# VULNERABILITY AWARE SAFETY MECHANISM FOR IEEE 802.15.4 BASED IOT SYSTEMS

**[1]Raguram Gopalswamy, [2]S.Hemalatha**

[1]Founder,Logimax Technologies (P) Limited, Anchorvale Gardens, Singapore.E-mail: ragu@logimaxindia.com
[2]Associate Professor, Department of Computer Applications,Nallamuthu Gounder Mahalingam College, Pollachi,Tamil Nadu, India. E-mail: hemalatha@ngmc.org

**Abstract** - The protocol IEEE 802.15.4 sets several security requirements for various protection grades in the network layer. Selecting the safety level for the collection of Internet of Things (IoT) terminals is a major challenge as it decides the safety protection and affects the system's efficiency. IoT-based safety method (IoT-SM) is proposed in this research. This research suggests a safe setup method for gathering and threatening, considering the characteristics of security attacks and gathering effectiveness. The model's findings show that the suggestion can pick the appropriate safety configuration based on the system safety threats, service demands, and collected energy. The suggested technique can prolong working hours, leading to enhanced system performance, compared with current approaches. In addition, the proposed setup technique for security may also fulfill various service needs.

**Keywords** : IoT, IEEE 802.15.4, security, protection

## 1 INTRODUCTION TO THE IOT AND IEEE 802.15.4

The Internet of Things (IoT) platform is predicted to grow recently, as 5G may greatly increase the network capabilities and the quality of service (QoS) through the next generations of cellular telecommunications technologies rapidly [1]. Cisco's research showed how three times the world's population would be reached by 2022 with interconnected gadgets. IoT technologies and specifications such as the IPv6 through the Low Power Wireless Personalised Areas (6LoWPAN) and Long Distance networking have been suggested (LoRa) [2].

The IEEE 802.15.4 specification for low-price and low-rate IoT systems is among the modern technologies [3]. The hardware and media accessing control (MAC) levels are defined and used in the higher layers of mobile networks. It provides less capacity but less power than other systems, such as a Wi-fi system [4]. This standard is thus extensively used in intelligent agriculture, intelligent medicine, and even the automobile Internet.

In the IoT system, privacy concerns have received more attention as the risks from malware attacks, denial of service (DoS) assaults, and breaches have been developing dramatically over the past several times [5]. IEEE 802.15.4 specifies eight security guidelines that ensure various security and privacy grades at the link layer for IoT systems to comply with multiple applications' diverse security needs [6].

Since low energy and basic connections generally restrict end terminals of IEEE 802.15.4 systems, traditional security setup procedures usually contemplate a fixed safety grade or a randomized one which can ease safety and energy administration [7]. Furthermore, due to continuous threats to the network and future diverse security agencies, standard setup approaches are inappropriate. The safety configuration must react to network risks and collect performances with minimal complication and good energy effectiveness to offer competent security for various IoT services [8].

In IEEE 802.15.4 based IoT systems, the protection efficiency has been researched extensively. Scholars have studied and made some useful recommendations for accomplishing safety requirements established in IEEE 802.15.4 standard [9]. In addition, tests have examined the additional energy usage at different degrees of protection offered by IEEE 802.15.4. These research articles focus largely on system safety power usage and do not consider the mechanism of energy collection [10]. Because IoT gadgets have restricted capacities, the energy administration was examined and enhanced to use the collected energy optimally.

Researchers have developed ways to plan tasks that account for the changing energy supply and time limitations [11]. Therefore, these studies do not examine how to set up safety levels for IoT nodes that can be harvested. Given the efficiency of current IoT technologies in system performance optimization, maximum precision may be used to anticipate the collection of IoT end components and cybersecurity risks [12]. Thus, it makes sense to concentrate on the security settings on the gathering of IoT systems and threaten them. The Software Defining Networking (SDN) administrator precisely predicts the risk of the system because it has a complete network perspective [13].

