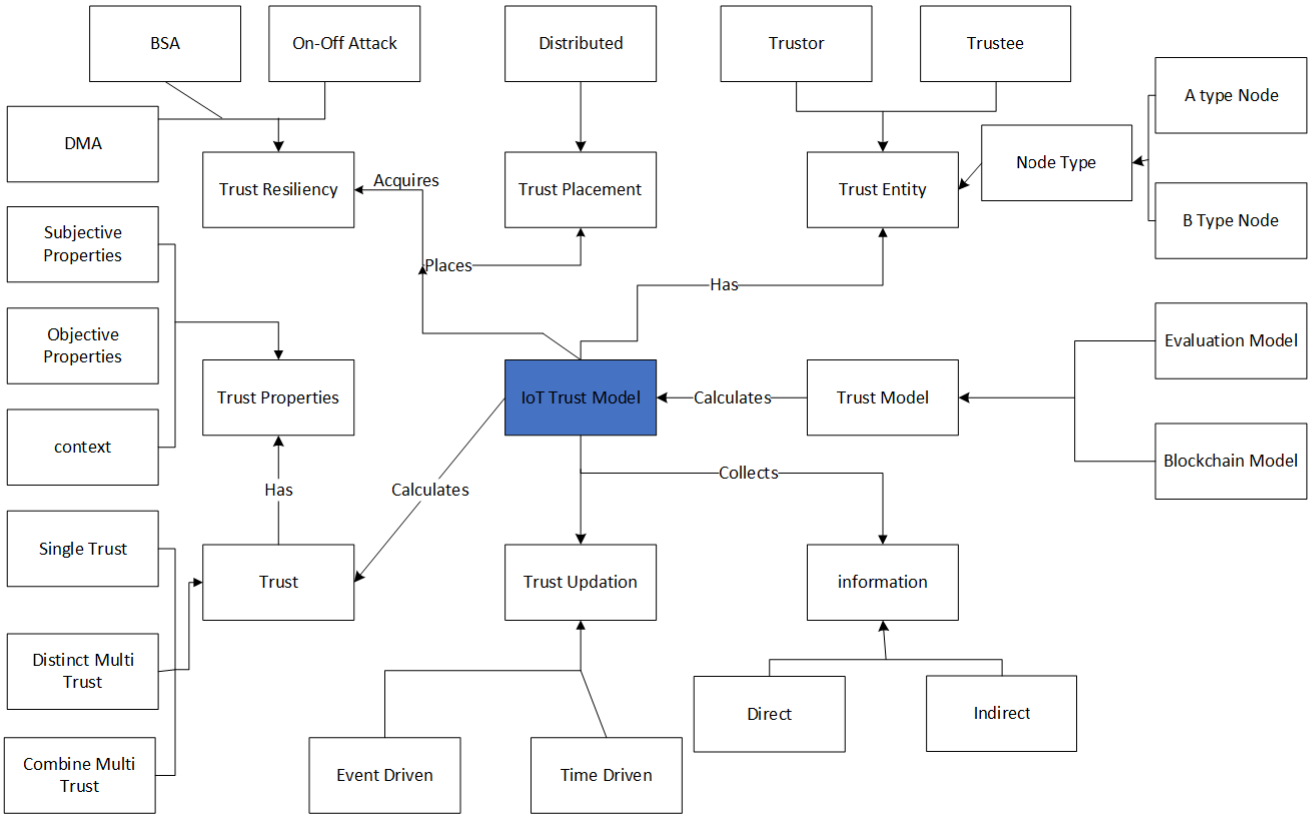

FIGURE 1. Conceptual framework for IoT trust model: In this model various Trust components are discussed.

the most significant trust quality. The trust model also makes generalizations for nodes and initial settings, like ''nodes will offer correct recommendations'' or ''starting trust values are known in advance.'' Moreover, based on the environment's complexity, the trust model designed for IoT settings must fulfill one or more functional criteria. These features and functions include node dynamic behavior, device heterogeneity, and resource limits. Finally, the proposed trust model must be put through its paces and made resilient against service threats. There has been a list and description of service attacks in the IoT context.

This study's main goal is to plan a new trust management system based on blockchain technology and a machine learning model. Our platform intends to create and calculate a trust values for each node, as well as safely store and disseminate these ratings across the IoT network, ensuring transparency, integrity, authenticity, and authorisation. The overall architecture of our suggested scheme will be described in the following sections. We must first understand the exact structure of our system in order to correctly compute trust values and securely store and process them inside the blockchain environment. A brief overview of the needed behaviors will also be provided.

A. SYSTEM MODEL

Our proposed system consists of many smart buildings where IoT devices are installed, these devices may include, i.e., common actuators, sensors, computers, IoT (Internet of Things) nodes, etc.). There is a verification manager is also working to verify device characteristics, to make access control decisions, and producing access control tokens, etc. Additionally, each IoT device on the smart building is also attached to a trust manager, who is responsible to compute each related device's degree of trustworthiness as well as evaluating and computing a complete trust value. The blockchain system, which is composed of an ordinal scale of believed that the number along with every block mentioning the one before it, known as the parent node, and stores trust data, is then implemented to receive trust values, create components out of all of this, and transmit it there. This enables trust data verification. the elements that support each entity in the proposed system as well as any possible relationships between them. The next section has further details.

B. PROPOSED SYSTEM ARCHITECTURE

Our proposed system consists of three conceptual layers.

