ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20230602000691
Original scientific paper

Support Vector Machine Classification using Proximity Authentication and Surveillance System in IoT Industrial Network

Salem Jeyaseelan W. R. *, Sudhakaran P., Rajakani V., Parameswari A.

Abstract: This research focuses on developing a proximity-based authentication and surveillance system using Internet of Things (IoT) devices in industrial networks. The system aims to improve security measures by ensuring only authorized personnel have access to critical areas of the network. Researching authentication mechanisms and protocols, examining network authentication system features and application environments, and developing an online-based, real-time monitoring authentication system are the goals of this article. The system will utilize sensors and cameras installed in strategic locations to detect and track personnel movement within the network. When a person approaches a secured area, their identity will be verified using proximity-based authentication using RFID technology. The system will also monitor and record any suspicious activity, providing real-time alerts to security personnel. To detect malicious behavior on short-range, low-rate, and low-power networks, such as those found in the Internet of Things (IoT), we advise utilizing SVM models. The proposed system is expected to increase security and reduce the risk of unauthorized access to industrial networks, ultimately enhancing overall network reliability and safety. The results are compared with various parameters.

Keywords: authentication; industrial network; internet of things (IOT); proximity; reliability and safety; RFID

1 INTRODUCTION

The internet of things (IoT) has revolutionized the way devices communicate and interact with each other, providing unprecedented connectivity and automation. This has led to the widespread adoption of IoT devices in industrial networks, where they are used for various applications such as monitoring, control, and optimization of processes.

However, the increasing number of IoT devices in industrial networks has also raised security concerns. Traditional security mechanisms, such as passwords and usernames, are no longer sufficient to protect these devices from unauthorized access, as they can be easily compromised. As a result, there is a growing need for more advanced security measures that can provide better protection against cyber threats.

In this project, we propose the use of proximity authentication and surveillance as a means of securing IOT devices in industrial networks. Proximity authentication involves using physical proximity as a factor in the authentication process. This can be achieved by equipping IOT devices with sensors such as RFID or Bluetooth, which can be used to detect the presence of authorized personnel or devices.

Background knowledge on authentication and SVM is provided in Section 2. The method for developing IDS using SVM is presented in Section 3, and the training and evaluation outcomes of the suggested solutions are presented in Section 4. The current work is concluded in Section 5.

2 RELATED WORK

Many research works have investigated the problem of security issues in industries.

Proximity Based IoT Device Authentication by Jiansong Zhang et al., [1]. This paper proposes a proximity authentication scheme for mobile devices in IoT-based industrial applications that uses Bluetooth Low Energy (BLE) technology to verify the proximity of the device to the access point. The proposed scheme was tested in a real industrial environment and showed improved security and convenience compared to traditional authentication methods.

In order to overcome this problem, this paper introduces a single IoT framework built on the MobilityFirst future Internet architecture that places a clear emphasis on enabling IoT security. With the help of our design, local IoT systems can be connected to the global Internet without sacrificing usability, interoperability, or security. In particular, we developed an IoT middleware layer that links local IoT devices' heterogeneous hardware to the worldwide Mobility First network [2].

IoT that uses physical proximity between devices to authenticate and establish a secure key [3]. The proposed protocol was evaluated using simulation and showed improved security compared to traditional methods.

In order to overcome this problem, this paper introduces a single IoT framework built on the Mobility First future Internet architecture that places a clear emphasis on enabling IoT security. With the help of our design, local IoT systems can be connected to the global Internet without sacrificing usability, interoperability, or security. In particular, we developed a IoT middleware layer that links local IoT devices' heterogeneous hardware to the worldwide Mobility First network [4].

This study aims to present a collection of fresh research paths and concepts for 5G/6G enabled IoT and new IoT technology developments. A variety of issues are currently being faced by the IoT, including access to a large number of IoT devices, network performance, security, standardization, and key applications [5].

Artificial Intelligence (AI)-based algorithms can utilize data gathered from IoT-based smart fitness devices and users to improve training results. Another noteworthy subject that may be applied by social IoT, which can share information, expertise, and training experiences of users from various places and times, is sensor-to-sensor relations [6].

