Smart-Sec: DL-based Cyber Threat Detection Approach for Autonomous Smart Home System to Enhance Human Life Expectancy

Naman Jain, Manas Patel
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
{22bce202, 22bce256}@nirmauni.ac.in

Fenil Ramoliya
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
21bce244@nirmauni.ac.in

Rajesh Gupta
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
rajesh.gupta@nirmauni.ac.in

Sudeep Tanwar
Department of Comp. Sci. & Engg.
Institute of Technology,
Nirma University, Ahmedabad, India
sudeep.tanwar@nirmauni.ac.in

Hossein Shahinzadeh
Department of Electrical Engg.
Amirkabir University of Technology
Tehran Polytechnic, Tehran, Iran
h.s.shahinzadeh@ieee.org

Deepak Garg
School of Computer Science and AI
SR University
Warangal, Telangana, India
deepak.garg@sru.edu.in

***Abstract*—The current evolution of technology has changed the way we use, control, and interact with devices in our day-to-day lives. Autonomous Smart Home (ASH) integrates various sensors and Internet-of-Things (IoT) modules to automate and enhance the functionality of a residence. ASH is an interconnected IoT communication paradigm with the characteristics of precise (motion, thermal, environmental) sensing for decision-making, data analysis for energy and resource optimization, automation of tasks during triggered events, and remote accessibility. The connectivity of modules through both wired and wireless channels may give rise to cyber-security-related challenges. This threat includes data privacy concerns, authentication vulnerabilities, potential device tampering, network weaknesses, lack of standardization, and risks associated with firmware and software vulnerabilities in ASH environment. Potential catastrophic effects of cyber breaches in ASH incorporate life-threatening scenarios, like unauthorized control of critical home medical systems, emergency response interference, automated lock system failure, and critical home-appliance sabotage. To mitigate this pressing concern we propose *Smart-Sec*. Our proposed approach leverages DL-based Convolutional Neural Network (CNN) architecture. The performance evaluation of *Smart-Sec* has been done through various optimization algorithms, accuracy comparison, loss depiction, confusion matrix, precision, recall, and f1-score. Out of all used optimization algorithms, our one-dimensional CNN architecture performed exceptionally well with RMSProp optimizer.**

***Index Terms*—Smart Home, Network Security, CNN, IoT, DL**

I. Introduction

Autonomous Smart Home (ASH) are Internet of Things(IoT) based smart residences with minimal human intervention. A variety of IoT devices are connected simultaneously to a base to communicate and share data to operate intelligently without any human operation. These devices are either wired or non-wired. The residential environment of ASH is enabled to boost the efficiency, safety, security, and convenience of residents. ASH-equipped devices impart various facilities such as an auto thermostat for adjustment of temperature in accordance with the resident. Auto lock system allows access to residence with custody of security. Smart air purifiers ensure the elimination of contaminants from the domain, raising air quality index and life expectancy of residents. Sensory devices for the detection of motion, temperature, and humidity simultaneously share data to other devices assisting them to function impeccably. Wired security cameras for surveillance of domain coordinating data for safety of domain. Wireless Smart Speakers such as Amazon Alexa or Google Assistant have voice command control for the assistance of residents to deliver services. Wireless smart plugs to control connection remotely are unavailable at the estate through WIFI or other protocols.

While ASH is efficient and convenient, it poses significant security threats. Wrong data due to miscalculation, hardware failures in memory elements, bugs or glitches in software due to incompatibility of devices or older versions of software could create unintended situations putting human lives on stake. ASH having wide compatibility needs data storage units in the forms of Solid-State Drive (SSD), Hard Disk Drive (HDD), Network Attached Storage (NAS) or External Hard Drive, here data can be manipulated by external forces. Malicious data caused by viruses, unauthorized sources, DNS Spoofing, Trojans, and manipulated file downloads poses an unintended situation that can create catastrophic effects. Considerable threats incurred by IoT utilization would be an alteration of owners identity in wired security cameras through invasion, eliminating access related to facial recognition. Data breach in storage units results in leakage of confidential, private, and unauthorized information having control and accessibility over the complete IoT network of an ASH [1].

Further, we discuss research contributions that have been done since recent years in direction of development and enhancement of security for ASH. In Past few years tremendous growth has been marked down towards security

and efficiency aspects of ASH. There has been various improvement in ASH by introducing concept of blockchain, Artificial intelligence (AI), Deep Learning (DL) and cyptography. In 2021, Qashlan *et al.* [2] with increment in usage of IoT devices which shapes the structure of smart home environment proposed an authentication scheme to combine attribute based access control along with smart contracts and edge computing which reinforces scalability to system by offloading heavy processing activities, also using differential privacy method to send data to clouds with security and privacy. They claim that there framework achieves desired security and privacy goals which is resilient towards DoS attacks, linkage attack, data mining and modification. They also demonstrated efficiency of there proposed model.