1) IoT LAYER

Devices from the Internet of Things (IoT) that collect and analyse data make up this layer. Measurement tools, controllers, RFID readers, computers, robotic systems, and other apparatus fall under this area. Requesting and acquiring data (e.g., area, elevation, moisture, and other primary jobs), as well as executing tasks as well as other primary activities, are among their main responsibilities. These devices will

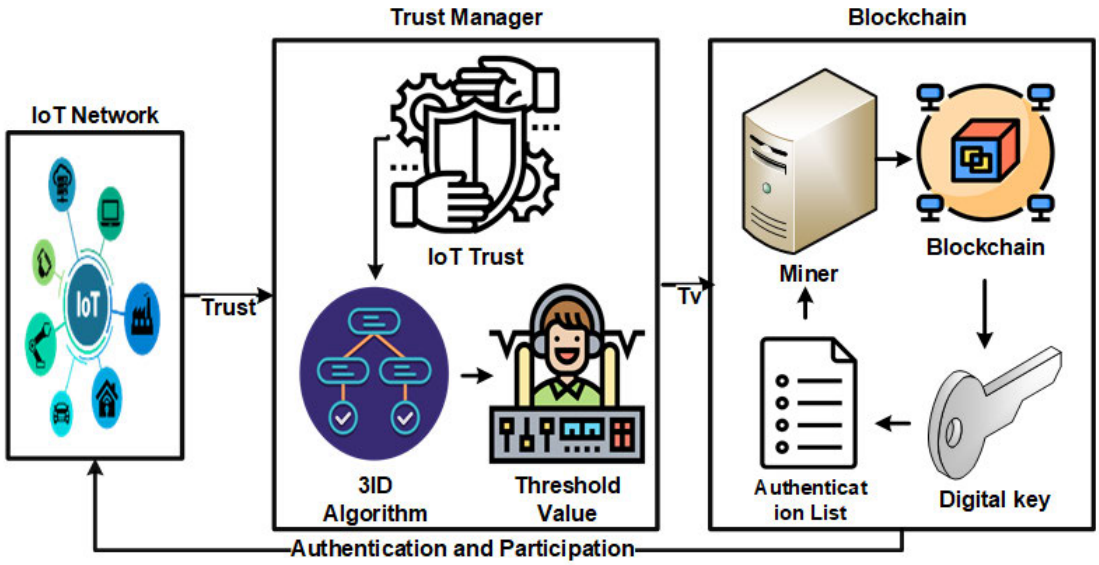

FIGURE 2. A layered model of IoT in which different layers communicate with each others.

carry out extra trust management tasks that are exclusive to and pertinent to our suggested system. They will be able to communicate, analyse, and collect information about the trust from the management system. On the basis of their quantitative trust scores, which are generated, processed, and maintained by System management, these are additionally connected with other services via the Internet to learn about and monitor their status as well as any pertinent data. To achieve this, each device will evaluate their behavior throughout the engagement using measures such as packet delivery ratio, collection of people, and the truthfulness with which recommendations are credited after speaking with other devices. These indications will be discussed in further depth in the following section. The assessment result will be sent to the trust manager entity, which will calculate the corresponding trust value and send it to the blockchain environment after authentication.

2) TRUST LAYER

This layer is made up of linked cutting-edge hardware components that are in charge of safeguarding the setup, functionality, and dependability of the suggested scheme. Particularly for this layer, data computations, authentications, and analyses linked to trust are performed. Additionally, it offers details on acts affecting trust and reputation scores that are safely archived and indexed in a decentralised environment, allowing for their usage at a later time as required or desired. The final action is propagated through a blockchain network of consensus objects to make sure it has been validated, audited, and confirmed. The layer is also in responsible of preserving each Node's action keys for data access under general system trust and authenticating each Node.

- **IoT Devices Trust Manager**: With the help of this device, a safe and reliable environment can be established where devices may connect with one another and with for-profit IoT services without worrying about the integrity and veracity of trust scores being jeopardised.As a consequence, people may make reliable judgments and get information based on the assessed levels of trust. A relationship of trust exists between two nodes: a trustor, who is the assessor, and a trustee, who is the assessed. This connection is restricted to a present value, i.e. the period during which the evaluation occurred. Furthermore, direct observations and exchanges, referred to as direct trust, and recommendations given between neighbors, referred to as indirect trust, are used to establish this link. In this case, trust can be characterized as a link between three parties: the trustee, the evaluator, and the assessed trustor. This relationship is based on the value of time used to assess a node. The connection between the trustor "tr" and trustee "ti" at a certain time "n" was described by the following variables: trust(tr*ti)t. The value T ti(t), which denotes the trust value of any device "a" for any other device "b," is assigned to this relationship. The range of this trust rating is -5 to $+5$, with -5 signifying complete ignorance and $+5$ signifying absolute trust. The suggested model includes a cyclic sequence of numerous processes, as shown below. 1) Direct observations of packet delivery behavior and suggestions from nearby entities are used to gather trust-related data. 2) Each individual's trust was calculated, specifically the Direct and Indirect trust. Direct trust was measured based on entities' cooperativeness, knowledge, and a group of interest, with each computation focusing on numerous traits and factors. The entities' integrity was measured against the published suggestions to determine indirect trust. 3) By combining these qualities with earlier trust evaluations throughout time, an aggregate trust score

may be calculated to reliably and simply maximize protection within the framework in issue. We combine the most recent trust assessment with prior ones done during the time period "t" to generate a final trust value weighted average of two components, as shown in Equation 2.

$$T_ab = tri1 * (T_ab)(t-1) + tri2 * (T_ab)(\Delta t) \quad (1)$$

Delta t was assigned the threshold values of $tri1$ and $tri2$, where tri1 + tri2 = +5. The entity's behavior is always changing, any entity manages trust properties relating to the neighbors with whom it communicates, such as cooperativeness, capacity, and a group of attention, where (x) The system to work property represents entity e's cooperativeness level as defined by entity exy through action observation over the time span [0....t]. Throughput is calculated by dividing the number of successfully transmitted packets by the total number of packets being sent by the transmitter. (ii) The aptitude things determines the level of an individual's skill to carry out its planned functions, which is assessed using the entity's energy and computing capability to determine whether it is capable of carrying out its responsibilities. It is measured in terms of throughput, which divides the number of successfully transmitted packets by the total number of packets sent out by the sender. (ii) The aptitude property determines the level of an individual's ability to carry out its planned functions, which is assessed using the entity's energy and computing capability to determine whether it is capable of carrying out its responsibilities. The community interest factor measures the degree of mutual interest or related activities as a percentage of their shared community values over the whole amount of their common interests.