Numerous studies are being performed to solve the security issue posed by IOT, including but not limited to those utilizing edge/fog computing, machine learning, and block chains. In order to safeguard the network against

hostile users, authentication and authorization are crucial parts of the CIA trinity. However, due to the size of IoT networks and the limited resource availability of devices, existing authorization and authentication techniques are insufficient for dealing with security [7].

Researchers indicate that an intruder may calculate prior-established session keys and that the application of a constant pseudo-identity in the scheme allows the user to be observed. We provide a novel authentication method for multi-gateway-based WSNs rather than attempting to rectify a flawed technique. Then, we use Prove if to demonstrate the proposed scheme's security and the NS-2 simulation to assess the scheme's performance [8].

To efficiently verify a single tag, this protocol relies on the Physical Unclonable Functional (PUF) and lightweight cryptography. The protocol has the following steps: update, mutual verification, and tag identification [9].

By using software-defined radios that operate in 5G frequency bands and a 1-bit RIS with 64 × 64 sections, the effectiveness of the suggested system is tested in real-world applications. The outcomes show enhanced key extraction efficiency and heightened defense against denial-of-service attacks [10].

The pairing protocol's energy consumption is reduced while still achieving acceptable security performance by solving an optimization problem [11-15]. A possible method for enabling safe pairing of a IoT device with a wireless network is proximity-based device authentication [16]. Existing networks, however, do not consciously take into account energy efficiency or the trade-off between energy use and security level during the pairing process. By improving the energy efficiency and analyzing the trade-off between energy consumption and security strength of an existing proximity-based IoT device authentication protocol called Move2Auth, this research fills the security gap mentioned earlier.

In this paper, we present DC-IIoT, a distributed control plane-based authentication protocol that is efficient and secure for IIoT-based applications [16]. By incorporating physically distributed and logically centralized SDN controllers, DC-IIoT may accomplish the required security and design features and eliminate single points of failure.

To begin effective packet transmission, network and routing assumptions are created in the first step of the study. To maximize energy efficiency, stability metric for the cluster is established in the second step. For the analysis of network stability, two cluster metrics are used. The third phase involves initializing the ideal cluster design model to balance network integrity and energy efficiency [17].

Instead of producing several random phase sequences, the SM-OHOCO algorithm produces a better result with fewer searching rounds, highlighting the creativity of the effort. The OHOCO method is utilized since the phase sequence optimization of the SLM technique is thought to be an NP-hard optimization problem [18]. The principles of the HOCO algorithm and the oppositional-based learning (OBL) technique were combined to create this method. This survey paper provides an overview of the security challenges and solutions for Industrial IoT, including proximity authentication and surveillance. The authors discuss the importance of secure authentication and surveillance mechanisms in ensuring the security and privacy of Industrial IoT applications.

This paper proposes a secure and efficient proximity-based authentication and key agreement scheme for Industrial IoT that uses both physical proximity and a shared secret key to authenticate devices and establish a secure key [19]. The proposed scheme was evaluated using simulation and showed improved security and efficiency compared to traditional method.

The current work proposed a two-step machine learning strategy built on our previously established optimization algorithm and the support vector machine classifier in order to decrease the forecast time and address the second and third constraints [24-25].

These are the issues identified in existing works.

- Lack of visibility.
- Limited security integration.
- Improve network visibility.
- Lack of physical security is available. Attackers can sometimes make physical changes in IoT devices located in remote places for long periods of time.
- By monitoring and responding to emergency situations more quickly and effectively, the Internet of Things can assist to improve public safety.

This new methodology used to solve the above existing issues, and comparative results are given in result sections. This methodology increases visibility and security, and quick response for emergency situations.

3 PROPOSED METHODOLOGY

A proposed Methodology for proximity authentication and surveillance in industrial networks using IoT devices would typically consist of several components.

IoT devices: The system would include IoT devices equipped with sensors and communication capabilities to enable proximity authentication and surveillance. These devices would be connected to the industrial network and would be capable of transmitting data to other components of the system.

