JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVIEW ON INTRUSION DETECTION MEHODS FOR SMART HOME SECURITY IN IOT

[1] Mrs. Divya Jose J, Assistant Professor, Department of Computational Science, Nehru Arts and Science College, Coimbatore. [2] Dr. D. Vimal Kumar , Assistant Professor, Department of Computational Science, Nehru Arts and Science College, Coimbatore.

ABSTRACT

Internet of Things (IoT) plays an important role for managing the observation in and around the smart homes. With the utilization of IoT-enabled development, smart home security is enhanced by automatically examine and managing the security of home devices. Security system provides tracking information and the person accessing devices when they are equipped with smart locks. The sensors are used in IoT devices to attain characteristics of any device or objects. There are various category of sensor such as camera based sensors, temperature control, pressure sensor, image sensor, water quality sensors, chemical sensors, moisture sensor and smell sensors and so on. The considered sensor IoT devices are used reduce common hazardous risk that happens in many home using various IoT applications. Thus, IoT sensor system is more effective to achieve accurate security on smart home than other traditional method. The IoT sensors gives better quality of smart home security by minimizing hazard like electricity management, water management kids monitoring, kitchen gas related risk, keyless entry, locker touch, face recognition system, alarm alert, Information passing to nearest police station etc. Different approaches are designed for improving smart home security performance in IoT devices. However, the designed method failed to improve the performance that used in different sensors. In order to address the above mentioned problems, different methods are discussed for enhanced smart home security.

Keywords: Risk, IoT devices, Sensors, Security, Communication

1. INTRODUCTION

Internet of Things (IoT) illustrates physical objects that are surrounded with sensors and actuators. Here, the sensors are connected with computing devices through either wired or wireless networks. The connected sensors are used to monitor smart home appliance with better security. With the arrangement of artificial intelligence, IoT device provides smart home security. Based on performance of sensors such CCTV camera, elegant illumination, doorbells, and combustion sensors, enhanced security is attained. The monitoring of IoT smart security achieves data loss prevention, secure associations, device authentication and management.

The smart home security systems are made relation with internet for accessing data by users through mobile function, receiving warning messages when alarms go off and manage the system remotely. The security data access using home security system provides home safety and family protection. The smart home connectivity attains more benefits such as real time alters, live monitoring of appliance, video recording and more customizable for better smart home security.

The main purpose of the article is described as follows: Section 2 reviews the existing works of secure and efficient smart home. Section 3 explains the existing smart home security in IoT devices. Section 4 describes the experimental analysis with result and discussion part. Section 5 gives the limitations of existing IoT sensor methods and future directions. Section 6 concludes the paper.

2. LITERATURE REVIEW

The Multi-tiered ANN Model for Intrusion Detection (MAMID) approach was designed in [1] to attain scalable solution. The computation overhead occurred during ANN architecture design is reduced. But the performance of home device analysis was not performed effectively to minimize the overall processing time. An authentication protocol named as Ethereum blockchain Device-to-Device (D2D) interactions was presented in [2]. The D2D interconnection manages attacks by using a lightweight authentication mechanism. Though energy consumption was minimized, the computational cost was not minimized.

An effective Facial Authentication system was analyzed in [3] to find faces via Siamese neural network. The speaker recognition as well as authentication is carried out. Features are extracted with aid of Mel Frequency Cepstral Coefficients. Speakers are discovered by Gaussian mixture model. The designed holistic approach improves privacy and security of smart home appliance. But, the precision was not improved. A two-party collaborative signature scheme based on the SM9 algorithm IS portrayed in [4] to reduce the risk of leakage of the signature private key. The signature private key generation and signature verification is performed. The signature private key is created by key generation center. Whole private key is prevented with collaborative signing process. Hence, the security of signature scheme is proved in the arbitrary oracle model and resulted with higher complexity.