C. MACHINE LEARNING ALGORITHM

Following trust computation, we store all trust in an array. We utilise a machine learning method to classify the trust after putting it in an array. We used a decision tree and the ID3 approach to determine which device had the most trust among the others. Ross Quinlan developed ID 3, which is a top-down greedy technique. The ID3 algorithm is a supervised machine learning method that chooses the best feature that produces the most Information Gain or the lowest amount of entropy in order to build a decision tree. Information theory uses entropy as a metric for impurity or uncertainty in a collection of data. Information gain is defined as the amount of knowledge obtained by a characteristic about a category, and it describes how data is split by a decision tree. Information gain may be used to decide how the features are arranged in a decision tree's nodes. We denoted the array as a 'En' letter.

$$entropy(En) = (-p)/(p+n)log_2(p/(p+n)) \\ -n/(p+n)log_2(n/(p+n)) \quad (2)$$

The entropy is depicted in this equation. The array/dataset is denoted by the letter E. P denotes a positive value, while n denotes a negative value. Then we choose the node with the maximum entropy. It is the value that we use as a starting point. The ID3 method is a supervised machine learning strategy that chooses the best feature with the maximum Information Gain or lowest amount of entropy to build a decision tree using a greedy approach. Entropy is a measure of impurity or uncertainty in a set of data used in information theory. It specifies how data is divided by a decision tree, while information gain is defined as The amount of knowledge gained by a characteristic about a category. The arrangement of features in the nodes of a decision tree may be determined via information gain. The calculated trust of all nodes is stored in an array of values. These values are given to the ID3algorithm that is trained on trust values. The ID3 generate a decision tree of nodes based of the trust values. The value of root node of generated tree will be considered as the threshold value for the network

D. AUTHENTICATION OF THE DEVICES

This device is in charge of evaluating device IDs and the integrity of requests and requirements delivered to both trust information management and storage systems. Using the credentials provided, IoT nodes and smart devices are authorized. We use OIDC (OpenID Connect), an authentication component placed on top of the OAuth 2.0 protocol, in my system. It allows customers to use an OpenID Provider to validate the node and receive basic device profile details in a REST-like approach. We chose OpenID Connect because it possesses a number of characteristics that are relevant to Scenarios. OIDC is a free, open, and decentralized database (relying parties and service providers are not approved or registered by a central body). Its installation does not necessitate a lengthy software upgrade. It does, in fact, adopt a laid-back demeanor that makes it simple to use and interact with. Furthermore, a JSON structure token with device-specific data can be used.

E. MINER

This entity is in charge of examining trust records and transaction data to ensure their security, reliability, and validity. This will be sent to the network of miners, who will verify its legitimacy before putting it into a block that, if received, will be linked into the ledger. Our design makes use of multichain blockchain technology, a private blockchain protocol that controls block access via a list of registered players. Those who have signed up already have access to the database's reading and writing blocks. We choose Multichain primarily because it meets the vast majority of our requirements. A permissioned private blockchain is Multichain. The independent append-only collection of objects known as streams makes sure that shared data is kept more secret. Second, it stands out for its versatility, which allows for changes in authorization and delegation. Third, it is based on the RR consensus mechanism, which requires no complex computation resources in terms of processing capabilities, computing power, or time for block validation, let alone currencies, unlike bitcoin-based solutions, which require miners to perform compute -

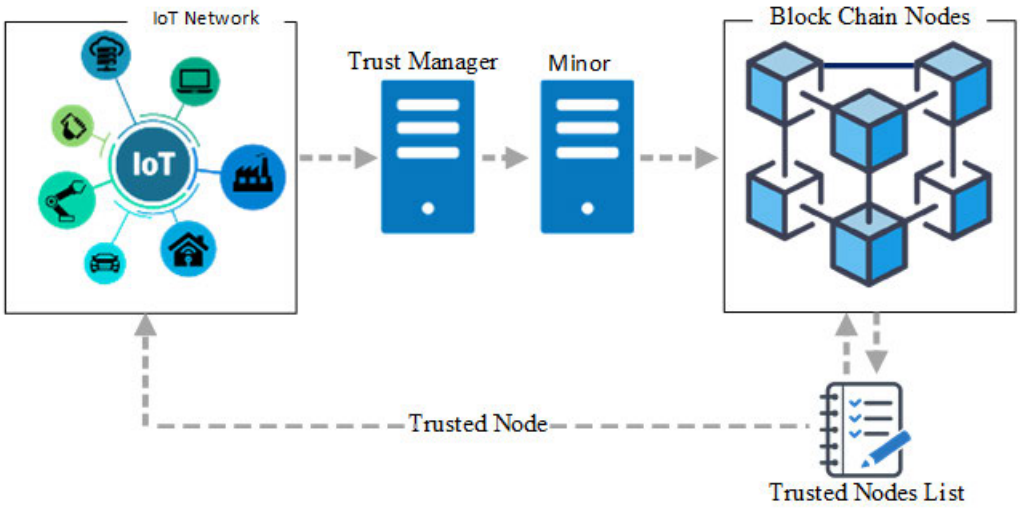

FIGURE 3. Interaction of different components of the proposed system.

intensive calculations utilizing their computational power in order to confirm new blocks and append them towards the blockchain.

In our scenario, an IoT node will use the Blockchain network to store trust scores. The device requires a valid authorization credential to gain access to the system at the initial stage. This entity is working in a distinct and additional commanding network node in the case of resource-limited IoT devices, whereas it is expected to be a component of a more powerful device in the case of a more powerful device. The trust management entity will be in charge of employing the formulae to calculate the Reputation score as well as an overall trust score. The transaction is relayed to the entire network once it has been received by the miners, where each entity validates the transaction's legality before collecting confirmed communications into a block to be added to the current ledger.