Furthermore, depending on past data of the sensor nodes, the access points can anticipate gathering efficiency. In each time frame, the residual energy and the collecting force are then analyzed. This article determines the permitted safety arrangement based on the danger, service requirements, and excess flow. A safety setup technique is thus suggested to select appropriate fittings for the provision of safeguarded operations and maximize the duration of work in a gathering knowledgeable area.

The rest of this article as follows: Section 2 illustrates the background of the security protocols. The proposed IoT-based safety method (IoT-SM) is designed and implemented in section 3. The software analysis and performance evaluation of the proposed method are discussed in section 4. The conclusion and future scope are listed in section 5.

## 2 BACKGROUND TO THE SECURITY PROTOCOLS

Some commonly used confidence evaluation approaches have been presented from diverse viewpoints to measure cloud services' dependability [14]. One of them is the QoS-driven cloud servers' trust evaluation technique. A multi-dimensional confidence assessment method was suggested that allows cloud server credibility (CSC) to judge a cloud system participant's (CSP) reliability [15]. This solution supports CSC in selecting a CSP among the candidates which meet its required QoS needs. Soliman et al. provided a hypergraphic and bilateral fruit fly optimizing trust-centered strategy to determine appropriate and reliable CSPs [16].

Ammar et al. have put out a new cloud modeling theory-based approach and trust mechanisms [17]. Following this procedure, the CSCs pick the right cloud service using the analytical hierarchical process technique. A methodology for confidentiality assessing the confidence of CSPs was suggested, based on the quality assurance method [18]. Furthermore, it is challenging to obtain QoS information from cloud applications and often insufficient them. Moreover, cloud providers' QoS data may not be accurate. The accuracy of CSPs can thus only be determined based on the QoS level.

Evaluating the confidence of cloud computing based on CSC views (i.e., review ratings) is also popular. Alzubi et al. have called for a framework for big data handling to evaluate the confidence of cloud providers [19]. The CSC's evaluation rankings are pre-processed using a cloud brokerage with the Map Reduce architecture [20]. To detect malevolent CSCs and their response evaluations, the Probabilistic gaming model integrated a unique trust evaluation approach. The earlier is used to investigate and recognize false accounts, while the latter is utilized to detect and respond to harmful users [21]. A reputational trust monitoring model was created and applied by Noor et al. [22]. The trustworthiness of feedback assessments to safeguard cloud storage from harmful CSCs may be measured using this approach.

A minimal cloud service-based reputation assessment technique was presented. This approach employs fuzzy set theory to get cloud solutions' reputational values following CSC feedback evaluations [23]. Furthermore, in practical cloud environments, fraudulent users and dishonest feedback rankings substantially impact CSPs' credibility. Likewise, the genuine confidence of CSPs can only be achieved based on customer feedback.

Some research combining relative and absolute evaluation techniques is also available. Makhdoom et al. suggested a credible cloud provider selection methodology [24]. This methodology introduced an integrative trust evaluation approach, including a quantitative trust analysis (QoS surveillance) and a qualitative trust analysis (feedback rankings). Consequently, the unreliable calculations might incorrectly omit reputable customers and their real feedback rates [25]. A unique methodology was presented that integrates the QoS forecasts with consumer satisfaction estimates for performing cloud services trust assessments.

This approach focuses on the correctness and client satisfaction estimates for an objective cloud provider in the QoS value estimates of quantitatively trustworthy characteristics. Furthermore, the effect of the time element and the biased comments on the QoS forecasts were not considered [26]. A quality measurement technique was suggested by Ly et al. to exploit the QoS offering and CSC response rankings [27]. Although it examined both the viability and the relationship of each partner's activities, its subjective qualities were represented, and the QoS' adaptive elements were disregarded.

The article aims to pick reliable service providers by assessing the reliability-based upon in-context input from various sources, including comments from customers worldwide advisories and comments from third parties [28]. It depends heavily on personal information and does not recognize the relevance of objective factors.

In addition to the trust-mentioned evaluation methodologies, there are several more approaches for ensuring the confidentiality of the cloud infrastructure.

