A Secure Architectural Model using Blockchain and Estimated Trust Mechanism in Electronic Consumers

Akshay Kumar, Geetanjali Rathee, Chaker Abdelaziz Kerrache, Muhammad Bilal *Senior Member, IEEE*, and Thippa Reddy Gadekallu

***Abstract*—Consumer electronics devices, such as refrigerators, washing machines, TVs, smartphones, and household appliances, have become integral to human activities. However, these devices are vulnerable to security breaches and cyber-criminal threats, which can result in the theft and misuse of sensitive information. Existing security surveys and proposed schemes have encountered limitations in terms of redundancy and effectiveness. In this paper, we present a novel approach that ensures secure and transparent communication in consumer electronics. We introduce a multi-criterion decision-making model called TOPSIS, along with a weighted product model, to enhance the security and accuracy of the system. Furthermore, our proposed scheme employs a blockchain system for continuous tracking and monitoring of devices, ensuring accountability and surveillance of their past communications. Through comprehensive validation and verification against existing approaches using various security metrics, our proposed scheme demonstrates superior performance and effectiveness.**

***Index Terms*—Blockchains, Trust management, Consumer protection, Smart devices, TOPSIS.**

I. Introduction

The advancements in network communication have given rise to a multitude of new technologies that not only enhance connectivity but also enable efficient and seamless communication within society [1], [2]. Among these technologies, the Consumer Internet of Things (CIoT) stands out as a burgeoning field in consumer electronics, facilitating effective and efficient connectivity among smart electronic devices [3]–[6]. Consumer Internet of things is a network in which smart devices are connected with each other and respond to the environment. However, this connectivity is seen not only as one of the eases of usage but also a major concern where connected smart devices are prone to various security threats. Further, the devices connected or providing services to a particular network may bring the entire communicating environment a risk by [7]–[10] jeopardizing the privacy of the consumers which may be considered as another major concern.

A. Motivation

One might question the potential security implications that arise when household smart devices, interconnected and operating within a network, are considered. This pertains to the scenario where consumer devices such as refrigerators, air conditioners, and laptops establish connections for the purpose of transmitting and receiving information amongst themselves. To illustrate, envision a situation where a user innocently opens their refrigerator to retrieve a chilled glass of water, only to be promptly greeted by a message on the display demanding a significant financial payment to cyber-criminals, under the threat of service disruption [11]–[13]. The cyber-criminal may attack any type of household device either to jeopardize the appliance or to steal private network information. It may end up in extortion of money either by blackmailing due to hijacking of sensitive data or by demanding unnecessary charges for services whose subscription has already been bought. That probably means that one might need to pay using their own device at their space. This type of threat is considered as ransomware. Another type of threat may be distributed denial of service where the intruder by using a given device and network may attack some other organization by flooding a lot of traffic or jamming messages with the aim of crashing their websites. Moreover, the intruders may also plant viruses or spy-wares within the home network.

One of the dangerous cyber-attacks may be where cyber-criminals may get access to audio and video feeds from security cameras or any other devices with built in microphones in the home network. Many organizations and small businesses are using consumer electronic devices without being aware of risks and harms.Various existing consumer electronic surveys have investigated technical security aspects while purchasing these devices such as digital forensics, mathematical and trust computation model, IoT-based technology and so on. However, the development and designing of an efficient and secure communication method/scheme for reducing the delay and improving the accuracy of the network for consumer electronic is still in its early stage [14]–[16]. In order to ensure a secure and trusted consumer electronic system, we have proposed a trusted and secure architecture by proposing the TOPSIS and

(Corresponding Authors: Muhammad Bilal)

Akshay Kumar is with the Department of Computer Science and Engineering, Jaypee Institute of Information Technology, NOIDA, Uttar Pradesh 201309, India. (e-mail: akshayrathee01@gmail.com)

Geetanjali Rathee is with the Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi-110078, India. (e-mail: geetanjali.rathee123@gmail.com)

Chaker Abdelaziz Kerrache is with the Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat, Algeria. (e-mail: ch.kerrache@lagh-univ.dz)

Muhammad Bilal is with the School of Computing and Communications, Lancaster University, Bailrigg, Lancaster LA1 4WA, United Kingdom (e-mail: m.bilal@ieee.org)

Thippa Reddy Gadekallu is with the Zhongda Group, Haiyan County, Jiaxing City, Zhejiang Province, China, 314312, as well as with the Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon, as well as with the School of Information Technology and Engineering, Vellore Institute of Technology, India, as well as with the College of Information Science and Engineering, Jiaxing University, Jiaxing, 314001, China, and with the Division of Research and development, Lovely Professional University, Phagwara, India (e-mail: thippareddy.g@vit.ac.in)

blockchain technology for sensing, evaluating and analyzing the communicated device in the network.

B. Contribution

To ensure a secure and privacy-preserving experience for individuals utilizing consumer electronic devices, this paper presents a novel architectural model that integrates a trusted blockchain mechanism. The proposed system leverages the TOPSIS method and weight product model (WPM) to assess and gauge the level of trust during inter-device communication [17]–[19]. Furthermore, the adoption of blockchain, a cutting-edge transparent technology, enables seamless and ongoing analysis and surveillance of the devices. By incorporating these innovative components, the proposed model aims to establish a foundation for safeguarding security and privacy concerns while enhancing the overall trustworthiness of consumer electronic devices in human life. The blockchain technology where consumer devices are connected and analyzed with some trust level along with continuous surveillance while transmitting the information in the network as illustrated in Fig. 1.