The proposed model structure is illustrated in Figure 3. There are Five main components in it, i.e., IOT devices, Trust manager, Minner, Blockcahin nodes, Trusted node list. The devices are located in the IOT network, Trust computation and broadcasting is done in the trust manager, Minner and blockcahin components, while trusted devices information are saved in the trusted list. Assume the trust in IoT in smart Building devices ranges from -5 to +5. Initially, we gather the trust of each IoT in smart Building system and store it on the trust manager server. The trust of all systems is held in an array by the trust manager. The calculated trust of all nodes is stored in an array of values. These values are given to the ID3algorithm that is trained on trust values. The ID3 generate a decision tree of nodes based of the trust values. The value of root node of generated tree will be considered as the threshold value for the network. This threshold value is saved in the trust manager and sent to another server named the miner, where it is broadcasted through the blockchain network. When a node joins the network, the trust manager server calculates the trust value and compares it to a threshold value. If the new node's trust value matches the threshold value, it is passed to the blockchain host, i.e., miner. The miner broadcasts the node into the blockchain network, where its trust is validated against the threshold value once again. If it meets the threshold value it is stored into the trusted devices list. After a specified time, interval, the trust value of all IoT in smart Building nodes which are already part of IoT in smart Building network is evaluated and stored into trust manager and new threshold is determined. Again, this threshold value sends to miner and miner broadcast this value into blockchain network. After new broadcasting of threshold values into blockchain network that threshold value and listed node check again their trust with new threshold value if meet then system allow it for making transaction.

F. COMPLEXITY OF SOLUTION

The network's intricacy is what gives blockchain its charm. The greater the number of participants involved in a transaction, the more widely applicable the blockchain will be. A single block hash value links the blockchain; however, this connection is unidirectional, making it impossible to find a prior block unless a later block discovers it. In order to identify the preceding block using this hash value, and so forth, the standard retrieval technique first acquires the hash value of the end-of-chain block from the end-of-chain file. The complexity of its sequential search time is O(N). The chain will continue to grow as new blocks are continually created and added as blockchain technology is used. The number of blocks will increase steadily over time. This sequential retrieval method's effectiveness will drop very quickly. In extreme situations, it may result in protracted operation, impairing the system's functionality. The number of iterations in constructing a blockchain-based trust management system might be exponential. A straightforward

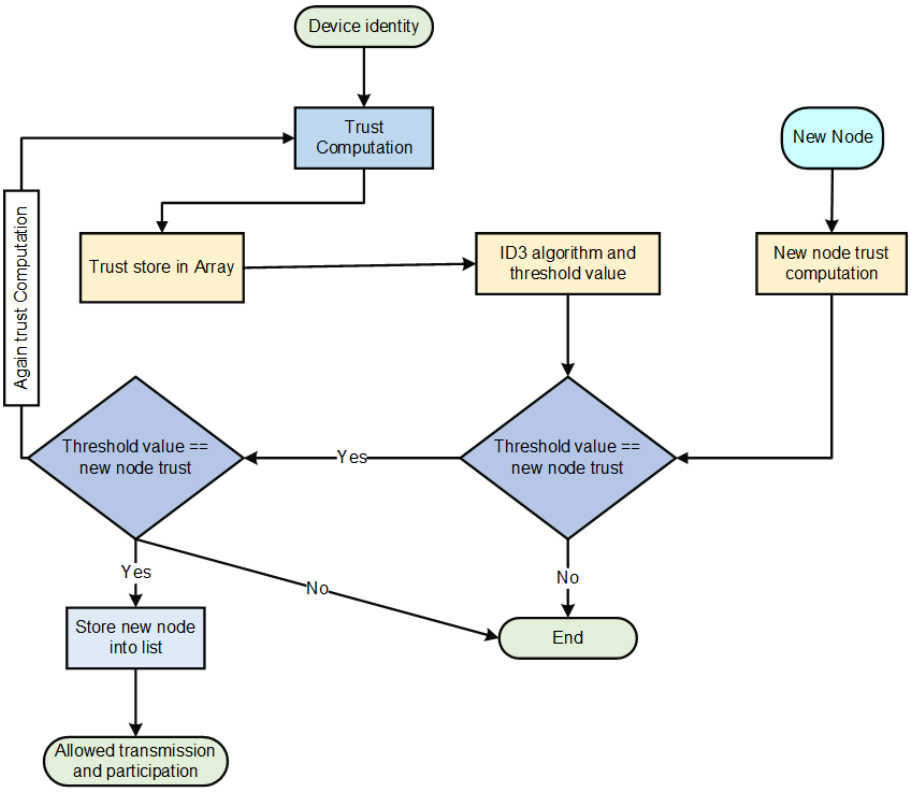

FIGURE 4. Flow diagram of the entire model.

TABLE 2. Simulation environment settings.

Simulation parameter	Values
Simulator	NS 3.29
Simulation Run Time	2.5 hours
Nodes Distribution	Random
Total number of nodes	30 100
No.of compromise Node	20% to 40 %
Trust Update Time	500s
Starting trust value	1.0
Trust interval	0..1
Poor witness nodes (%)	20%
Malicious assisting nodes (%)	10%
Type of traffic	Multimedia/messaging
Packet Size	Constant

implementation will have an O(n) time complexity if there are m transactions with n nodes each.

IV. PERFORMANCE AND EVALUATION

The experiments are carried out on an HP envoy computer running the Linux operating system Ubuntu 18.04, with a 8th generation Intel Core i5 CPU and 8 Gb of RAM for the multichain network. The proposed system is developed using the industry-standard simulation tool ''NS3''. It is a widely used discrete network simulator that was created mainly for educational and research purposes. A smart building with IoT devices is designed and tested using this tool. With different smart building devices ranging from 30, 50, 70, 90, and 100, an IoT in a smart building environment is taken into consideration. Due to the fact that the devices belong to the same category, have similar values, or carry out similar functions within the network, the system distributes confidence in the blockchain network at random. The number assigned to each device ranges from 0 to 10. These values signify a device's affiliation with one of the network's 10 recognised communities of interest. Additionally, one, two, or three civilizations may exist simultaneously. A variety of malevolent devices, which make up 20% of all network devices, are also present in the unsafe model. The lifespan of the start network determines how these devices behave initially. The proposed model primarily investigated three kinds of attacks that are discussed below:

A. BAD MOUTHING ATTACK

It is a specific form of attack in which compromised or untrusted nodes try to damage or degrade the integrity of other trustworthy devices by making false recommendations against them. By this, they decrease the trust value of trusted nodes in any IoT network in a smart buildings.