Alabady et al. suggested an upgraded trustworthy cloud computing platform to safeguard the condemnation and authenticity of user information and calculations [29]. This dedicated system gives safe and efficient procedures for managing virtual machines to protect them from surveillance and manipulation during transmission and to safeguard internal intruders in the virtual environment.

A novel confidence model was presented based on fuzzy cloud mathematical concepts. The reliability of public clouds has been calculated based on the characteristics and linguistic trust in the useful and unsuccessful contacts between cloud organizations. Rathore et al. presented a technique of trust measurement based on a complete cloud concept [30]. It also established the Cloud Platform Trust Framework, which sets user preferences trust level to safeguard customer information.

From work described above, many current cloud computing evaluation research has been largely divided into two groups, including QoS-based methods and feedback-based methods, which were widely utilized in the cloud platform confidence evaluation. Furthermore, this work is not considered one of the most important elements to guarantee that cloud providers are credible for cybersecurity.

The proposed model has an extensive confidence evaluation methodology that combines safety characteristics and credibility for cloud providers, unlike prior studies that don't address the security issue in cloud storage evaluations. In addition to evaluating the level of cloud computing protection, this methodology analyses the credibility of cloud systems based on CSC's comments. In addition, it can modify the confidence of cloud computing to the degree of protection and credibility.

## 3 PROPOSED IOT-BASED SAFETY METHOD (IOT-SM)

This article concentrates on IEEE 802.15.4 single-hop IoT systems that install IoT end terminals around gateways that gather information from the sensor and deliver it to the web servers. There are limited battery gateway nodes at the edge devices, while gateways are linked to the external power source. This article only considers the IoT end systems that can gather solar power, vibrations, and other renewable energies.

### 3.1 System Model

The proposed model is subdivided into three models: network model, package processing model, and power management model. Each model is explained separately in the following sections.

### 3.1.1 Network Model

IoT-SM design is considered where the sensor plane comprises multiple terminals that serve specific IoT services. Although these IoT networks might be based on many protocols, only IEEE 802.15.4 systems comprising final nodes, bridges, and server software are emphasized. The end devices are responsible for detecting the medical, commercial production, or environmental surveillance data. At the same time, the access points gather the data and deliver it to the appropriate software routers from the edge devices.

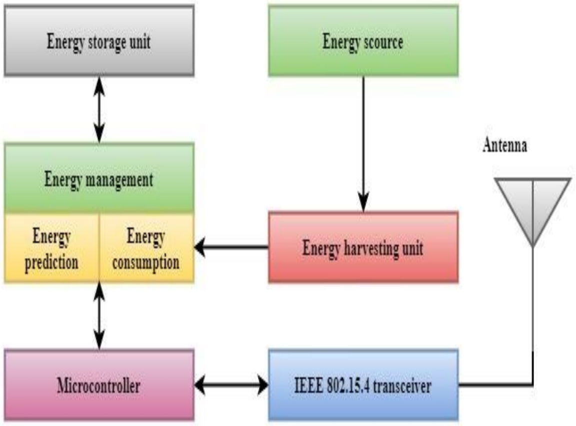

**Figure 1** The system model of the proposed IoT-SM

Fig. 1 shows the system model of the proposed IoT-SM. It has three modules. The energy storage unit is used to manage the energy prediction and energy consumption modules. The energy source is harvested using a harvesting unit and then given to the energy management unit. The transceiver module is used to transmit and receive, and it is connected with the energy management module through a microcontroller.

The end terminals and their respective gateways are topographically distributed in a star-way connection in mobile networks. The routers are also linked to the mobile networks, which are frequently utilized. The sensor gathered data through the gateways is thus sent via cellular connections to the internet. The operator can forecast the risks to the system in preparation as it has a perspective of the overall system.

### 3.1.2 Package Processing Model

The microcontroller unit is also accountable for packet computing while voltage regulation supplies the energy needed in the examined model. The messages are forwarded via the IEEE 802.15.4 transmitter and antenna units to the access points after they have been analyzed. The microcontroller must also do the verification and encrypting procedure besides creating the digital certificates.