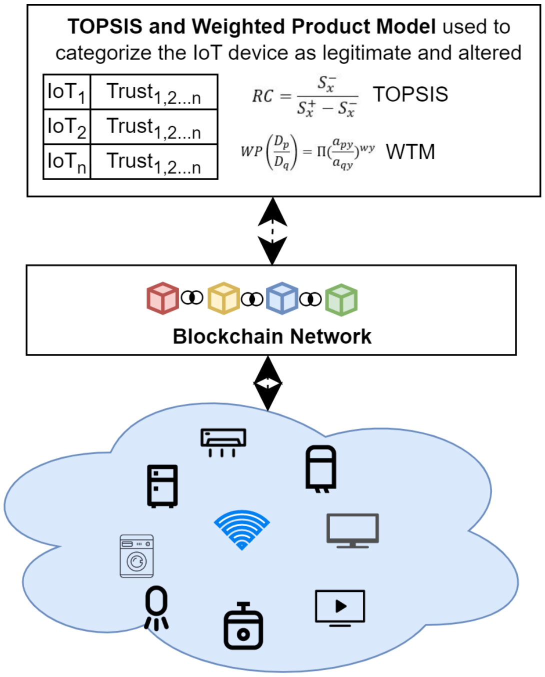
TOPSIS and Weighted Product Model used to categorize the IoT device as legitimate and altered
IoT_1 $Trust_{1,2...n}$
IoT_2 $Trust_{1,2...n}$
IoT_n $Trust_{1,2...n}$
$RC = \frac{S_x^-}{S_x^+ - S_x^-}$ TOPSIS
$WP\left(\frac{D_p}{D_q}\right) = \Pi(\frac{a_{py}}{a_{qy}})^{wy}$ WTM
Blockchain Network

Fig. 1. Blockchain-based Consumer Electronics System

The detailed contribution of the proposed solution is discussed as follows:

- A TOPSIS and weighted product model is used to provide a multi criterion decision for analyzing the trust level of each communicating device in the network.
- A blockchain-based network is used for further surveillance and to track the legitimate communicating devices in the network.
- The proposed mechanism is further verified and validated against various security metrics specifically related to consumer electronic devices such as ransomware, distributed denial of service, data falsification attack and authentication.

The novelty of this contribution is the integration of the above mentioned mechanisms for ensuring secure communication by computing device trusts using weights and multiple criterion decisions. TOPSIS is defined as multi criterion decision method that considers number of communicating attributes to decide or identify the legitimacy of each device. In addition, though TOPSIS or weight product are being used in number of other applications, however, the integration of both the methods for ensuring the security of consumer electronics by identifying their historical behaviour and interactions among other devices is a completely novel approach that has not been used by previous research. Further, the blockchain-based mechanism is integrated after applying TOPSIS and weight product model for consumer electronics-devices. In this case, the blockchain is maintained for legitimate devices that have permission to interact in the network. The proposed mechanism is verified against various security metrics specifically related to consumer electronic devices such as ransomware, distributed denial of service, data falsification attack and authentication.

The remaining structure of the paper is organized as follows. The number of literature and security methods proposed by several scientists is discussed in section 2. A secure and efficient multi-criterion decision making model TOPSIS and weighted product model along with blockchain technique is detailed in section 3. In addition, the validation and verification of proposed scheme in terms of several security parameters along with existing approach is illustrated in section 4. Finally, section 5 concludes the paper along with its future direction.

II. Related Work

Number of authors/scientists have proposed consumer electronics techniques and methods for benefiting the society. However, very few of them have highlighted the point of security and trust while communicating and operations through smart/intelligent devices. The section has discussed numerous security and trust based approaches as presented in Table I. Hahn et al. [20] have proposed surveyed the advancements and benefits of using consumer electronics among users in a variety of domains. The authors have discussed the entertainment, comfort, efficiency and services of using such technologies in the market. In addition, the authors have highlighted the privacy and security issues of using and emerging such technologies with the existing techniques. They have discussed the application of healthcare systems where sensitive information gathering of patients may further bring new challenges and devices concerns in the network.