B. BALLOT STUFFING ATTACK

Unlike the previous attack, malicious nodes in this attack motivate other malicious nodes by giving them favorable opinions about themselves, increasing their probability of being trusted.

C. ON-OFF ATTACK

In this case, as its name suggests, the malicious node alternately acts well enough and badly. It could, therefore,

probably throw out an attack until the trust mechanism is aware of it.

The multichain network is implemented and established with the functionalities of miners inside the blockchain network. Trust Value Computation: The ability-based trust value of the resources is determined utilizing criteria such as accessibility, dependability, and trust values. The efficiency of turnaround and resource value in terms of reputation. It produces a graph of reputation performance. The size of the trust information determines the ratio of active storage transaction data in the multichain network. To do so, we measured the percentage by adding the total amount of known transactions to the number of successfully processed transactions. The proposed technique performs well in terms of effective storage transfers by scoring a good throughput. The followings are the parameters for evaluation.

D. RESPONSE TIME

A packet's transit time over a network route from a sender to a receiver is measured as network latency, also known as network reaction time. The performance may be impacted by network route delay. The metrics for comparison were typical platform response times relative to devices count and error rates in user request responses.

E. ENERGY CONSUMED

All energy needed to carry out an activity, create something, or just occupy a structure is energy consumption. Additionally, it displays the network's IoT application burden. It impacts energy use since an increased workload might result in higher energy use. A unique loT environment with just wireless sensors and QoS trust metrics like packet forwarding/delivery ratio and energy consumption is taken into account by the trust management model.

F. SUCCESSFUL PACKET DELIVERY

The ratio of the total number of packets received at destinations to the total number of packets sent from source nodes is known as successful packet delivery. Generally speaking, throughput indicates the average speed at which a data packet is successfully transmitted from one node to another via a communication network. The following function may be expressed in bits per second: where denotes the number of delivered packets and denotes the size of a packet.

We analyze the suggested scheme's effectiveness and dependability against various attacks. The results of the study are divided into three parts. In the first, phase the resiliency of the proposed model is evaluated against compromise actions. The feasibility of our blockchain network storage and sharing strategy is then evaluated by measuring the overall reaction time, the number of transactions and computing services used by each group involved in the mining activity.

G. RESILIENCE IN THE FACE OF ATTACKS

This section investigates the vulnerability of our proposed architecture to destructive attacks initiated by various devices

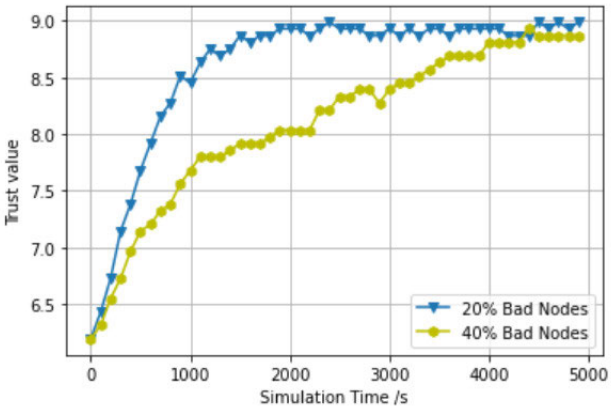

FIGURE 5. Comparison of well behaved node trust evolution.

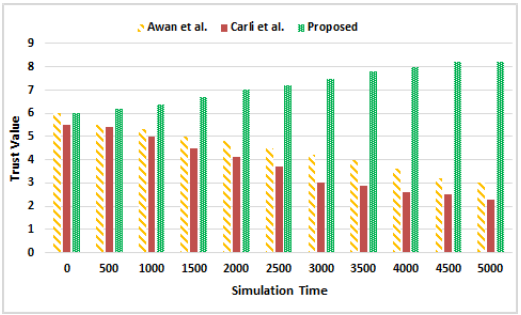

FIGURE 6. Malicious node trust evaluation.

inside the IoT network of smart buildings. Second, we calculate the overall trust value of a well-behaved system when altering the cumulative number of malicious nodes that launch bad mouth attacks as shown in Figure 5.

Figure 6 evaluate the malicious node's trust value as the percentage of accumulated poor nodes initiating On-Off Attack and ballot stuffing attacks. An on-off attack occurs when an attacker node alternates between good and poor packet transmission performance. To be more precise, in order to achieve high trust ratings, the negative node sends packets at the required duration. The proposed solution is compared with existing solution, i.e., Awan et al. [14] and Carli et al. [21]. The results shows that the proposed solution has higher trust value than the existing approaches. When it comes to the effect of the number of malicious nodes, we discover that when this ratio is more, the trust levels fluctuate, meaning that more malicious nodes collaborate to support the bad node and rapidly push the trust level up.

The findings of trust value against number of IoT nodes is illustrated in Figure 7. Assume that each node computes a new score based on previous and historical trust assessments. This is shown that how blockchain technology can increase the trust value and reliability of a network with on-off attacks as compared to previous approaches. The blockchain has traceability feature, in which trust information is time-stamped and securely stored in the database for future use. For example, by monitoring and analyzing past trust scores, we can detect some other malicious activity and,

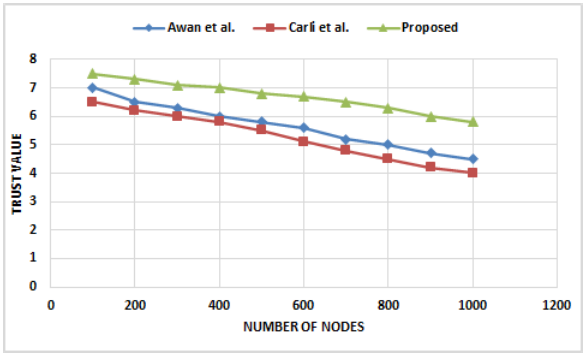

FIGURE 7. Trust computation with varying number of nodes.