The accepted encryption technique is the Advanced Encrypting Standards (AES) with 128-bit encryption, whereas the Messaging Integration Coding (MIC) is available in varying lengths. Precisely eight distinct security suites are established in the IEEE 802.15.4 standard to safeguard a layer of connection that may be broken down into four clusters: no protection, simply encrypting, identification, and authentication plus identification.

MIC code sizes of 32, 128, or 256 bits and package credibility can be protected by larger MIC. As an additional burden, energy usage and networking transport result from the encrypting and authenticating procedure, the selection of safety suites depends on service needs and networking risks. The remainder power must also be considered to increase the QoS.

### 3.1.3 Power Management Model

Power is extracted from the batteries and power harvesting in each endpoint. Electricity harvesting has various kinds according to renewable resources, such as solar cells, wind turbines, and other actuators. They may also be divided as per their controlled and expected nature into four sorts. The collected energy, $E_h(X)$, may usually be expressed as following within the time frame (0, X):

$$E_h\,(X) = \int_0^X \beta P_h(x)dx$$

$P_h(x)$ is the power harvested at x. $\beta$ is the effectiveness of energy conversion. Because many energy supplies are predicted, three types of harvests are considered in this article, including vibrations, radio frequency (RF), and solar. End devices for numerous IoT applications are combined as per requirements and comfort with various harvested units.

In the end, equipment used to monitor the surroundings and solar panels may be added, while vibrations collecting can be utilized for Internet of Vehicles (IoV) or even intelligent buildings. Several effective approaches such as logistic regression, exponentially flattening, and Kalman filtering has been developed to forecast future collected energy. Given the very effective and precise demonstration of these approaches, it is fair to believe that the findings of this article are included in the power predictions.

### 3.2 The Proposed IoT-SM for Gathering Energy and Protection

As noted previously, existing IoT operations have diverse security control needs. In addition, consumer operations face dynamic risks to the network. The security prevention implemented for various applications should thus be adaptable to the power limitations and the networking risks. Eight safety standards have been developed for varying degrees of safety in the IEEE 802.15.4 standard to fulfill these criteria.

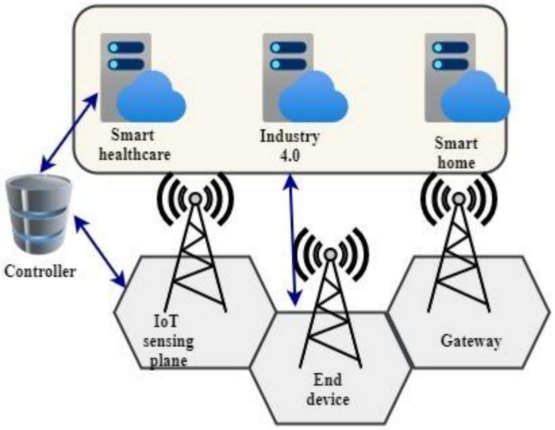

**Figure 2** The architecture of the proposed IoT-SM

Fig. 2 shows the architecture of the proposed IoT-SM. It has an IoT sensing plane, end devices to interface with users, gateway to connect with other networks. The controller is used to manage the smart healthcare network, industry 4.0, and smart home for energy harvesting and security. In today's IoT systems, the end terminals are generally configured at a predetermined degree of safety, making the setup complicated. Even while the AES 128 encryption package for all IoT operations is the safest to pick, it is not the perfect option. First of all, it uses more power and hence wastes, particularly if there are no significant or unlikely security risks within the networks when the operational demand is not met.

Furthermore, the objective for future 5G service-oriented systems that aspire to deliver varied QoS is to offer equal security. Moreover, inadequate protection often generally causes energy loss when the gathering capacity is large. An adaptable system security method must collect authorized nodes considering the various requirements, the changeable power supply, and even the evolving network risks. The recommended technique of collection is listed in the upcoming sections.