Pal et al. [21] have used a hybrid design for gathering the information by combining the stated-choice and semi-structured experiments. The authors have used an exploratory factor analysis for determining the personal factors. Further they have used a multinomial model for testing the casual model.The authors have not only examined the functions and decisions in specific domains but have also addressed the associated security risks. Additionally, they have presented diverse research outcomes and incorporated community perspectives. In a related study, Kahleifeh and Thapliyal [22] proposed an energy-efficient security mechanism for smart consumer electronics utilizing adiabatic logic. By employing adiabatic circuit design,

TABLE I
LITERATURE SURVEY

Author's Name	Technique	Performance Metrics	Limitation
Hahn et al. [20]	Advancements and benefits of using consumer electronics	highlighted the privacy and security issues of using and emerging such technologies with the existing techniques	No proposed mechanism
Pal et al. [21]	Hybrid design by combining the stated-choice and semi-structured experiments	an exploratory factor analysis for determining the personal factors	Lot of computational delay is there
Kahleifeh and Thapliyal [22]	energy efficient security mechanism for adiabatic logic	The authors have introduced a 2-EE-SPFAL scheme by constructing the two-phase clock generators	System has complex computation
Ding et al. [23]	Novel digital forensic tool	The system was efficient for high-quality real-time services at consumers end	Leads to networking security threats
Lipoff [24]	Platform of services ranging from entertainment to commercials	The authors discussed the business models such as subscribing fees to advertising support among the users	Didn't propose any model
Macedo et al. [25]	Two-level approach called mathematical trust computation	They have provided various security benefits among smart devices in the network	Two level trust leads to cost of security
Ngoepe and Ngwenya [26]	IoT based technology to generate a smart assemblage	The authors have utilized the delphi and qualitative inquiry technique for further exploring the information security issues in the network	Needs to improve security for real time transmission

the authors successfully mitigated side-channel threats through reduced energy consumption. They introduced a 2-EESPFAL scheme, which involved the construction of two-phase clock generators. The experimented results of proposed framework are analyzed against various security metrics such as false rejection rate and false positive rate in respect of existing approach. Ding et al. [23] have proposed a novel digital forensic tool to secure the end users by building a deep learning scheme along with the realization of classification and attack detection methods. The authors have validated the proposed solution by comparing it with existing schemes in terms of various metrics such as robustness, efficiency, detection and data gathering. Further, the proposed approach was efficient for high-quality real-time services at consumers end.

Lipoff [24] have illustrated the increasing rate of using consumer electronics in market among the customers. They have provided a platform of services ranging from entertainment to commercials. The authors have discussed the business models such as subscribing fees to advertising support among the users. Along with various benefits, the privacy and security are considered as one of critical and crucial issues that may benefitted available targets for the future usage. Macedo et al. [25] have focused on certain challenges associated with trusted communication among smart devices while applying in consumer IoT applications. The authors have presented a two-level approach called mathematical trust computation to present the assessment of objectives and confidence among the consumers. Further, the authors have provided various security benefits among smart devices in the network. Ngoepe and Ngwenya [26] have proposed an IoT based technology to generate a smart assemblage and eco-system to ensure a secure communication system in the network. The authors have utilized the delphi and qualitative inquiry technique for further exploring the information security issues in the network. In addition, they have discussed various paths for resolving the security dispute with improved security and safety among electronic vehicles.

Though consumer electronics is termed as one of oldest and significant research where scientists have been working on it for years for providing a comfortable and ease of life to their consumers. However, the security and privacy of consumer electronics is still at its early stage. In addition, very few research discussed security concerns while combining and operating large number of smart devices in the network. In order to ensure a secure and trusted consumer electronic system, we have proposed a trusted and secure architecture by proposing the TOPSIS and blockchain technology for sensing, evaluating and analyzing the communicated device in the network. The literature survey is further improved by adding the recent papers on consumer security in the updated manuscript. However, in our proposal, the impact of intrusion is limited as the devices will be unable to delete or alter the data. This is due to the fact that our suggested approach is based on blockchain in the back-end which provides transparency among all the IoT devices and users so that a single change would reflect in all others' database and would become easily traceable.

III. PROPOSED MODEL

A. System Model

The system model of proposed model consisting two security model such as TOPSIS and weighted product model having 'n' number of consumer devices are illustrated in Fig. 2. The presented Fig. 2 consists of various smart devices that generated and gathers the information from the environment and send it to the base station. The proposed security framework is divided into three phases such as devices phase where all the devices are integrated and communicated among each other. The second phase is networking phase where the secure communication among each device is ensured using TOPSIS and WPM models. The TOPSIS and WPM models continuously analyse and sense the trust level of each communicating device. In addition, the transparency of each communication history is maintained via blockchain network. The blockchain solution keeps the track of each device history and previous communication records. Finally, the third phase of proposed framework is the classification of devices such as legitimate and malicious (malevolent). The devices having higher trust value and clean communication records are designated as legitimate. While the devices having

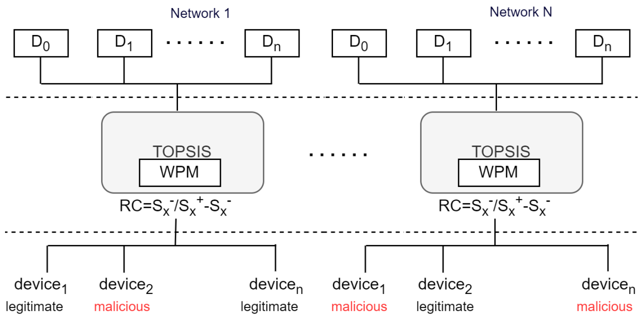

Fig. 2. Proposed Security Framework.

lesser trust value and incorrect past record may recognize it as malevolent device.