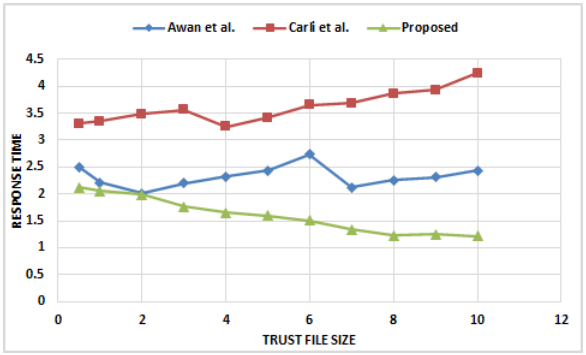

FIGURE 8. Average response time.

as a result, penalize and discourage the malicious node from reaching high trust scores in the future.

The size of the trust information determines the ratio of active storage transaction data in the multichain network. To do so, we measured the percentage by adding the total amount of known transactions to the number of successfully processed transactions. In terms of effective storage transfers, the proposed technique performs well by scoring a good throughput. The response time is determined by varying the file size containing trust information and trust scores for each analyzed device in the network. The average wait time of the blockchain network generally increases to the extent of the trust information list, as seen in Figure 8. In this process, we evaluated the computational resources needed by the miners to manage incoming requests and transactions to determine the performance of the proposed methodology, its applicability and importance in IoT environments. We compared the response time of the proposed work with Awan et al. and Carli et al. and the result shows that the proposed technique has less response time than other schemes. When there are number IoT nodes communicating with each other to share different files, we can compute the energy required to make this process successful. Figure 9 compares the energy consumed for different trust file sizes. As the trust file size increases the energy consumption is also increases. The results show that the proposed solution energy consumption is less than other approaches.

In order to do this, we keep track of when a successful transaction confirmation is received as well as when the trust information file is transferred for storage within the

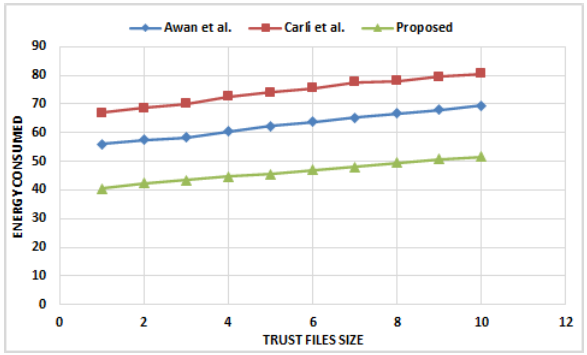

FIGURE 9. Energy consumed with trust file size.

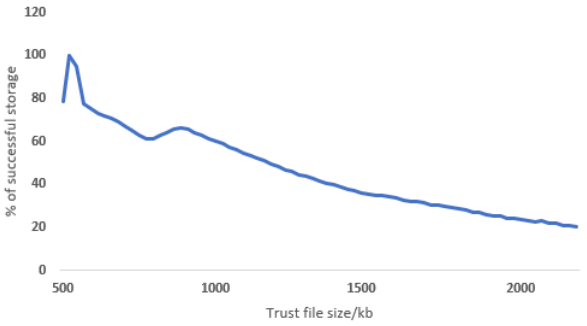

FIGURE 10. Success full transaction.

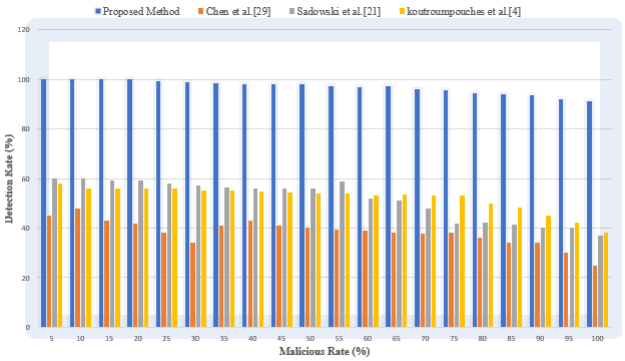

FIGURE 11. Successful detection rate.

blockchain network. The results show that for a 512Kilobyte trust file size, this calculation and communication take 750ms to complete, and 35 percent of CPU and 0.016Gb of RAM consumption is needed for transaction confirmation, block formation, and incorporation into the blockchain network. This shows and proves the deployability and viability of blockchain technology to IoT environments. Figure 10 illustrates the proportion of active storage transactions completed in the multichain network as a function of trust information file size. Comparing the total number of known transactions to the number of successfully executed transactions yields the resultant ratio.Thus, as seen in Figure 10, the proposed technique is helpful in terms of storage transactions.

H. COMPARISON

Figure 11 indicates that our approach improves Chen et al. [31], Sadowski et al. [23] and koutroumpouches et al. [5]

approach 's in terms of successful detection rate, even when 100 percent of malicious nodes are present. Block chain trust performs well, with a successful detection rate of 100% if the malicious rate 20% and 90% if the malicious rate increasing the 20%. Our 2-layer architecture achieves these results by ensuring a global view of trustworthiness over the whole network with only a few exchanges, allowing it to deal effectively with high mobility scenarios

I. DISCUSSION

This section looked at how well our suggested architecture handled on-off and bullet stuffing assaults, reaction times, computing resources, and transaction processing. Our analysis of these factors showed that our strategy is more attack-resistant than the straightforward one without blockchain. This occurs as a result of the traceability feature of blockchain technology, which permanently stores both trust information files and established transactions within the ledger. This feature allows our framework to provide a comprehensive view of entities' prior behaviour, which may be useful for anticipating the behaviour of harmful entities in the future when initiating a spec. Furthermore, we evaluated the reaction time necessary to process storage and transactions in order to show the blockchain's suitability inside such a paradigm while fully preserving the design goals we first stated. Additionally, we showed that even with increasing file sizes, this last stays minimal, supporting the goal of real-time review. The security of smart buildings has not yet been implemented using the blockchain. Blockchain, on the other hand, has been used to improve the security of smart devices in intelligent buildings. Overall, the suggested approach improved IoT network security.