A private blockchain technology and localization method is designed in [5] for detecting smart home devices. The designed approach minimizes the computation time but the storage cost on devices was not minimized. In [6], secure and lightweight three-factor based privacy-preserving authentication scheme was presented to control various home devices with enhanced accuracy. But, a lightweight technique was not applied to guarantee security in IoT environment. A Robust Two-Factor User Authentication scheme was designed in [7] for analysis home devices based on IoT. This supports to increases data security communication in IoT home devices but the overhead was not reduced. The fall detection technique is designed in [8] for determining low-power wireless sensing network. It effectively attains point to point communication with reduced complexity. But it failed to apply machine learning approaches to improve the performance of security while transmitting smart home device data.

3. SMART HOME SECURITY IN IOT NETWORK

Internet of Things (IoT) is allows significant features to perform secure data communication in smart homes that are connected in network. The IoT helps to provide enhanced devices interconnection for efficient transmission. IoT is a type of smart devices that are connected with each other using security threats along with device configuration. The IoT helps to communicate the smart homes with other devices directly within the communication range by providing unique identifiers. The process of managing huge volume of data by IoT devices is a significant challenge in smart home security. Thus, IoT based smart homes are capable of detecting malware, spyware and other malicious software in network. With detection of various attacks, smart home devices are monitored with minimum delay and energy utilization for better lifetime. The utilization of authentication protocol and detection process provides early prediction on network attack by monitoring environment. There is several ensemble classification techniques were presented with various classifier process. By classifying home devices, attacks in home security are effectively predicted.

3.1 Multi-tiered ANN Model for Intrusion Detection model

The IoT includes number of sensors, apparatus, engineering applications, databases, services, etc. The sensors employed in the IoT network generate a massive amount of information where discovering the behavior of smart home devices is for securing applications from attacks. Therefore, an efficient intrusion detection system is necessitated to preserve an IoT. Based on the motivation, Multi-tiered ANN Model for Intrusion Detection (MAMID) model was designed to distinguish security attacks in network with high accuracy. Artificial Neural Networks (ANN) is provided for detecting optimal hyper parameters with enhanced security. The design of ANN supports to select optimal parameters with minimized overhead and improved performance of security attack detection. The selected parameters are appropriate to predict secure smart homes with enhanced accuracy and reduced computational overhead.

The developed MAMID model performs intrusion detection through the different processes namely device preprocessing, relevant feature selection, ANN optimized classification and prediction process. Initially, data preprocessing is performed on each data considered from smart home device dataset. During pre-processing, any redundant data is removed and missing values are eliminated to attain valuable data for classification process. With obtained preprocessed data, feature selection process is achieved using hybrid Feature Selection approach. The measurement of AAN function helps to identify optimal relevant features and irrelevant features from dataset. Followed by, ANN optimizer is performed to carry hyper parameter selection process. Here, optimal neural network topology and hyper parameters are determined to organize training and testing model of smart home devices. Finally, prediction process is applied to classify given input data. The designed classifier effectively classifies smart home data for controlling smart home scenario. Based on the classification results, the real-time detection is accurately predicted with lesser time and complexity.

The designed ANN model comprises with three different layers such as input, hidden and output layer. In each layer, there are several nodes named neurons. At first, a number of smart home devices are considered from network as input and presented at input layer. Every neuron from the input layer is interrelated with one or more neurons in the hidden layer with a weight. Based on input weight and bias, output of input layer is determined. Consider three-layer ANN, the weights and a bias term among the input layer and the hidden layer are W^1 (x_1, x_2, x_3) and b_1. The inner product among the weight matrix and the input data is broadcasted by Sigmoid activation function ‘g(x)’ for predicting data. Followed by, hidden layer is presented by receiving the device data and performing binary classification. For binary classification, there is only one neuron in the output layer. The feed-forwarded process ‘$f(x)$’ is expressed as given in eqn (1),

$$f(x) = W^2 g(W^1 X + b^1) + b^2 \qquad \text{….. Eqn (1)}$$

$$g(x) = 1/(1 + \exp(f(x))) \qquad \text{….. Eqn (2)}$$

From expression (1 and 2), sigmoid logistic activation function ‘$g(x)$’ is determined. In above expression, ‘W^1’ and ‘W^2’ denotes weight value of input and hidden layer. Similarly, ‘b^1’ and ‘b^2’ specifies bias of hidden and output layers. Finally, output of activation function is applied to identify the intrusion with minimal error for each prediction result based on hyper parameter. Hence, MAMID model achieves efficient detection of intrusion with increased accuracy.