First, it constructs the cycle times to estimate the produce unit energy, denoted as X. While the gathered power varies throughout each X cycle, the harvesting energy consistent for a set time frame, which may be referred to as $\Delta x$, should be considered. In addition, the X and the $\Delta x$ values fulfill the connection is expressed in Equation (1).

$$X = n\Delta x \tag{1}$$

Where n is constant. It is believed the danger of a system may be found in cycles X, which remains unaltered in every slot of the period $\Delta x$. Since the collection energy is not accessible beyond X, it focuses on the safety setting throughout each collecting projection cycle X. The terminal node is not functioning if the remaining power cannot sustain the continual packet production for the whole $\Delta x$ slot. Furthermore, it may also assume that the operation of packet creation ceases, as IEEE 802.15.4 is employed in low-rate IoT systems when the necessary safety cannot be given. Given the threat from the system, it intends to maximize operating duration in cycle T while fulfilling the safety limit, and it is expressed in Equation (2):

$$\max x = \sum_{i=1}^{n} w_i \Delta x \tag{2}$$

Where $w_i$ shows if the component works on the gathering cycle's ith period. The timeslot is denoted as $\Delta x$. The working element is represented in Equation (3)

$$w_i \in (0,1) \tag{3}$$

Equation (4) indicates that the energy spent cannot surpass the combined batteries and harvested output power required.

$$\sum_{i=1}^{n} e_i r_i w_i \Delta x \leq E_r + E_h \tag{4}$$

In this calculation $e_i$ indicates the energy need of producing and transmitting every packet throughout this time frame $\Delta x$, which is very much connected with the selected security measures. The desired setup and the packet payload size are defined in each time frame. At the commencement of the harvested phase $S_i$, $r_i$ and $E_r$, indicate both the packet creation rate and the rest of the power.

The lower limit is expressed in Equation (5)

$$S_i \geq S_{r,i} \tag{5}$$

Moreover, $S_{r,i}$ is used to indicate the same time frame the lower limit of the protection setup stated, given the changing security attacks and diverse service requirements. The harvested phase is denoted as $S_i$. In particular, packet connectivity and confidentially security should be given for data-protected IoT systems that deal with private or corporate data, such as personal medical tracking. The safety packages should then be selected $(S_1, S_2, S_3)$ for such operations.

In contrast, just one of the three suites must safeguard messaging incorporation for privacy-insensitive IoT applications, such as environmental surveillance. This article does not suggest mode since the incorporation technique is not protected. The safety and risk may be divided into two values – low and high, preventable by the medium and maximum safety suits, and also that the fundamental protection of $S_4$ and $S_1$ is guaranteed. $S_5$ and $S_2$ should therefore be picked for responsive and unresponsive data protection services if the safety danger is significant. $S_i$ is denoted the harvesting phase.

Then it has to think about how to pick a safety system for each period of the harvested and threat-conscious cycle. Two steps are a major part of the approach. The first step is to identify the necessary safety suites following services. It initializes $i = 1$ in the examined cycle for the first period. Since the power intake must not exceed the residual power in the batteries and the power that is collected is the highest permissible energy usage, and it is calculated for each packet for the intervals between the ith and jth $\{j = i, i+1, \cdots, n\}$ time frames.

In these times, it may then compare $e_j(max)$ and $e_{S_{r,j}}$ to the maximum permitted security requirements. If $e_j(max)$ is below the minimum necessary $e_{S_{r,j}}$, the power supply is not sufficient for security. Therefore it is expected that the terminal node switches to rest in such a time frame to save power. It can retrieve the $i'$ index for the $S_k$ degree of security that is the least allowed. Thus, the permitted safety threshold is $S_{k'}$ during $i'$th primetime. The next stage is to continue the cycle to identify the backup level after $i'$. The energy required can be indicated as the equivalent in the jth period $E_{a_j}$ is expressed in Equation (6)

$$E_{a_j} = E_r + \sum_{i=1}^{j} E_{h_i} - \sum_{i=1}^{j-1} e_i r_i w_i \Delta x \tag{6}$$

The remaining energy is denoted as $E_r$, the harvested energy is denoted as $E_{h_i}$. The energy requirement, the packet creation rate, and the weight are denoted as $e_i, r_i, and\ w_i$. The tiemslot is denoted as $\Delta x$. After the suggestion, it can determine that the algorithm's runtime difficulty is $O(n^2 m)$, where n represents the size of end-nodes. Generally, the value of n is modest and meets $n >> m$. In addition, each gateway carries out the time difficulty computation for the edge devices of its covering. The primary overall calculation is thus predicted by the danger of networks and by the power collected.