Proximity authentication: The system would use one or more of the existing methods for proximity authentication, such as RFID, Bluetooth, Wi-Fi, or biometric authentication, to identify and authenticate IoT devices as they move through the network. The authentication process would control access to sensitive areas and ensure that only authorized devices are allowed to operate within the network.

Surveillance: The system would include surveillance components, such as cameras or other sensors, to monitor the environment and detect potential security threats. The surveillance data would be processed and analyzed in real-time to identify and respond to potential threats.

Data analytics: The system would use data analytics techniques to process and analyze the data collected by the IoT devices and surveillance components. This would enable the system to identify patterns and trends in device behavior and detect anomalies that could indicate potential security threats.

RFID readers are network-connected, portable or fixed devices. It uses radio waves to send impulses that activate the tag. When the tag is triggered, it transmits a wave back to the antenna, which converts it to data. The transponder is housed within the RFID tag [23].

Alerting and response: The system would be capable of generating alerts and responding to potential security threats in real-time. This would enable industrial workers to quickly respond to potential security breaches and take appropriate action to mitigate the risk.

3.1 System Architecture

The input of the Arduino Uno can be used to determine the environment. Here, lots of sensors serve as the input, and these sensors can influence their environment by managing motors, lights, other actuators, etc.

You can connect the DHT11 Digital Temperature and Moisture Sensor Device with LED to the Arduino controller and get readings for both moisture and temperature in the region around it [20].

Rapid Identity MFA (Multi-factor Authentication) identifies the user's information with RFID authentication once the user conveys the RFID device to a linked reader, such as a USB, embedded, or PC Express reader. No username is essential, but the user may be asked to provide a PIN or passcode as a choice.

In order to detect pollutants between a satellite and the ground, air quality sensors observe the energy that is emitted or reflected from the ground and the atmosphere.

Using the IDE (Integrated Development Environment) and the Arduino programming language, the ATmega328 microcontroller on the Arduino board may be programmed. The proposed method is shown in Fig. 1.

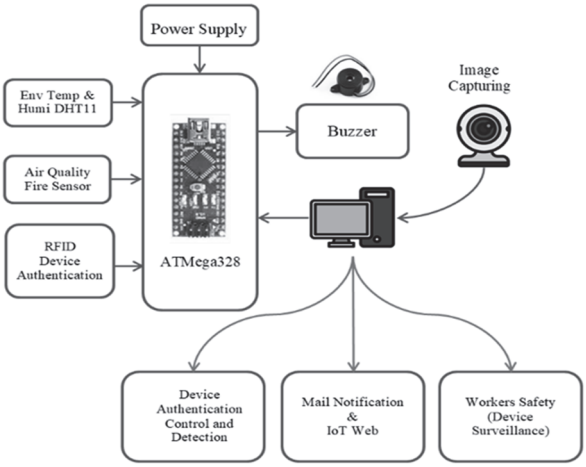

Figure 1 Proposed method block diagram

3.2 Proximity Based Access Control (PBAC)

Proximity-based access control algorithms can be used in IoT devices to provide secure access to devices and monitor the network for potential security breaches.

Proximity-based access control algorithms use proximity sensors to detect the presence of an authorized device or user within a certain range of a secured area [16]. Here are some common mathematical equations used in proximity-based access control algorithms.

3.2.1 Signal Strength

The signal strength equation is used to calculate the received signal strength at the receiver in Eq (1).

$$Signal\ strength = P_T - 10 \cdot n \cdot \log(d) + G_T + G_R \quad (1)$$

where P_T is the transmitted power, n is the path loss exponent, d is the distance between the transmitter and receiver, G_T is the gain of the transmitter antenna, and G_R is the gain of the receiver antenna.

3.2.2 Signal-to-Noise Ratio (SNR)

Where Noise is the background noise level. The SNR equation is used to measure the quality of the received signal in Eq. (2).

$$SNR = Signal\ strength / Noise \quad (2)$$

3.2.3 Proximity Detection

The proximity detection equation is used to determine whether an authorized device or user is within range of the secured area in Eq. (3).

$$Proximity\ detection = f(SNR, distance\ threshold) \quad (3)$$

where f is a function that determines whether the received signal strength and SNR are sufficient to establish proximity within a certain *distance threshold*.