3.2 Device-to-Device (D2D) interaction model

Device-to-Device (D2D) interaction model was proposed with the utilization of lightweight authentication mechanism in smart homes. Ethereum blockchain and smart contracts are presented for preventing attacks in network devices. The D2D interaction model authenticates the smart home devices during data communication in IoT system using registration and authentication process. At first, Ethereum blockchain allows decentralized prototype and peer-to-peer distributed ledger system to generate a server. It uses a server queuing system for performing authentication on various attacks. Followed by, authentication mechanism restricts number of service requests for detecting interaction in smart homes.

The D2D protocol is designed for detecting attacks between devices in smart home. The designed D2D protocol comprises with two different processes such as registration and authentication protocol. The performance of proposed model effectively detects attacks in external nodes and internal nodes in smart home. Initially, registration process is carried to register information of smart home devices in server. Enterprise architecture was presented to store information of Ethereum blockchain and address gateway of the smart home in various locations. After registering entire devices, device authentication is performed. The device communications between devices are established through the request and reply arrival from network. The requested message is communicated by smart gateway to registers devices in blockchain technology. The communication between D2D protocols are determined using signed devices as follows in eqn (3).

$$Token_{Device} = (UID, Time_S, D_{response}, D_{request}, smart_{GW}) \qquad \text{Eqn (3)}$$

Token devices are determined using expression (3) to establish signed devices to communicate data. Here, 'UID' denotes unique identification of devices, '$D_{response}$' denotes device request, '$D_{request}$' specifies device response and smart gateway '$smart_{GW}$'. Hashing smart gateway EA is generated with UID and the keccak256 cryptographic hash function is employed in eqn (4) to provide block timestamps.

$$Signed_{Device} = (Token_{Device}, data_P) \quad ..... \quad \text{Eqn (4)}$$

After that, signed devices are determined using expression (4) for providing device to device communication in efficient manner. After obtaining the acceptance token from the smart contract, the requester device will comprise the token in the service request message and transmit it to the responder device to request connection permission, as shown in expression (4). The responder device applies a token for confirming the requester device's validity via smart contract and then responds to the request accordingly. Once permission is established, the connection time is defined as the duration of one complete device-to-device communication. Thus, novel D2D protocol achieves higher security on various attacks in smart home.

3.3 An effective Facial Authentication system

For efficient performance of face recognition, facial authentication and speech recognition approach is developed. The proposed facial authentication system detects face images to enhance smart home security. The face is a significant characteristic for biometric identification and authentication systems since it helps for many real-time applications such as security and person identity authentication. Face recognition system establish the identity of a person by extracting suitable features from the facial images and it evaluates with pre-recorded features using machine learning techniques. Face recognition faces various demands due to the pose, expressions, illumination variation, and particularly age factors. After recognizing face images, speech recognition process is carried to identify speaker with more home security.

The Siamese neural network is utilized to design effective facial authentication system for obtaining smart home security. The performance of authentication system is carried with three different sections namely face recognition and authentication, masked-face recognition and authentication system and speaker recognition and authentication system. At first, face recognition system is carried with authentication of input images. From smart homes, number of face images is captured and detected through Siamese neural network. The considered input images verify that the person is not wearing a mask. Followed by, similarity between detected images and captured images are estimated to differentiate two different classes. Then, distance between classes is calculated to recognize face and performs speaker authentication.