J. TRADE-OFF ANALYSIS

A participatory technique called tradeoff analysis (TOA) integrates foresight analysis with simulation modeling tools from the Internet of Things framework, including economics, to make and assess future-looking, strategic choices in complex systems with high degrees of uncertainty. With a prototype framework for designing and assessing a blockchain-based framework for IoT-based sustainable development. We go through the benefits of a blockchain-based architecture for managing trust in smart buildings that gather node trust evidence. Each node is given a trust score, securely stored in an array, and the ID3 Algorithm is used to calculate the threshold value. The blockchain network receives and stores the IoT threshold value in the trusted list. The results show that our strategy includes security measures for IoT in smart buildings, such as tamper-proofing, attack resistance, dependability, and low functionality. The proposed solution justifies the tradeoff between the traditional approach and the proposed approach as follows: If there is 1 invalid transaction in the block, for Nval = 15, each validator should validate at least 18 transactions so that the probability of not detecting the invalid transaction in the block is less than 0.001. There is a tradeoff between the computational cost of block validation and the probability of a successful attack by a malicious gateway Our findings demonstrate that, in the context of false recommendation attacks carried out by malicious nodes, a tradeoff occurs between the precision of trust assessment and the speed of trust convergence. With the help of blockchain-based service composition, we show the usefulness of the suggested trust management framework. Our findings show that blockchain-based trust computation performs noticeably better than non-blockchain-based trust computation, and its performance is close to the highest level that can be achieved with global knowledge.

V. CONCLUSION

In order to gather trust evidence and securely store and communicate it both inside and beyond the Blockchain network, a strong trust management system based on Blockchain technologies is conceptualised and implemented in this study. By using such technologies, we provide a more secure trust information confidentiality and credibility verification during storage and exchange and give a time-stamped record of all entities' activities. Our analysis shows that the structure we've suggested is workable, deployable, and appropriate for IoT settings. The decentralised nature, ongoing protection, and resistance to a range of threats, as well as the minimal overhead and inadequate capital requirements of the suggested architecture, make it practicable as well. In the future, we will extend our trust model to assist other groups like miners and the device's judgement of trustworthiness. In order to reduce the cost and increase the effectiveness of our plan, we also aim to incorporate more benchmarking blockchain consensus methods.

REFERENCES

[1] E. Zhuravskaya, M. Petrova, and R. Enikolopov, "Political effects of the internet and social media," *Annu. Rev. Econ.*, vol. 12, no. 1, pp. 415–438, Aug. 2020.
[2] E. G. Popkova, E. N. Egorova, E. Popova, and U. A. Pozdnyakova, "The model of state management of economy on the basis of the Internet of Things," in *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*. Springer, 2019, pp. 1137–1144.
[3] N. Ahmed, R. Amin, H. Aldabbas, D. Koundal, B. Alouffi, and T. Shah, "Machine learning techniques for spam detection in email and IoT platforms: Analysis and research challenges," *Secur. Commun. Netw.*, vol. 2022, pp. 1–19, Feb. 2022.
[4] M. D. Alshehri, F. K. Hussain, and O. K. Hussain, "Clustering-driven intelligent trust management methodology for the Internet of Things (CITM-IoT)," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 419–431, Jun. 2018.
[5] N. Koutroumpouchos, C. Ntantogian, and C. Xenakis, "Building trust for smart connected devices: The challenges and pitfalls of TrustZone," *Sensors*, vol. 21, no. 2, p. 520, Jan. 2021.
[6] S. Ramzan, A. Aqdus, V. Ravi, D. Koundal, R. Amin, and M. A. Al Ghamdi, "Healthcare applications using blockchain technology: Motivations and challenges," *IEEE Trans. Eng. Manag.*, early access, Jul. 25, 2022, doi: 10.1109/TEM.2022.3189734.
[7] L. Geoff, *Building Energy Management Systems: An Application to Heating Natural Ventilation Lighting and Occupant Satisfaction*. 2013.
[8] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.
[9] D. W. Haoxiang, "Trust management of communication architectures of Internet of Things," *J. Trends Comput. Sci. Smart Technol.*, vol. 2019, no. 2, pp. 121–130, Dec. 2019.