3.2.4 Authentication

These equations are used in various combinations to implement proximity-based access control algorithms in IIoT applications such as secure building access, asset tracking, and personnel safety monitoring.

$$Authentication = f(proximity\ detection, access\ control\ list) \quad (4)$$

where f is a function that checks whether the detected device or user is authorized to access the secured area based on the access control list in Eq. (4). The authentication equation is used to grant or deny access based on the proximity detection and access control list.

3.3 Support Vector Machine (SVM)

Support Vector Machines (SVMs) can be used in IoT devices for surveillance in industrial network to detect and classify potential security breaches based on data collected from various sensors and devices in the network. Here are some ways SVMs can be implemented.

Anomaly detection: SVMs can be used to detect anomalies in the data collected from IoT devices in the network. The algorithm can be trained on normal patterns of behavior and then used to detect any deviations from those patterns. This can be useful in detecting potential security breaches or abnormal behavior that could indicate an attack.

Classification: SVMs can be used to classify data into different categories based on their features. For example, data collected from sensors can be classified as either normal or malicious based on certain features such as the

time of day, the location of the sensor, or the type of data collected.

Intrusion detection: SVMs can be used to detect potential intrusions in the network. The algorithm can be trained on normal patterns of behavior and then used to detect any deviations from those patterns that could indicate an intrusion attempt [21-22].

Predictive maintenance: SVMs can be used to predict when a device or system may fail based on the data collected from sensors in the network. This can be useful in preventing downtime and minimizing the risk of security breaches caused by a failure in the system.

The SVM classification model can be represented by the following equations.

3.3.1 Decision Function

In Eq. (5), x is the feature vector of the input data, w is the weight vector, b is the bias term, and sign is the sign function denoted.

$$f(x) = \text{sign}\left(w^T x + b\right) \tag{5}$$

3.3.2 The Objective Function

Where C is the regularization parameter, ξ_i are the slack variables, and y_i is the class label of the i^{th} training example shown in Eq. (6) and Eq. (7). The objective function is minimized to find the optimal hyperplane that maximally separates the two classes while also minimizing the classification error.

$$\text{Minimize}: 1/2 \left\|w\right\|^2 + C\sum_{i=1}^{m} \xi_i \tag{6}$$

$$\text{Subject to: } y_i\left(w^T x_i + b\right) \geq 1 - \xi_i \text{ and } \xi_i \geq 0 \text{ for } i = 1, ..., m \tag{7}$$

3.3.3 The Dual Problem

In Eq (8) and Eq. (9) α_{iw} are the Lagrange multipliers, and the solution of the dual problem can be used to obtain the weight vector w and bias term b.

$$\text{Maximize:} \sum i=1^m \cdot \alpha_{i-1/2} \sum i=1^m \sum j=1^m \alpha i \alpha j y i y j x i T x j \tag{8}$$

$$\text{Subject to: } 0 \leq \alpha i \leq C \text{ and } \sum i=1 m \alpha i y i = 0 \text{ for } i = 1, ..., m \tag{9}$$

3.3.4 The Kernel Function

The kernel function allows for efficient computation of the decision function without having to explicitly compute the feature mapping function as shown in Eq. 10.

$$K\left(x_i, x_j\right) = \varphi\left(x_i\right) T\, \varphi\left(x_j\right) \tag{10}$$

where φ is a feature mapping function that maps the input data into a higher-dimensional space where it is more separable.

3.4 Design Workflow

According to the design flow, we must gather IOT input via data collection devices and then pre-process it by converting the raw data into a usable format. The extraction of features the kernel trick is a method used by SVM in which the kernel converts a low-dimensional input space into a higher-dimensional space. To put it simply, the kernel raises the number of dimensions in a problem to make it separable. SVM is more potent, adaptable, and accurate as a result.

The majority of the time, as a result of the many services and contents made available via mobile devices, these devices have been clogged with crucial personal user information. As a result, hackers are targeting mobile devices in addition to the current PC and Internet environments. In this study, we use a linear support vector machine (SVM) to identify the effectiveness of SVM in detecting malware in comparison to other machine learning classifiers. We demonstrate that the SVM outperforms alternative machine learning classifiers through experimental validation.