Secondly, masked face recognition system and authentication is performed. The real-time images are captured with person wearing a mask. The recognition process is difficult when the person face is covered with mask. For attaining efficient face recognition, frontal face images are extracted such as nose, right eye, left eye, right eyebrow and left eyebrow, etc. Based on extracted face features, facial information are detected to provide home security. If the detected face images are stored in stored in database, then speech authentication is performed. Otherwise, alter message is provided to owner for securing smart homes. Lastly, speaker recognition and authentication is performed with verified face images. Here, Mel Frequency Cepstral Coefficients are used to store extracted features of captured images. In addition, Gaussian mixture model is provided for determining speakers. If authenticated face speaker is matched with stores speak, the, users are allowed to access home devices, otherwise, alter is forwarded to owner that unknown person is accessing smart home devices. Thus, the solution of smart home security is enhanced with higher accuracy and precision rate.

3.4 Two-party collaborative signature scheme

The Internet of Things (IoT) is a network of physical devices that are used to collect, exchange, and analyze data within the smart homes. A wide range of IoT applications has been implemented and deployed in smart homes, enhancing the capacity to monitor and control devices remotely, as well as automating various household tasks. For obtaining secure and efficient smart homes, a two-party collaborative signature scheme was introduced based on SM9 algorithm. There are two various processes such as signature private key generation and signature verification. Initially, number of data from device is collected for smart home security system. For each data device, key generation center is applied to generate signature private key. Then, the generated private key is related with stored signature private key in two devices. After key verification process, collaborative signing process is presented to prevent the entire private key.

A two-party collaborative signature algorithm attains efficient security for smart home devices. The smart home includes various devices such as user's mobile device, control terminal, business platform and smart home cloud service platform. With consideration of smart devices, SM9 key generation center is provided to generate signature private key for the user in smart device. Then, collaborative signature is carried for verifying generate private key. By sending request massage with random number from one device to another device, signatures are verified and ensure secure enhanced smart home security. The quantitative and qualitative results demonstrate that the two-party collaborative signature scheme efficiently recognizes the face images with minimum time consumption and computational complexity than other related approaches.

4. EXPERIMENTAL SETTINGS

The experimental evaluation of different existing techniques namely Multi-tiered ANN Model for Intrusion Detection (MAMID) model [1], Device-to-Device (D2D) interaction protocol [2], facial authentication system [3] and two-party collaborative signature scheme [4] are carried by implementing using the Python. The experimental evaluations of considered methods are performed with NF-ToN-IoT dataset taken from https://www.kaggle.com/datasets/dhoogla/nftoniot. The considered dataset classifies various network attacks, such as DoS, DDoS, and injection, occurring during data transmission in smart home environments. The dataset includes 14 attributes and total of 1,379,274 data samples. The experimental analysis on [1], [2], [3] and [4] are conducted with several parameters namely accuracy precision and computational cost with respect to number of data samples. The experiments are conducted by comparing dissimilar existing methods. The number of data samples in the range of 10000-100000 samples is considered for conducting experimental purpose. The performance analysis results are discussed with tables and graphical illustrations.

4.1 Performance analysis on accuracy

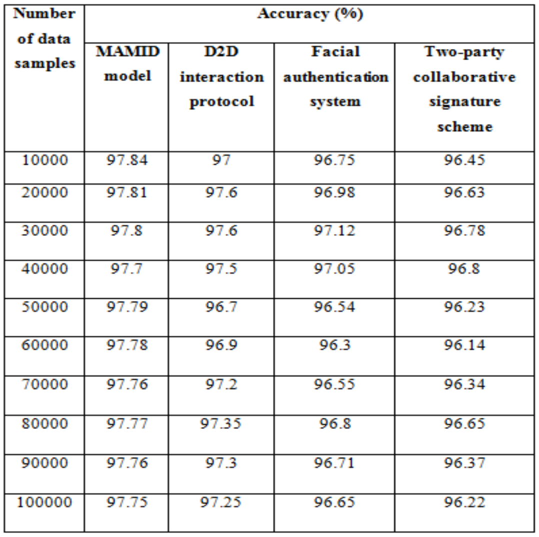
The ratio of number of data sample from smart home that are correctly classified for detection attacks is described as accuracy. It is measured in percentage (%). The accuracy is measured in given below eqn (5),

$$Accuracy = \frac{correclty\ detected\ data\ samples}{Data\ samples} * 100 \quad \ldots.\ \text{Eqn (5)}$$