The first portion is carried out by the software-defined network (SDN) control module, which typically comprises sufficient calculation resources and contains an insight into the whole network. The latter is carried out using the gateways, which have minimal complication and good precision for Kalman filtering and nonlinear analysis techniques. Furthermore, the harvested forecast of the edge devices within its range is solely accountable for every gateway, which minimizes the further complication.

## 4 SOFTWARE ANALYSIS AND EVALUATION

The simulation is carried to assess the effectiveness after presenting the idea. It assumes a mobile network comprising three neighboring mega cells covered by 5km x 5km. Various IoT terminals are installed and linked with multiple standards for each macrocell. It exclusively concentrates on the IoT system configurations based on IEEE 802.15.4 and presumes that 200 terminal nodes and 40 access points are equally distributed.

**Table 1** Simulation metrics

| Metrics | Value |
|---|---|
| **Payload size** | 52Bytes |
| **Frequency** | 2.4GHz |
| **Sending rate** | 300Kbps |
| **Battery capacity** | 80mJ |
| **Number of nodes** | 200 |
| **Gateway** | 40 |

Table 1 shows the simulation metrics of the proposed model. The simulation is analyzed using Network simulator 2. The parameters such as frequency, number of nodes, number of gateways are mentioned in the above table.

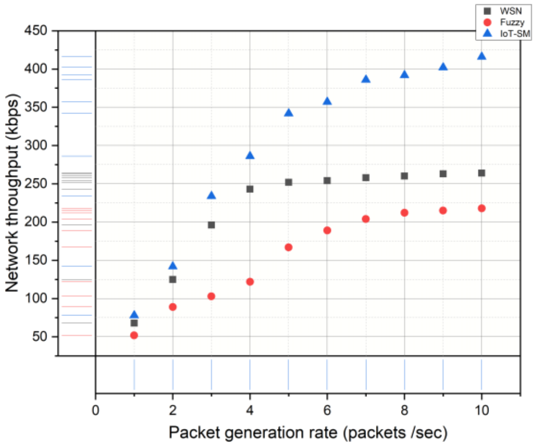

**Figure 3** Network throughput analysis of the proposed IoT-SM

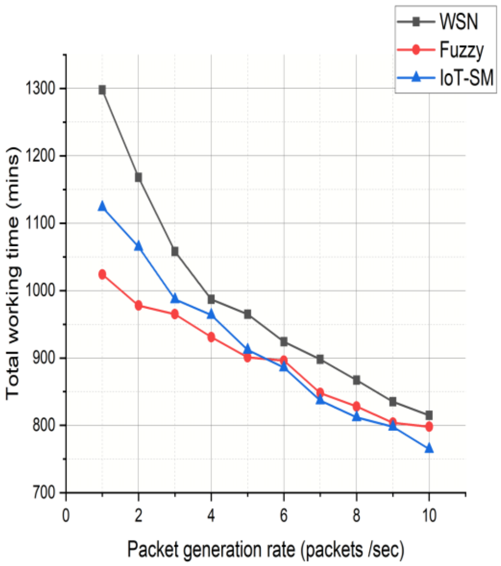

**Figure 4** Total working time analysis of the proposed IoT-SM

Fig. 3 shows the network throughput analysis of the proposed IoT-SM. The simulation is carried out by varying the packet generation rate from 1 to 10 packets/second. The respective performance of the proposed IoT-SM is evaluated and compared with the existing models cush as wireless sensor network (WSN) and fuzzy. The results indicate that the proposed IoT-SM IoT-SM has higher throughput than the current models. As the packet generation rate increases, the number of received packets also increases, enhancing the throughput.