The handling and controlling of alerts can be made simpler via anomaly detection. An anomaly alert will track the prior reading of the metric and be triggered when the metric has an anomalous value compared to the past, rather than setting precise conditions on measurements that may not be known in advance or change as data changes. Setting an anomaly on a run length is a common example; when the run duration reaches an excessively high value, an alarm is sent.

The authentication process is not only more safe and reliable when location is included as a mandatory authentication factor, but it can also be made to feel much more natural and incorporated into the user's workflows. Both time-coding and geo-location factors and our own special dynamic proximity factors are included in proximate solutions, allowing for the incorporation of true real-time close-in proximity factors.

Greater visibility, which can result in quicker and more focused issue responses, is the value that continually tracking delivers to your operations.

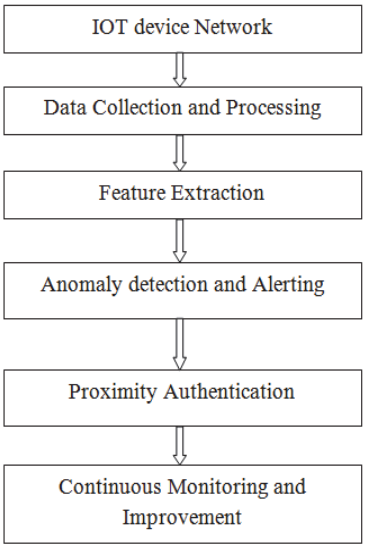

Figure 2 Proposed method design workflow

The Arduino IDE is used to programme the microcontroller in the Arduino board so that it can connect to a sensor network, receive its data, and then transfer that data over a Wi-Fi network after pre-processing. Steps must be completed in order for the sensor gearbox to be successfully shown in Fig 2. To make the system more sophisticated, adaptable, and efficient, the services or data on the servers are provided via the Internet and made accessible to clients via cutting-edge mobile phones, internet browsers, or other internet browser devices.

4 RESULTS

The serial connection on the RFID is used to transfer data between the Arduino Uno and the device. After that, the database that has been created is synchronized with the data that the sensor has successfully captured. The data are then displayed in a web form so that the user may better comprehend them after they have been successfully entered in the database. The connection is wireless or Wi-Fi, and by maintaining an internet connection, this instrument can be operated remotely without the need for human interaction and can display real-time data in line with the previously discussed IoT concept. By visiting the website, users can view this update on the air quality.

The results of our simulation studies are presented in this section.

The hardware system's results IIOT Device turns on for authorized user was implemented in a prototype with a little house outfitted with every system function, as shown in Fig. 2.

All of the sub-systems can function properly based on the implementation and validation processes of the intended system. The system can unlock the network using a password and can detect RFID cards that are coupled with notification systems by sending emails to family members in the home security area.

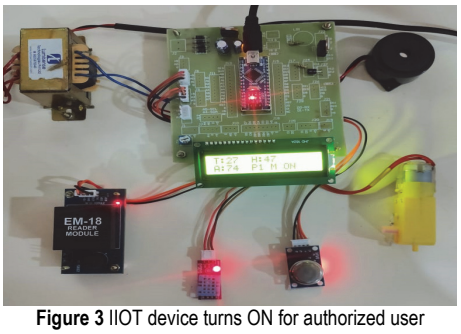

Figure 3 IIOT device turns ON for authorized user

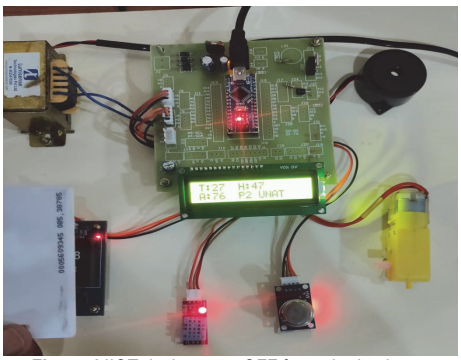

Figure 4 IIOT device turns OFF for authorized user

Fig. 3 explains that the hardware results of IIOT Device turn ON for authorized user, when we are giving the input from RFID tag.