From expression (5), the accuracy is calculated. While conducting experiments, the values are measured using expression (5) and tabulated in table 1. The experimental outcome of the accuracy of existing methods [1], [2], [3], [4] versus distinct numbers of samples from 10000-100000 for a simulation of 10 runs is provided in Table 1.

The description of accuracy is presented in table 1. The number of data samples ranges from 10000 to 100000 data from dataset using all considered methods. Let us consider 10000 number of data samples for measuring experiments in the first iteration. 9784, 9700, 9675, 9645 data samples are correctly classified and the accuracy is 97.84%, 97%, 96.75%, and 96.45% whereas the accuracy percentage of the [1] [2], [3], and [4] are respectively. Followed by, various performance results are observed for each method. For each method, ten different results are observed. From result of experimental analysis, [1] attains higher accuracy while compared with other approaches. This is because of using ANN optimizer classification process to classify data with higher security. Accuracy using MAMID model is increased by 0.55%, 1.06% and 1.36% compared to [2], [3] and [4].

Table 1 Tabulation for accuracy



Number of data samples	Accuracy (%)			
	MAMID model	D2D interaction protocol	Facial authentication system	Two-party collaborative signature scheme
10000	97.84	97	96.75	96.45
20000	97.81	97.6	96.98	96.63
30000	97.8	97.6	97.12	96.78
40000	97.7	97.5	97.05	96.8
50000	97.79	96.7	96.54	96.23
60000	97.78	96.9	96.3	96.14
70000	97.76	97.2	96.55	96.34
80000	97.77	97.35	96.8	96.65
90000	97.76	97.3	96.71	96.37
100000	97.75	97.25	96.65	96.22

4.2 Simulation analysis of precision

The ratio of true positive rate to the sum of true positive and false positive data estimated from smart home device is defined as precision and it is computed in eqn (6).

$$Precision = \left[\frac{T_p}{T_p + F_p}\right] \qquad \ldots\ldots \text{ Eqn (6)}$$

Where, precision is calculated using above expression (6) by true positive ‘ T_p’ and false positive data ‘ F_p’. For conducting experiments, the values are computed using expression (6) and mentioned in Figure 1. The experimental outcome of precision of existing methods [1], [2], [3], [4] with numbers of samples for a simulation of 10 runs is presented in Figure 1.

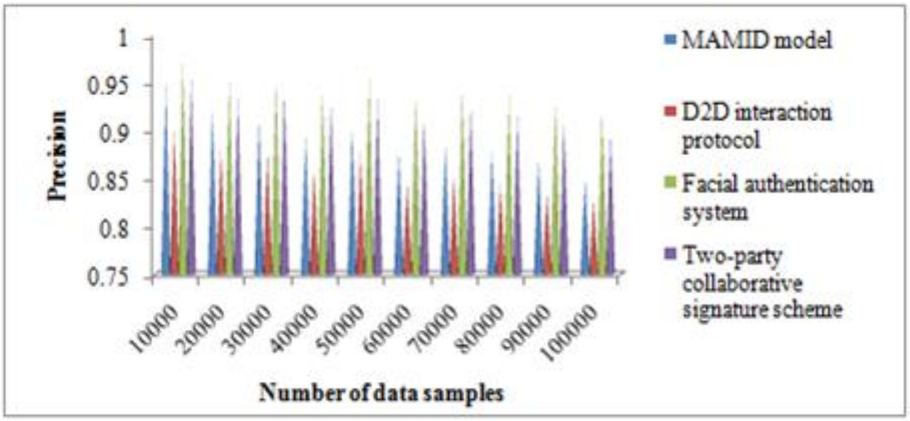


Figure 1 Outline figure of precision

Figure1 depict results of precision. From table value, facial authentication system is higher than existing methods. The proposed authentication system carries face recognition and speech authentication process for detecting images. This supports for facial authentication system [3] to get enhanced precision result. Therefore, precision is improved by 5.6%, 9.7% and 1.9% compared to existing [1], [2] and [4].