Fig. 4 shows the total working time analysis of the proposed IoT-SM. The simulation has analyzed the performance of the proposed IoT-SM and compared it with the existing models such as WSN and fuzzy. The simulation is run for one week, and the result is calculated and plotted in the above figure. The result indicates that the proposed IoT-SM has an average total working time which results in a moderate level of energy consumption than the existing models. Total working time is calculated as the variation of the change in packet generation rate.

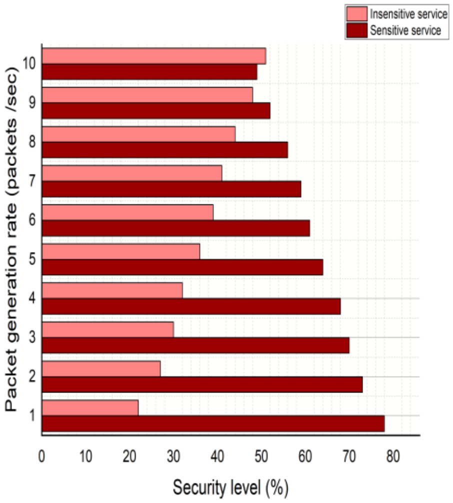

**Figure 5** Security level analysis of the proposed IoT-SM

Fig. 5 shows the security level analysis of the proposed IoT-SM. The simulation is carried out by varying the number of packets generated from 1 packet/second to 10 packets/second. The respective performance of the proposed IoT-SM is analyzed for the sensitive service and insensitive service and plotted in the above figure. The findings show that the proposed IoT-SM has the highest security. As the packet generation rate increases, the security level decreases.

The proposed IoT-SM is implemented, analyzed, and performance is evaluated in this section. The simulation outcomes such as total working time, security level, and network throughput of the proposed IoT-SM are analyzed and compared with the existing models. The results show that the proposed IoT-SM has the highest performance of the current models.

## 5 CONCLUSION AND FINDINGS

This article presents a safeguarding technique for harvesting and threats used in the IoT systems based on IEEE 802.15.4. IoT-based safety method (IoT-SM) is proposed in this research. Every IoT device in the analyzed network can modify its safety settings to the anticipated danger, provided services and energy required. The simulated findings show that the method presented can enhance working hours, which improves overall performance. The study also demonstrates that this approach may deliver IoT solutions with sufficient security guarantees.

## References

[1] Hassan, W. H., “Current research on the Internet of Things (IoT) security: A survey”, Computer networks, Vol. 148, pp. 283-294, 2019.

[2] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, “A survey on IoT security: application areas, security threats, and solution architectures”, IEEE Access, Vol. 7, pp. 82721-82743, 2019.

[3] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N., “Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations”, IEEE Communications Surveys & Tutorials, Vol. 21, No. 3, pp. 2702-2733, 2019.

[4] Minoli, D., & Occhiogrosso, B., “Blockchain mechanisms for IoT security”, Internet of Things, Vol. 1, pp. 1-13, 2018.

[5] Khan, M. A., & Salah, K., “IoT security: Review, blockchain solutions, and open challenges”, Future Generation Computer Systems, Vol. 82, pp. 395-411, 2018.

[6] Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., & Pustišek, M.,“Towards decentralized IoT security enhancement: A blockchain approach”, Computers & Electrical Engineering, Vol. 72, pp. 266-273, 2018.

[7] Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., & Imran, M. ,“Deep learning and big data technologies for IoT security”, Computer Communications, Vol. 151, pp. 495-517, 2020.

[8] Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A.,“An efficient Lightweight, integrated Blockchain (ELIB) model for IoT security and privacy”, Future Generation Computer Systems, Vol. 102, pp. 1027-1037, 2020.

[9] Sha, K., Yang, T. A., Wei, W., & Davari, S.,“A survey of edge computing-based designs for IoT security”, Digital Communications and Networks, Vol. 6, No. 2, pp. 195-202, 2020.

[10] Kumar, V., Jha, R. K., & Jain, S.,“NB-IoT security: A survey”, Wireless Personal Communications, Vol. 113, No. 4, pp. 2661-2708, 2020.