In order to ensure the secure of each device that submitting the generated or collected information is further measured through a security model based upon multiple criteria decision method and WPM. The WPM is used to assign some random weights to the system that is again increased and decreased depending upon their interactions in the network. The device having higher weighted value is considered as legitimate and devices having lower weights are mostly defined as malicious. The TOPSIS and WPM are considered as one of the security models that ensures a secure transmission and communication among devices by computing trust values that is dependent upon their ideal and non-ideal alternates and parameters. The legitimacy of each communicating device is finalized by analyzing their multiple criteria's using TOPSIS method. However, the multi-criteria decision method takes the decision of device's legitimacy upon receiving its WPM into two categories such as malevolent and legitimate. The WPM model is integrated with TOPSIS in order to further accurate the legitimate decisions of each communicating device in the network. The explanation of each security model is further explained in below text. The list of abbreviation is now listed below II.

TABLE II
TABLE OF ABBREVIATION

Abbreviation	Description
S_c	Selection criteria
$SC_1, SC_2, ...SC_n$	Selection criteria of device 1,2,...n
$A_I and A_N$	Ideal and Non-ideal alternatives
D_{cxy}	Interaction of each alternatives
$D_1, D_2...D_n$	Number of devices
$D_p and D_q$	p and q devices D
$NDC_{m\times n}$	Normalized 2-dim matrix having m devices and n selection criteria
W_y	Weight of selection criteria
A_x, C_y	Alternate and criteria value of device x and y
RC	Relative closeness
$S_x^- and S_x^+$	Distance of alternative x of ideal and non-ideal separation measures
W_y	weight of selection criteria
$Z^- and Z^+$	associate criteria of ideal and non-ideal

B. Improved TOPSIS using weight product model

The main procedure of improved TOPSIS is discussed as follows:

Step 1: Initially we construct a 2-dim matrix $(D_c)_{m\times n}$ having m number of devices D_m and n no. of selected criteria's S_c, with the interaction of each alternatives defined as D_cxy, $x = 1, 2, \ldots m$ and $y = 1, 2, \ldots .n$. the matrix represents the m number of devices as $D_1, D_2, \ldots .D_m$, and $S_{c1}, S_{c2}, \ldots S_{cn}$ criteria's value and S_cx, y denotes criteria value of y^{th} criteria of x_{th} D.

Step 2: The $(D_c)_{m\times n}$ matrix is further normalized as $(ND_c)_{m*n}$ whose values ranges from 0 to 1 means 1 is the most required criteria and 0 is the least required criteria. The normalized 2-dim matrix is further defined as:

$ND_c = (D_cxy)_{m\times n}$ that can be further defined as:

$$ND_c = (D_cxy)_{m\times n} \tag{1}$$

$$ND_c = \frac{D_cxy}{\sqrt{\sum_{x=1} mD_cxy^2}} \tag{2}$$

where, $x = 1, 2, ...m$ and $y = 1, 2...n$.

Step 3: A set of weights W_y (for $y = 1, 2, \ldots n$) have to be decided for S_c parameters. Further, the weights are defined according to the selected criteria and alternates. The weighted product model is used to further categorize the devices according to their alternates and criteria's:

Step 3a: Let W_y represents the relative weight of selected criteria S_cx and a_xy denotes the alternates performance value in terms of alternate A_x and criteria C_y. The following product can be used to finally decide the weight on devices D_p and D_q where $(m >= P, Q >= 1)$.

$$W(D_p/D_q) = \sum_{y=1}^{n}(a_py/a_qy)^{wy}, forp, q = 1, 2...m \tag{3}$$

That represents that if the ratio of $P(D_p/D_q)$ is more than 1 then D_p is more trusted than D_q.

Step 4: The normalized decision matrix is computed as:

$$W = (t_{m\times n}) = (w_yND_{cxy)})_{m\times n} \tag{4}$$

$i = 1, 2...m$ and $j = a, 2....n$, where

$$W_y = W_y \sum_{y=1}^{n} W_y, y = 1, 2, ...n \tag{5}$$

Step 5: Further illustrate the non-ideal $(A_{non-ideal})$ and ideal alternatives (A_{ideal}) for every S_c parameter.

$$\begin{aligned} A_{ideal} = min(z_{xy}|ideal = 1, 2, ...m)|z\epsilon Z >, \\ < max(z_{xy}|x = 1, 2, ...m)|z\epsilon Z_+ \\ z_{ideal}|Z = 1, 2, ...n \end{aligned}$$

$$\begin{aligned} A_{non-ideal} = < max(z_{xy}|ideal = 1, 2, ...m)|z\epsilon Z >, \\ < min(z_{xy}|x = 1, 2, ...m)|z\epsilon Z_+ \\ z_{non-ideal}|Z = 1, 2, ...n \end{aligned}$$

$$\begin{aligned} Z_+ = z = 1, 2...n|zassociateswithcriteria \\ having + veimpact \\ z_- = z = 1, 2...n|zassociateswithcriteria \\ having - veimpact \end{aligned}$$

Step 6: The separation measures are obtained for each alternate using Euclidean distance using:

$$S_x^+ = \left\{\sum_{y=1}^{n}(z_{xy} - z_{ideal_y})^2\right\}^{0.5}$$

$x = 1, 2, ...m$ and $y = 1, 2, ..n$.

$$S_x^- = \left\{\sum_{y=1}^{n}(z_{xy} - z_{non-ideal_y})^2\right\}^{0.5}$$

$x = 1, 2, ...m$ and $y = 1, 2, ..n$.