The simulation results between IoT sensors with Temperature, real time monitoring of sensors using IOT web are shown in Fig. 5.

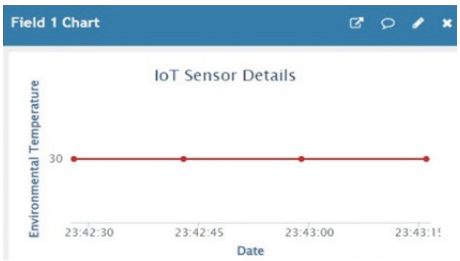

Figure 5 Real time monitoring of IoT sensors with temperature

The unit of date is taken as horizontal axis (here date is consired with time for validation), Environmental temperature in y axis. IoT sensors can provide accurate real-time data on the environment around us, allowing us to better understand how we affect the environment and take measures to improve city quality of life. Environmental sensors have become smaller and less expensive. The quantitative measures of compared values are shown in Tab. 1.

Table 1 IoT sensors with environmental temperature, real time monitoring of sensors

S.No	Environmental temperature	Real time on date
1	30 °C	23:42:30
2	30 °C	23:42:45
3	30 °C	23:43:00
4	30 °C	23:43:15

The simulation results between IoT sensors with humidity, real time monitoring of sensors using IOT web are shown in Fig. 6.

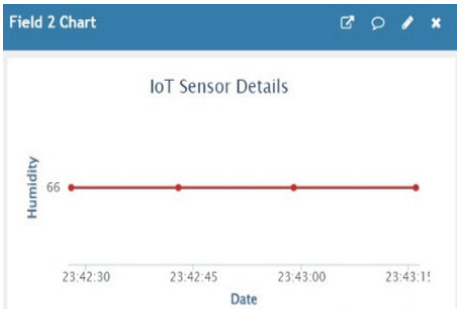

Figure 6 Real time monitoring of IoT sensors with humidity

An efficient system that includes temperature and relative humidity sensors for measurement is a smart Internet of Things-based temperature and humidity real-time monitoring and reporting system. The relative value of IoT sensors with humidity, real time monitoring details are shown in Tab. 2.

Table 2 IoT sensors with humidity, real time monitoring of sensors

S.No	Humidity	Real Time on date
1	66 °C	23:42:30
2	66 °C	23:42:45
3	66 °C	23:43:00
4	66 °C	23:43:15

The simulation results between IoT sensors with air quality, real time monitoring of sensors using IOT web are shown in Fig. 7.

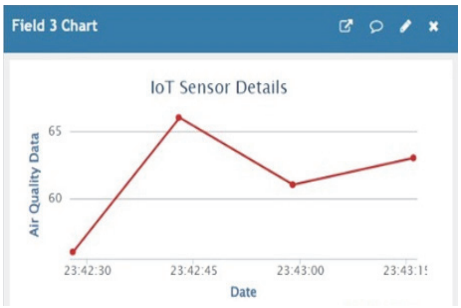

Figure 7 Real time monitoring of IoT sensors with air quality

Chemicals such as ozone and particulate matter, both of which are dangerous to human health and the environment, are detected by air quality sensors. The comparative values of the IoT sensors with air quality data, real time monitoring of sensors are shown in Tab. 3.

Table 3 IoT sensors with air quality data, real time monitoring of sensors

S.No	Air quality data	Real Time on date
1	2 °C	23:42:30
2	66 °C	23:42:45
3	61 °C	23:43:00
4	63 °C	23:43:15

The experiment's objective was to install a platform for monitoring indoor air quality for the first time. Smart-Air effectively identified the interior air quality state and showed it via the web and software after wirelessly transmitting the observed data to the web server. Additionally, the data were saved in the web server's database in the manner intended so that future research on trends in air quality could be done.