[11] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P.,“LSB: A Lightweight Scalable Blockchain for IoT security and anonymity”, Journal of Parallel and Distributed Computing, Vol. 134, pp. 180-197, 2019.

[12] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S.,“Survey on IoT security: challenges and solution

using machine learning, artificial intelligence, and blockchain technology", Internet of Things, 2020.

[13] Latvala, S., Sethi, M., & Aura, T., "Evaluation of out-of-band channels for IoT security", SN Computer Science, Vol. 1, No. 1, pp. 1-17, 2020.

[14] Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., & Chen, D., "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach", IEEE Access, Vol. 7, pp. 9368-9383, 2019.

[15] Mukherjee, B., Wang, S., Lu, W., Neupane, R. L., Dunn, D., Ren, Y.,& Calyam, P., "Flexible IoT security middleware for end-to-end cloud–fog communication", Future Generation Computer Systems, Vol. 87, pp. 688-703, 2018.

[16] Soliman, S., Jaela, M. A., Abotaleb, A. M., Hassan, Y., Abdelghany, M. A., Abdel-Hamid, A. T., & Mostafa, H., "FPGA implementation of dynamically reconfigurable IoT security module using algorithm hopping", Integration, Vol. 68, pp. 108-121, 2019.

[17] Ammar, M., Russello, G., & Crispo, B. "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications, Vol.38,pp. 8-27, 2018.

[18] Hou, J., Qu, L., & Shi, W. "A survey on internet of things security from data perspectives", Computer Networks, Vol.148, pp.295-306, 2019.

[19] Alzubi, O. A., Alzubi, J. A., Dorgham, O., & Alsayyed, M. "Cryptosystem design based on Hermitian curves for IoT security", The Journal of Supercomputing, Vol. 76, No. 11, pp. 8566-8589, 2020.

[20] Park, K. C., & Shin, D. H. "Security assessment framework for IoT service", Telecommunication Systems, Vol.64,No.1,pp.193-209, 2017.

[21] Wang, H., Zhang, Z., & Taleb, T. "Special issue on security and privacy of IoT", World Wide Web, Vol. 21, No. 1, pp. 1-6, 2018.

[22] Kumar, N. M., & Mallick, P. K. "Blockchain technology for security issues and challenges in IoT", Procedia Computer Science, Vol. 132, pp. 1815-1823, 2018.

[23] Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. "Security, privacy & efficiency of sustainable cloud computing for big data & IoT",Sustainable Computing: Informatics and Systems, Vol. 19, pp. 174-184, 2018.

[24] Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. "Blockchain's adoption in IoT: The challenges, and a way forward", Journal of Network and Computer Applications, Vol. 125, pp. 251-279, 2019.

[25] Kimani, K., Oduol, V., & Langat, K. "Cybersecurity challenges for IoT-based smart grid networks", International Journal of Critical Infrastructure Protection, Vol. 25, pp. 36-49, 2019.

[26] Bujari, A., Furini, M., Mandreoli, F., Martoglia, R., Montangero, M., & Ronzani, D. "Standards, security and business models: key challenges for the IoT scenario", Mobile Networks and Applications, Vol. 23, No. 1, pp. 147-154, 2018.

[27] Ly, P. T. M., Lai, W. H., Hsu, C. W., & Shih, F. Y. "Fuzzy AHP analysis of Internet of Things (IoT) in enterprises", Technological Forecasting and Social Change, Vol. 136, pp. 1-13, 2018.

[28] Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N., & Boukerche, A. "A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications",Future Generation Computer Systems, Vol. 104, pp. 105-118, 2020.

[29] Alabady, S. A., Al-Turjman, F., & Din, S. "A novel security model for cooperative virtual networks in the IoT era.", International Journal of Parallel Programming, Vol. 48, No. 2, pp. 280-295, 2020.

[30] Rathore, S., Kwon, B. W., & Park, J. H. "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network", Journal of Network and Computer Applications, Vol. 143, pp. 167-177, 2019.