Step 7: In addition, the relative closeness for a specific alternative corresponding to the ideal solution is determined as:

$$RC = \frac{S_x^-}{S_x^+ - S_x^-}, i = 1, 2...m \tag{6}$$

Step 7: Rank the devices according to $RC_x = (x = 1, 2 \ldots m)$.

C. Blockchain-based Edge Computing Framework

The decision making and mathematical model are further used to ensure the security and legitimacy of each and every communicating entity in the network that can be further traced using blockchain network. The TOPSIS model is used to provide an accurate transmission of industry 4.0 information among workers, devices and other communicating entities while WPM model in TOPSIS is used to analyses the legitimacy of each device that is involved while transmitting the information. In addition, blockchain system is used to ensure the transparency and privacy among communicating entities by continuously verifying or analysing the generated reports by legitimate devices. Any alteration in data and involvement of malicious devices may immediately know by other sensors and can be traced and tackle the issue at once. Figure 2 depicts the proposed framework of blockchain-based computing scenario where each and every block contains the smart devices which are being traced regularly in order to ensure a transparent and legitimate communication mechanism in the network. A single alteration in any block can be immediately known by the remaining entities and blocked for future communications in the network. The working of the entire proposed mechanism can be easily understood using an Algorithms 1 and 2 as explained below.

Algorithm 1 Secure Algorithm

```
Prerequisite: 10% of devices are altered from legitimate to malicious by the intruders upon increasing the network size. All the communicating devices are legitimate upon establishing the network
Input Value: (1) A network N having $N = n_1, n_2, n_3 \ldots\ldots n_n$ number of IoT devices
Output: Device is legitimate or altered
Given: Trust-based computation using TOPSIS model by identifying the legitimacy of each device using WPM and a blockchain network
Step 1: A network of Blockchain $N$ consists of $d$ IoT devices having several values of trust.
Step 2: Establish the networking environment.
all nodes $I_n = I = 1, 2, \ldots .N$ p=1 to N Compute Trust of each device using estimated TOPSIS() Model
(Device is ideal) Maintain a blockchain () network of legitimate devices and permit further communication  Block/deny further communication
Step 3: Each ideal device is surveillance using blockchain
```

IV. Performance Analysis

A. Dataset and Baseline Approach

The validation and verification of proposed solution in terms of several security parameters such as ransomware, distributed denial of service, authentication and data falsification threat is performed over various numerical results on the basis of generated synthesized dataset. The simulation model is purely based on NetLogo for modelling and exploration of complex networking systems. The proposed mechanism is related to trust and blockchain mechanism for ensuring a secure and transparent communication among devices in the network. The significant threats that affect the overall performance of consumer electronics networks are Ransomware and Distributed Denial of Service attack. The present paper display both threats along with their comparison with the traditional approach. This paper does not specifically address the time requirements for mining and transaction processing within the network. Instead, it primarily emphasizes the importance of transparency and security aspects, which can be effectively resolved through the integration of blockchain technology and trust-based mechanisms. By incorporating blockchain and leveraging trust-based approaches, the proposed solution aims to provide robust solutions to enhance transparency and security in the network. The proposed mechanism is further analysed by focusing only consumer electronics threats such as ransomware, distributed denial of service and authentication. In addition, the proposed algorithm simply presents the integration of blockchain and trust-based method along with their computational formulas. The trust is computed to speed the communication process among legitimate users by distinguishing among malicious and ideal devices. The threat model of proposed solution is further discussed in the updated manuscript. The % of malicious behavior where intruders are invited to perform some illegal activities are allowed in order to further analyze and compare the security results as compare to traditional approach. In order to reach the desired goal, the volume of generated dataset is obtained from crawling microblogs that specially concentrated on recent and incorrect information received from various communicating devices.

Further, the proposed solution is analyzed over one recent existing approach in which Macedo et al. [25] have focused on certain challenges associated with trusted communication among smart devices while applying in consumer IoT applications. The authors have presented a two-level approach called mathematical trust computation to present the assessment of objectives and confidence among the consumers. Further, the authors have provided various security benefits among smart devices in the network. The proposed method is compared and analyzed against Macedo et al. [25] security method over various security metrics.

B. Simulation Setups

The numerical simulation is done over both adversary and legitimate models by publishing both ideal and intruders' devices in the network. The intruders may steal or hack the consumer

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2023.3336597

Algorithm 2 TOPSIS() and WPM() Model

Step 1: The normalized 2-dim matrix is further defined as: $ND_c = (D_cxy)_{m \times n}$ that can be further defined as:

$$ND_c = (D_cxy)_{m \times n} \tag{7}$$

$$ND_c = \frac{D_cxy}{\sqrt{\sum_{x=1} mD_cxy^2}} \tag{8}$$

Step 2: The following product can be used to finally decide the weight on devices D_p and D_q where $(m >= P, Q >= 1)$.