5 CONCLUSION

An IoT device proximity authentication and surveillance system in an industrial network is a critical component in ensuring the safety and security of the network. The use of advanced technologies such as Support Vector Machine (SVM) algorithm can enhance the system's ability to detect and prevent unauthorized access and potential cyber-attacks. The system's accuracy, reliability, scalability, and cost-effectiveness should be evaluated to ensure that it is an effective solution for the industrial network. By continuously monitoring and improving the system, it can adapt to new threats and challenges and maintain its effectiveness over time. Overall, the implementation of an IoT device proximity authentication and surveillance system in an industrial network can help prevent security breaches, ensure the safety of the network, and provide peace of mind for system administrators and users alike. Future investigations might focus on finding malware that is almost impossible to identify using resource data and a more accurate system. Because mobile malware is changing and appearing in a range of variations and new forms, more research on a technique that could detect future malware should be planned. Future development may make advantage of the highly energy-efficient Bluetooth Low Energy (BLE) technology. Compared to RFID, BLE is more flexible and easier to implement, however it is less precise. It is a crucial investment for any industrial network project to ensure its long-term success and sustainability.

6 REFERENCES

[1] Zhang, J., Wang, Z., Yang, Z., & Zhang, Q. (2017). Proximity Based IoT Device Authentication. *IEEE INFOCOM 2017 IEEE Conference on Computer Communications.* https://doi.org/10.1109/INFOCOM.2017.8057145

[2] Liu, X., Trappe, W., Zhao, M., Li, S., & Zhang, F. (2017). A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet*, *9*(3), 27. https://doi.org/10.3390/fi9030027

[3] Qureshi, U. M., Hancke, G. P., Gebremichael, T., Jennehag, U., Forsström, S., & Gidlund, M. (2018). Survey of Proximity Based Authentication Mechanisms for the Industrial Internet of Things. *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society.* https://doi.org/10.1109/IECON.2018.8591118

[4] Tange, K., Donno, M. D., Fafoutis, X., & Dragoni, N. (2020). A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Communications Surveys & Tutorials*, *99*, 1-1. https://doi.org/10.1109/COMST.2020.3011208

[5] Li, S., Iqbal, M., & Saxena, N. (2022). Future Industry Internet of Things with Zero-trust Security. *Information Systems Frontiers.* https://doi.org/10.1007/s10796-021-10199-5

[6] Farrokhi, A., Farahbakhsh, R., Rezazadeh, J., & Minerva, R. (2021). Application of Internet of Things and artificial intelligence for smart fitness: A survey. *Comput. Netw*, 189, 107859. https://doi.org/10.1016/j.comnet.2021.107859

[7] Ahmed, K. I., Tahir, M., Habaebi, M. H., Lau, S. L., & Ahad, A. (2021). Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction, *Sensors*, *21*(15), 5122. https://doi.org/10.3390/s21155122

[8] Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K. K. R., Wazid, M., & Das, A. K. (2017). An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. *J. Netw. Comput. Appl*, *89*, 72-85. https://doi.org/10.1016/j.jnca.2016.12.008

[9] Xu, H., Ding, J., Li, P., Zhu, F., & Wang, R. (2018). A lightweight RFID mutual authentication protocol based on physical unclonable function. *Sensors*, *18*, 760. https://doi.org/10.3390/s18030760

[10] Mahmoud, A., Shawky, S. T. S. Q. H., & Abbasi, M. H. (2023). RIS-Enabled Secret Key Generation for Secured Vehicular Communication in the Presence of Denial-of-Service Attacks. *Sensors (Basel)*, *23*(8), 4104. https://doi.org/10.3390%2Fs23084104

[11] Osamh I. K. & Abdul, S. (2020). Energy-Efficient Routing and Reliable Data Transmission Protocol in WSN. International *Journal of Advances in Soft Computing and its Application*, *12*(3), 45-53.