[10] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: Challenges, issues and solutions at different IoT layers," *J. Supercomput.*, vol. 77, no. 12, pp. 14053–14089, Dec. 2021.
[11] J. Lin, Z. Shen, and C. Miao, "Using blockchain technology to build trust in sharing LoRaWAN IoT," in *Proc. 2nd Int. Conf. Crowd Sci. Eng.*, Jul. 2017, pp. 38–43.
[12] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.
[13] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social Internet of Things: A taxonomy, open issues, and challenges," *Comput. Commun.*, vol. 150, pp. 13–46, Jan. 2020.
[14] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "Holitrust-A holistic cross-domain trust management mechanism for service-centric Internet of Things," *IEEE Access*, vol. 7, pp. 52191–52201, 2019.
[15] A. Singh, A. Payal, and S. Bharti, "A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues," *J. Netw. Comput. Appl.*, vol. 143, pp. 111–151, Oct. 2019.
[16] H. Baqa, N. B. Truong, N. Crespi, G. M. Lee, and F. Le Gall, "Quality of information as an indicator of trust in the Internet of Things," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 204–211.
[17] I. U. Din, A. Bano, K. A. Awan, A. Almogren, A. Altameem, and M. Guizani, "LightTrust: Lightweight trust management for edge devices in industrial Internet of Things," *IEEE Internet Things J.*, early access, May 18, 2021, doi: 10.1109/JIOT.2021.3081422.
[18] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a trust evaluation mechanism in the social Internet of Things," *Sensors*, vol. 17, no. 6, p. 1346, 2017.
[19] C. Panteli, A. Kylili, and P. A. Fokaides, "Building information modelling applications in smart buildings: From design to commissioning and beyond a critical review," *J. Cleaner Prod.*, vol. 265, Aug. 2020, Art. no. 121766.
[20] K. Siountri, E. Skondras, and D. D. Vergados, "Developing smart buildings using blockchain, Internet of Things, and building information modeling," *Int. J. Interdiscipl. Telecommun. Netw.*, vol. 12, no. 3, pp. 1–15, Jul. 2020.
[21] R. Carli, G. Cavone, S. Ben Othman, and M. Dotoli, "IoT based architecture for model predictive control of HVAC systems in smart buildings," *Sensors*, vol. 20, no. 3, p. 781, Jan. 2020.
[22] R. Casado-Vara, A. Martin-del Rey, S. Affes, J. Prieto, and J. M. Corchado, "IoT network slicing on virtual layers of homogeneous data for improved algorithm operation in smart buildings," *Future Gener. Comput. Syst.*, vol. 102, pp. 965–977, Jan. 2020.
[23] S. Sadowski, P. Spachos, and K. N. Plataniotis, "Memoryless techniques and wireless technologies for indoor localization with the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10996–11005, May 2020.
[24] K. Akkaya, I. Guvenc, R. Aygun, N. Pala, and A. Kadri, "IoT-based occupancy monitoring techniques for energy-efficient smart buildings," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Mar. 2015, pp. 58–63.
[25] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Exp. Syst. Appl.*, vol. 168, Apr. 2021, Art. no. 114384.
[26] W. Yao, J. Ye, R. Murimi, and G. Wang, "A survey on consortium blockchain consensus mechanisms," 2021, *arXiv:2102.12058*.
[27] B. Sriman, S. G. Kumar, and P. Shamili, "Blockchain technology: Consensus protocol proof of work and proof of stake," in *Intelligent Computing and Applications*. Springer, 2021, pp. 395–406.
[28] F. Saleh, "Blockchain without waste: Proof-of-stake," *Rev. Financial Stud.*, vol. 34, no. 3, pp. 1156–1190, 2021.
[29] G. Xu, Y. Liu, J. Xing, T. Luo, Y. Gu, S. Liu, X. Zheng, and A. V. Vasilakos, "SG-PBFT: A secure and highly efficient blockchain PBFT consensus algorithm for Internet of Vehicles," 2021, *arXiv:2101.01306*.
[30] A. S. Yadav and D. S. Kushwaha, "Digitization of land record through blockchain-based consensus algorithm," *IETE Tech. Rev.*, vol. 39, no. 4, pp. 1–18, 2021.
[31] G. Chen, F. Zeng, J. Zhang, T. Lu, J. Shen, and W. Shu, "An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems," *Comput. Netw.*, vol. 190, May 2021, Art. no. 107952.

FATHE JERIBI received the B.S. degree in information systems from Jazan University, Jazan, Saudi Arabia, in 2010, the M.S. degree in computer science and information technology from Sacred Heart University, Fairfield, CT, USA, in 2014, and the Ph.D. degree in information technology from Towson University, Towson, MD, USA, in 2018. He is currently an Assistant Professor with the College of Computer Science and Information Technology, Jazan University. His research interests include computer networks, SDN, software engineering, machine learning, wireless ad hoc networks, the IoT, and distributed computing.

RASHID AMIN received the Master of Science in Computer Science (MSCS) and Master of Computer Science (MCS) degrees from International Islamic University, Islamabad, and the Ph.D. degree in computer science from COMSATS University Islamabad, Wah Campus, Pakistan. He has been working as an Assistant Professor with the Department of Computer Science, University of Chakwal, Pakistan. Before this, he worked as a Lecturer at the Department of Computer Science, University of Engineering and Technology, Taxila, Pakistan, for seven years, and the University of Wah, Wah Cantt, Pakistan, for four years. He supervised many M.S. level student's theses, and five Ph.D. students are working under his supervision. He is co-editing some special issues in some renowned journals. He has published several research articles on ML, DL, and SDN in well-reputed venues, such as IEEE Communication Surveys and Tutorial, IEEE Access, *Electronics* (MDPI), and *IJACSA*. His current research interests include machine learning, deep learning, the IoMT, distributed systems, and cyber security. He has been serving as a Reviewer for international journals, such as NetSoft, LCN, IEEE GLOBECOM, FiT, IEEE Wireless Communication, IEEE Internet of Things Journal, IEEE Journal on Selected Areas in Communications, IEEE Access, and IEEE Systems Journal.

MOHAMMED ALHAMEED (Member, IEEE) received the M.Sc. degree in computer science from the School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, in 2013, and the Ph.D. degree in computer science from the Department of Computer and Electrical Engineering and Computer Science, Florida Atlantic University, in December 2018. He is currently an Assistant Professor with the College of Computer Science and Information Technology, Jazan University, Saudi Arabia. His research interests include computer engineering and networks, intelligent systems, artificial intelligence, and vehicular ad hoc networks. He is a member of the ACM.

ALI TAHIR received the B.S. degree in computer engineering and the M.S. degree in telecom engineering from the University of Engineering and Technology (UET), Taxila, Pakistan, in 2006 and 2010, respectively, and the Ph.D. degree in computer science from COMSATS University Islamabad (CUI), Wah Campus, Pakistan, in 2021. He worked at Nokia Siemens Network for two years as a BSS Engineer. He also worked at SCB and AHQ, Islamabad, as a Network Engineer. He is currently working as a Senior Lecturer with the College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia. His research interests include wireless networks, distributed systems, software defined networking, the IoT, network security, machine learning, and software engineering.