$$WP(D_p/D_q) = \phi_{y=1}n(a_py/a_qy)^{wy}, forp, q = 1, 2...m \tag{9}$$

Step 3: The separation measures are obtained for each alternate using Euclidean distance using:

$$S_x^+ = \sum_{y=1} n(z_{xy} - z_{ideal_y})^{2^{0.5}}$$

$x = 1, 2, ...m$ and $y = 1, 2, ..n$.

$$S_x^- = \sum_{y=1} n(z_{xy} - z_{non-ideal_y})^{2^{0.5}}$$

device for their own purpose or jam the network for producing distributed denial of service attack. The trust values and communication track of both legitimate and fake devices are recorded after every specific interval of time as $S(t)$. Let $N(I)$ represent the number of ideal consumer electronic devices communicating in the network and $N(M)$ denotes the number of malevolent number of communicating devices hacked by the intruders in the network. In addition, the simulation set up of proposed framework is further mentioned in Table III. The blockchain platform considered for verification of proposed mechanism is based on javascript by taking Proof of Work as consensus algorithm. The proposed mechanism throughput depends upon the difficulty level set for the number blocks in the network. The difficulty level that is being considered for this approach is four having mean time of 1.35 sec approximately. In addition, the block mining times further depends upon various difficulty levels over number of attempts. Further, the transaction latency of proposed approach is calculated by adding time of generating key pair to the block mining time. The average time to create a key pair is illustrated as 0.288375 seconds. This time can be added to the time taken to min block for various difficulty levels to get the transaction latency. For instance, for difficulty level 4, the transaction latency is 1.63875 seconds and the gas consumption for performing the transaction is approximately 12.19 GWEI.

C. Impact of Blockchain in CE

The blockchain is integrated into the network to continually monitor and enhance accuracy in decision-making and information transmission. This ensures a more secure and reliable network environment. The generated information from various devices kept secret and therefore, can be implemented using private blockchain. The accessing and recording of information is determined at various levels with the permission of administrator in private blockchain. Here we used private blockchain is maintained at various steps such as recording, data generation, analysis etc by encouraging the organizations to adopt and rely on this technique. Further, for realizing the integration with present network, we relied on Java for creation, insertion and validation of blockchain. The network contains the creation module responsible for block generation with their hashes.

TABLE III
SIMULATION METRICS OF PROPOSED FRAMEWORK

Metrics	Terms
Simulation area	800 m × 800 m
Number of communicating devices	100
% of malevolent devices	$[5, 15]\%$
Computed Trust Results	$[0, 1]$
Transmission power	$[15, 35]$ dBm
Receiver power	10 dBm
Resources	10^3 CPU cycle/unit time
Blockchain Platform	Javascript
Difficulty level	four
Transaction latency	1.63875 Sec
Gas Consumption	12.19 GWEI

D. Default Operations while Integrating Trust-based and Blockchain Schemes

The trust-based scheme, TOPSIS, that is used for the facilitation of accurate decision making during transmission of information can be made more effective and transparent by integrating it with blockchain. The chain of devices kept in the blocks containing the initial information such as identity, IP address, company name etc. may improve the overall trust and transparency in the network. Now, the default operations of the blockchain such as block mining, transaction addition and block creation are done via the legitimate devices which are identified through TOPSIS. The blockchain contains the block of legitimate devices which are further kept under continuous surveillance for tracking potential malicious behavior in the future. The below text illustrates the basic operations of the blockchain containing the chain of legitimate devices.

1) Block Mining: The blockchain will contain the legitimate devices which have already been identified or categorized via the TOPSIS method. After the identification of legitimate devices and their addition in the chain of legitimate blocks, further surveillance is carried out to prevent future malicious behavior. The intruders may recognize the pattern of communication and start compromising the devices at a very small pace by introducing Sybil attack which is not feasible to be tracked at the initial phase of network communication. The miners of blockchain will be the legitimate devices having higher trust value that may further be changed or swapped depending upon the continuous change in their trust values. In case the trust value of a device keeps on reducing, then another block having a higher trust value may get the chance to be a miner. The devices having same trust value will be elected on first come first serve basis.

2) Transaction addition: Whenever a new device enters into the blockchain, the miners will verify its credentials before validating it into the blockchain network.

3) Block creation: Initially, the devices with trust values between $7.5 - 10$ will be part of the blockchain that can further be subdivided into various smaller blockchains depending upon the overall size of the network. Upon change in the trust values, the miners of the blockchain will change automatically, the threshold value for miner selection is $9.5 - 10$. Any alteration or reduction in trust values will permanently block or remove the device from blockchain as well as from the network.

E. Evaluating Metrics

The following metrics are considered to analyze or generate the graphical results of proposed and existing approaches:

Ransomware: It is defined as one of the significant types of cyber-threat in consumer electronic where intruders may compromise the legitimate device in the network with the means of their own interest. The ransomware parameter is considered as the total number of devices present in the network over the summation of legitimate and compromised devices by the intruder in the network.

Distributed denial of service: it is defined as another significant type of threat in the network where the motive of intruders is to jam the network by flooding the traffic and consume the network resources. In addition, the resources may be hold by any of the altered device in order to delay in the network. The distributed denial of service can be identified as the summation of total number of devices or compromised devices.