[12] Zhang, M. & Chong, P. H. J. (2009). Performance Comparison of Flat and Cluster-Based Hierarchical Ad Hoc Routing with Entity and Group Mobility. *Proc. of IEEE Communications Society Conference on Wireless Communications & Networking*, 2450-2455. https://doi.org/10.1109/WCNC.2009.4917894

[13] Ganesh Kumar, K. & Sengan, S. (2020). Improved Network Traffic by Attacking Denial of Service to Protect Resource Using Z-Test Based 4-Tier Geomark Traceback (Z4TGT). *Wireless Personal Communications*, *114*(4), 3541-3575. https://doi.org/10.1007/s11277-020-07546-1

[14] Abdulsahib, G. M. & Khalaf, O. I. (2021). Accurate and Effective Data Collection with Minimum Energy Path Selection in Wireless Sensor Networks using Mobile Sinks. *Journal of Information Technology Management*, *13*(2), 139-153.

[15] He, Y., Zeng, K., Mark, B. L., & Khasawneh, K. N. (2023). Secure and Energy-Efficient Proximity-Based Pairing for IoT Devices. *2022 IEEE Globecom Workshops.* https://doi.org/10.1109/GCWkshps56602.2022.10008568

[16] Salam, R., Roy, P.K., & Bhattacharya, A. (2023). DC-IIoT: A Secure and Efficient Authentication Protocol for Industrial Internet-of-Things Based on Distributed, Control Plane, *Internet of Things*, 22, 100782. https://doi.org/10.1016/j.IoT.2023.100782

[17] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., & Thiruppathi, M. (2021). SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks. *Materials today: Proceedings*, *45*(2), 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

[18] Jayasankar, T. & Vinoth Kumar, K. (2022). Novel Selective Mapping with Oppositional Hosted Cuckoo Optimization Algorithm for PAPR Reduction in 5G UFMC Systems. *Tehnički vjesnik*, *29*(2), 464-471. https://doi.org/10.17559/TV-20210524085655

[19] Kamweru, P. & Robinson, O. O. (2020). Monitoring Temperature and Humidity using Arduino Nano and Module-DHT11 Sensor with Real Time DS3231 Data Logger and LCD Display. *International Journal of Engineering Research & Technology (IJERT)*, *9*(12).

[20] DHT11 humidity & temperature sensor (2018). *OSEPP Electronics.* https://www.mouser.com/ds/2/758/DHT11-Technical-Data-Sheet-Translated-Version-1143054.pdf

[21] Khan, N. A., Awang, A., & Karim, S. A. A. (2022). Security in the Internet of Things: A review. *IEEE Access*, *10*, 104649-104670. https://doi.org/10.1109/ACCESS.2022.3209355

[22] Sengan, S., Khalaf, O. I., Priyadarsini, S., Sharma, D. K., Amarendra, K., & Hamad, A. A. (2021). Smart healthcare security device on medical IoT using Raspberry Pi. *International Journal of Reliable and Quality E-Healthcare*, *11*(3), 1-11. https://doi.org/10.4018/IJRQEH.289177

[23] Ali Abdullah, S., Al Qahtani, Alamleh, H., & Smadi, B. A. (2022). IoT Devices Proximity Authentication In Ad Hoc Network Environment. *IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).* https://doi.org/10.1109/IEMTRONICS55184.2022.9795787

[24] Sobhanzadeh, Y. M. & Moghaddam, S. E. (2022). A real-time IoT-based botnet detection method using a novel two-step feature selection technique and the support vector machine classifier. *Computer Networks*, *109365*. https://doi.org/10.1016/j.comnet.2022.109365

[25] Ioannou, C. & Vassiliou, V. (2021). Network Attack Classification in IoT Using Support Vector Machines. *J. Sens. Actuator Netw.*, *10*(3), 58. https://doi.org/10.3390/jsan10030058

Contact information:

Salem Jeyaseelan W. R., Assistant professor
(Corresponding author)
Department of Information Technology,
PSNA College of Engineering and Technology (Autonomous),
Dindigul
E-mail: salemjeyam81@gmail.com

Sudhakaran P., Professor
Department of Computer Science and Engineering,
SRMTRPEngineering College,
Trichy

Rajakani V., Assistant professor
Department of Electronics and Communication Engineering,
Anjalai Ammal Mahalingam Engineering College,
Kovilvenni, Tiruvarur

Parameswari A., Assistant professor
Department of ECE,
Adithya Institute of Technology, Coimbatore,
Tamilnadu, India
E-mail: parameswari_a@adithyatech.com