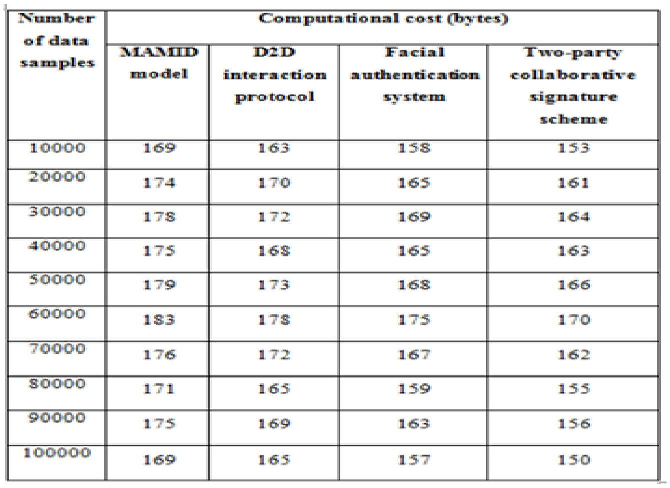
4.3 Impact of computational cost

The measure of memory space consumed to classify data sample is described as computational cost. It is measured in bytes. The computational cost is estimated in eqn (7),

$$CC = DS * Mem\ (DSDS) \qquad \ldots\ldots \text{ Eqn (7)}$$

By using expression (7), computational cost 'CC' is determined based on 'DS' number of data sample and memory consumed '$Mem\ (DSDS)$' for detecting single data samples. Table 2 explains the computational cost for four existing methods. To conduct experiments, the values are computed using expression (7) and tabulated in Table 2. The experimental outcome of computational cost of existing methods [1], [2], [3], [4] with numbers of samples for a simulation of 10 runs is illustrated in Table 2.

Table 2 Tabulated values of computation cost



Number of data samples	Computational cost (bytes)			
	MAMID model	D2D interaction protocol	Facial authentication system	Two-party collaborative signature scheme
10000	169	163	158	153
20000	174	170	165	161
30000	178	172	169	164
40000	175	168	165	163
50000	179	173	168	166
60000	183	178	175	170
70000	176	172	167	162
80000	171	165	159	155
90000	175	169	163	156
100000	169	165	157	150

Table 2 describes computational cost. In the first iteration, the number of data samples is considered as 10000 for experimentation. However, the memory space needed for classifying data samples is found to be 169 ms, 163 ms, 158 ms, and 153 ms using [1], [2], [3], [4]. The remaining nine runs are computed. In figure, two-party collaborative signature scheme [4] provides minimized computational cost than other existing methods. By signature private key generation and signature verification, significant smart home devices are selected with minimum memory space. As a result, computational cost using [4] is reduced by 8.5%, 5.6% and 2.8% than [1], [2] and [3].