Data falsification attack: it is defined as the incorrect or false information generated or broadcasted by the compromised device in the network. The data falsification threat majorly attacks the specific devices with the aim of performing hazardous attacks in the network.

Authentication: it is defined as the device that is further allowed to perform transmission in the network. Only legitimate devices are authenticated and permitted to perform continuous transmission of information in the network.

F. Comparison and Discussion of Results

Fig. 3 represents the ransomware metric as compared to proposed and existing schemes where the proposed approach outperforms because of multiple-criterion decision method along with weighted product model that computes the trust of each device in advance in the network.

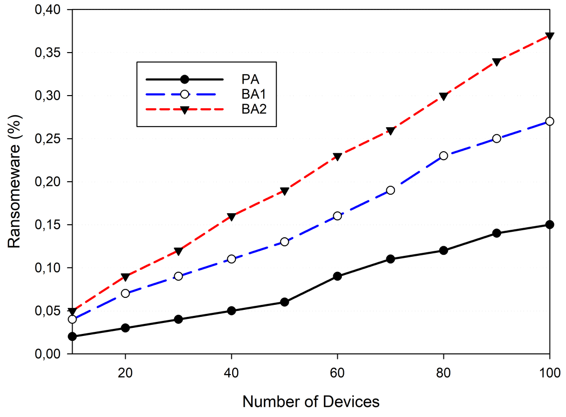

Fig. 3. Ransomware-related performance

Fig.4 presents the distributed denial of service where proposed mechanism is performing much better while identifying the compromised devices at the very first instance because of transparency through blockchain mechanism. In addition, the multiple criterion scheme may classify the devices based upon their interaction in the network.

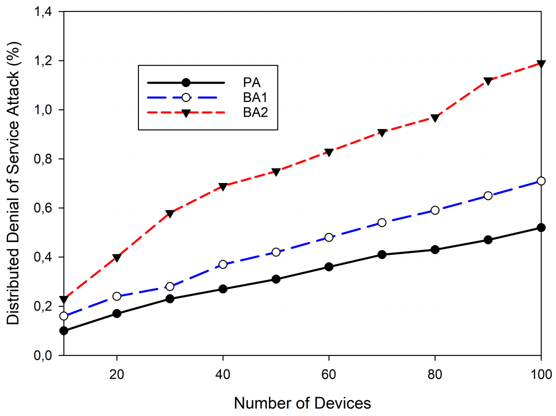

Fig. 4. Distributed Denial of Servic-related performance

Fig. 5 represents the data falsification threat where the amount of data compromised or altered by the proposed method is much less because of blockchain and weighted product model where each device is assigned some weight while distributing the information in the network. The device having higher weight is considered to be more trusted as compare to the approach used in baseline methods.

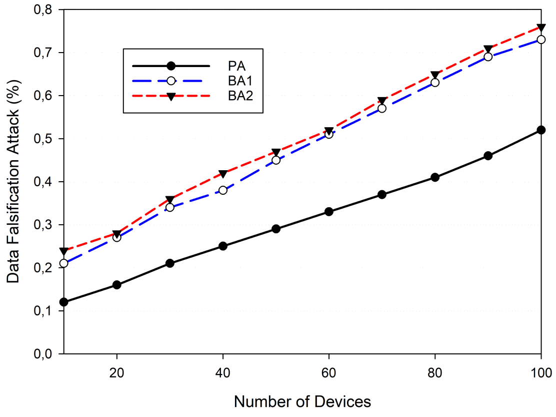

Fig. 5. Data Falsification-related performance

Finally, Fig. 6 deliberates the authenticity of the device that may further allowed to do the transmission in the network. The nodes having less weight can be considered as altered devices that are further analyzed after a specific interval of time until they are identified as completely authentic in the network. The proposed approach efficiently detects the authenticity of each communicating device using weighted product model by analyzing their weights in the network.

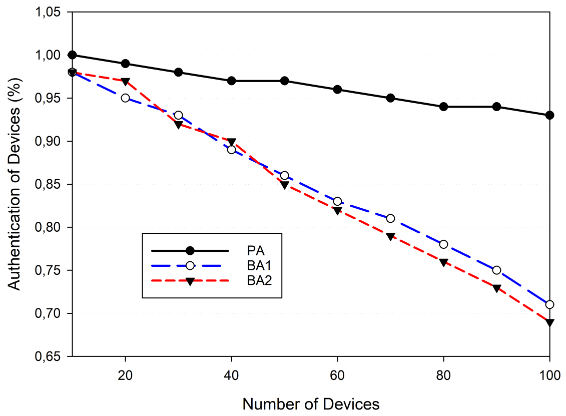

Fig. 6. Authenticity-related performance

G. Summary

The proposed mechanism is validated and verified against various existing schemes over several security measures such as ransomware, distributed denial of service, data falsification and authenticity. The presented graphs illustrates the out performance of proposed mechanism because of integration of trust-based and weight product model. The high computed trusted devices are involved in the communication process along with their continuous surveillance through blockchain mechanism. The proposed mechanism is successfully able to recognize the attack while transmitting the information in the network.