5. DISCUSSION ON SMART HOME SECURITY IN IOT ENVIRONMENT

MAMID approach was introduced to detect intrusion in accurate manner based on optimized hyper parameter. Here, preprocessing, feature selection and ANN optimizer is presented for increasing device security. In ANN optimizer, activation function was estimated to classify data into different classes to attain enhanced intrusion detection. But, it fails to avoid over-fitting difficulty during feature selection process. D2D protocol using lightweight authentication mechanism was explained to distinguish DDoS attack in a smart home network. With the aid of Ethereum blockchain technology, system security is enhanced with minimized computational cost. The existing security system improves accuracy but it fails to consider an enhanced deep learning model for accurately detecting and predicting DDoS attacks in systems. A facial authentication system with speaker recognition was developed to perform smart home security. The Siamese neural network uses Gaussian mixture to authenticate facial features by extracting relevant features of image. With extracted features, data from dataset is classified by comparing training and testing data. Though, the models were not trained on a large data set and difficult to recognize masked users. Lastly, two-party collaborative SM9 signature scheme address communication security by detecting malicious attacks in network. The designed signature scheme verifies signature of users for efficient smart home devices with higher security. It fails to perform multi-party collaborative process for signature verification of users. However, the continuous development of new devices and technologies avoid attackers to attain secure smart home devices in IoT devices.

5.1 Future Direction

The future direction of research can be carried out using convolutional neural learning and extreme learning techniques to improve the security level in IoT smart home devices through user authentication. Thus, future enhancement will focus on overcoming data security to avoid unauthorized users by using large datasets for data communication. In the future, more signature verification of users will be developed for performing multi-party collaborative processes to improve accuracy and precision. In addition, the attackers are identified for achieving secure smart home devices in IoT.

6. CONCLUSION

The paper describes the IoT and basic components of smart home security systems. IoT is one of the developing areas in recent times. A comparison of different user authentication techniques and intrusion detection models is studied and elaborated. The primary aim of the smart home is to control and access the home appliances from the cloud in a secure way. Some security issues and their countermeasures of IoT-based smart home explained. An example of smart home security issues is higher computational complexity and overhead by facial authentication of smart devices. In addition, the data security was not taken into consideration through communicating data between devices. The wide range of experiment on existing user authentication techniques enhanced the security performance with its limitations. Finally, the research work can be carried out using neural learning techniques for improving the data security performance with higher accuracy and lesser complexity. Experimental analysis results of the research work revealed that the computational complexity and overhead are significantly less compared to the existing approaches.

REFERENCE

[1] Shaleeza Sohail, Zongwen Fan, Xin Gu and Fariza Sabrina, "Multi-tiered Artificial Neural Networks model for intrusion detection in smart homes", Intelligent Systems with Applications, Elsevier, Volume 16, 2022, Pages 200152.

[2] Bello Musa Yakubu, Majid Iqbal Khan, Abid Khan, Farhana Jabeen and Gwanggil Jeon, "Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home", Digital Communications and Networks, Volume 9, 2023, Pages 383–392.

[3] Navya Saxena and Devina Varshney, "Smart Home Security Solutions using Facial Authentication and Speaker Recognition through Artificial Neural Networks", International Journal of Cognitive Computing in Engineering, Volume 2, 2021, Pages 154–164

[4] Shuang Gen Liu andRu Liu, Si Yuan Rao, "Secure and efficient two-party collaborative SM9 signature scheme suitable for smart home", Journal of King Saud University – Computer and Information Sciences, Volume 34, 2022, Pages 4022–4030

[5] Marc Jayson Baucas, Stephen Andrew Gadsden and Petros Spachos, "IoT-Based Smart Home Device Monitor Using Private Blockchain Technology and Localization", IEEE Networking Letters, Volume. 3, Issue. 2, June 2021, Pages 52-55

[6] Sungjin Yu, Namsu Jho and Youngho Park, "Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes" IEEE Access, Volume: 9, September 2021, Page(s): 126186 – 126197

[7] Shihong Zou, Qiang Cao, Chenyu Wang, Zifu Huang and Guoai Xu, "A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home in IoT", IEEE Systems Journal, Volume: 16, Issue: 3, September 2022, Page(s): 4938 – 4949

[8] Pravin Kulurkar, Chandra kumar Dixit, V.C. Bharathi, A. Monikavishnuvarthini, Amol Dhakne and P. Preethi, "AI based elderly fall prediction system using wearable sensors: A smart home-care technology with IOT" , Measurement: Sensors, Elsevier, Volume 25, February 2023, 100614, Pages: 1- 11