V. Conclusion

This paper proposed a multi-criterion decision making model known as TOPSIS and weighted product model where the trust of every consumer electronic device is analyzed and examined in the network. The trusted computed value may further decide the acceptance and rejection of the device in the network. Further, a blockchain technology is used for continuous surveillance and tracking on the devices. The proposed system is verified against various security parameters over existing approach. The out-performance of proposed scheme is due to multiple criteria used to analyze or decide the legitimacy of the consumer electronic device along with blockchain technology for their continuous analysis from the intruders. The intruders may not steal or get into consumers personal network without their permission.

As future work, additional metrics, such as the transaction delay of block verification and the selection of trusted miners, may be considered to ensure better accuracy and security.

References

[1] J. Li, X. Zeng, and A. Stevels, "Ecodesign in consumer electronics: Past, present, and future," *Critical Reviews in Environmental Science and Technology*, vol. 45, no. 8, pp. 840–860, 2015.

[2] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, vol. 58, no. 1, p. 102397, 2021.

[3] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to iot security," *IoT security: advances in authentication*, pp. 27–64, 2020.

[4] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry [future directions]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 19–23, 2017.

[5] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[6] G. Rathee, C. A. Kerrache, C. T. Calafate, and M. S. Halimi, "Secureblock: An ml-blockchain consumer-centric sustainable solution for industry 5.0," *IEEE Transactions on Consumer Electronics*, 2023.

[7] E. Hartono, C. W. Holsapple, K.-Y. Kim, K.-S. Na, and J. T. Simpson, "Measuring perceived security in b2c electronic commerce website usage: A respecification and validation," *Decision support systems*, vol. 62, pp. 11–21, 2014.

[8] R. K. Chellappa, "Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security," *under submission*, vol. 13, 2008.

[9] N. Duch-Brown, L. Grzybowski, A. Romahn, and F. Verboven, "The impact of online sales on consumers and firms. evidence from consumer electronics," *International Journal of Industrial Organization*, vol. 52, pp. 30–62, 2017.

[10] U. Ghosh, H. Maziku, H. P. Gupta, B. Sikdar, and J. J. Rodrigues, "Security, trust, and privacy solutions for intelligent internet of vehicular things—part i," *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 39–40, 2022.

[11] M. G. Galterio, S. A. Shavit, and T. Hayajneh, "A review of facial biometrics security for smart devices," *Computers*, vol. 7, no. 3, p. 37, 2018.

[12] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats and attacks to smart devices and applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021.

[13] S. Mare, F. Roesner, and T. Kohno, "Smart devices in airbnbs: Considering privacy and security for both guests and hosts." *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 2, pp. 436–458, 2020.

[14] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, and I. Rashid, "Alam: Anonymous lightweight authentication mechanism for sdn-enabled smart homes," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9622–9633, 2020.

[15] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222 310–222 354, 2020.

[16] M. Wazid, A. K. Das, and S. Shetty, "Bsfr-sh: Blockchain-enabled security framework against ransomware attacks for smart healthcare," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 18–28, 2022.

[17] A. Sengupta and M. Rathor, "Enhanced security of dsp circuits using multi-key based structural obfuscation and physical-level watermarking for consumer electronics systems," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 2, pp. 163–172, 2020.

[18] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius, "A state-of the-art survey of topsis applications," *Expert Systems with applications*, vol. 39, no. 17, pp. 13 051–13 069, 2012.

[19] S. S. Goswami, D. K. Behera, and S. Mitra, "A comprehensive study of weighted product model for selecting the best product in our daily life," *Brazilian Journal of Operations & Production Management*, vol. 17, no. 2, pp. 1–18, 2020.

[20] D. A. Hahn, A. Munir, and S. P. Mohanty, "Security and privacy issues in contemporary consumer electronics [energy and security]," *IEEE Consumer Electronics Magazine*, vol. 8, no. 1, pp. 95–99, 2018.

[21] D. Pal, V. Vanijja, X. Zhang, and H. Thapliyal, "Exploring the antecedents of consumer electronics iot devices purchase decision: a mixed methods study," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 4, pp. 305–318, 2021.

[22] Z. Kahleifeh and H. Thapliyal, "Adiabatic logic based energy-efficient security for smart consumer electronics," *IEEE Consumer Electronics Magazine*, vol. 11, no. 1, pp. 57–64, 2020.

[23] F. Ding, G. Zhu, M. Alazab, X. Li, and K. Yu, "Deep-learning-empowered digital forensics for edge consumer electronics in 5g hetnets," *IEEE consumer electronics magazine*, vol. 11, no. 2, pp. 42–50, 2020.

[24] S. Lipoff, "Paying for privacy: Increasing the privacy and security comfort of end users." *IEEE Consumer Electronics Magazine*, vol. 3, no. 3, pp. 76–78, 2014.

[25] E. L. Macedo, F. C. Delicato, L. F. de Moraes, and G. Fortino, "Assigning trust to devices in the context of consumer iot applications," *IEEE Consumer Electronics Magazine*, 2022 (early access).

[26] M. Ngoepe and M. Ngwenya, "Personal data and the assemblage security in consumer internet of things," *International Journal of Information Security and Privacy (IJISP)*, vol. 16, no. 1, pp. 1–20, 2022.