Zhang *et al.* [3] remarked rising concerns towards security and privacy for end users along with rapid development of IoT network in smart homes. Author described design of Sovereign IoT system framework that provides one-to-one, one-to-many and device-to-device control of system through wireless communication media which gives end-users complete control of IoT home system. They implemented Sovereign prototype of IoT home controller which delivers user systematic easy-to-use solution. Current stage of IoT technology is progressively prominent in social development as marked by Li *et al.* [4]. There artical put a light on upgrade of IoT security architecture with possibility of deep learning (DL), for capability of IoT devices to respond to cyber attack along with encrypt edge data transmission. The Artical enlightened point which include sharing of computational power by mean of edge network processing unit (NPU). Farooq *et al.* [5] proposed Fused Real-Time Sequential Deep Extreme Learning Machine (RTS-DELM) system model as Blockchain-based solutions are suitable for decentralized protection and privacy. This study works on a private blockchain based ASH network, analyzing possible intrusion detection. Fused RTS-DELM system model can significantly catch any malicious activity achieving highly significant level of stability along with low probability of intrusion activity in ASH environment.

In 2021, AlJanah *et al.* [6] put forward critical analysis about existing authentication solutions, as such current authentication solutions may not be secure for such environments. The paper contributed three aspects. Firstly, they presented a generic model for use case smart home. Second, threat analysis for possible ways of attack and change in security requirements. Third, analysis of existing authentication solutions and further ideas for efficient authentication in IoT environments.

To overcome security vulnerabilities of a smart environment that outside force can operate Illy *et al.* [7] came up with different intrusion detection and prevention systems (IDPSs) for which ML emerged as the most promising approach. The author proposed a Software-Defined Networking (SDN) based architecture of IDPSs for efficient intrusion prevention mechanism. Bagaa *et al.* [8] work presents security framework that is based on ML which can automatically cope up with growing security aspects of IoT domain. There framework presents Software Defined Networking (SDN) and Network Function Virtualization (NFV) for mitigating various threats. Their architecture leverages supervised learning, a distributed data mining system, and neural network for the achievement of result along with with high performance and low cost. The researcher Ahmed *et al.* [9] envisioned regardless of platforms hardware and software modules may be interacting in conjuction and for that Standard Security Framework (SSF) should be made mandatory for all nodes within the distributed network. Furthermore, usage of fog and edge computing combined with cloud applications has been the subject of analysis for the effectiveness and security of new innovations. Wan *et al.* [10] Unveiled IoTArgos which can collects, analyze, and characterize data communications of IoT devices through routers as a multi-layer security monitoring system. IoTArgos develops supervised learning methods and unsupervised learning algorithms to tackle intrusion scenario and unusual behaviors in smart home IoT systems, achieving a precision of 0.9876 and a recall of 0.9763. Edu *et al.* [11] presented a meticulous review of Smart Home Personal Assistant's (SPA) privacy and security issues, grouping the paramount attack possibilities and countermeasures. The Authors concluded affirming there work as first comprehensive review and characterization of Security and privacy vulnerabilities along with countermeasures related to SPA. There has been impressive work done by many researchers in this ASHA privacy preservation domain. Though, cryptography-based solutions faces key management complexity, performance overhead, vulnerabilities in implementation, physical security concerns, key exchange difficulties, backdoor risks, authentication issues, compatibility challenges, regulatory compliance, and resource constraints. While, ML and SDN-based solutions encounter adversarial attacks, bias, complexity, scalability problems, regulatory compliance and performance bottleneck in high number of attack types. *Smart-Sec* introduces DL-based solution to mitigate this pressing concern in ASH highly complex network environment for safeguarding overall system and increase human life expectancy.

A. Research Contribution

The following are the research contributions of the proposed approach:

- *Smart-Sec* is DL based cyber threat detection approach for Autonomous Smart Home systems running with IoT-sensor-enabled wired and wireless networks.
- Our proposed approach utilizes one-dimensional CNN-based architecture for accurately and reliably classifying ongoing network traffic into benign and malicious categories.
- Performance evaluation of *Smart-Sec* includes various optimization algorithms, accuracy plot, loss comparison, precision, recall, f1-score, and confusion matrix.

B. Organization of the Paper

The rest of the paper is organized as follows. Section II presents the system model and problem formulation. Section III elaborates the proposed approach in detail. Section IV highlights the performance evaluation of the proposed

approach. Finally, the paper is concluded with future work in Section V.

II. System Model and Problem Formulation

This section delves into the system model and problem formulation of the proposed approach.

A. System Model

The up-and-coming trend of integrating highly interconnected IoT devices in modern homes creates a fully automated seamless interaction with ordinary technologies within our ecosystem. Devices of varied functionalities, including a diverse array of both wired and wirelessly connected devices, pose a threat to the security and privacy of the end user. Devices communicating through a physical medium, such as smart lights, fire detectors, humidifiers, etc, can be denoted as α_1, α_2,...α_n. On the other hand, security cameras, motion sensors, and smartphones, operating on wireless technology like Bluetooth, Zigbee, WiFi, are distinguished using β_1, β_2,...β_n. The ongoing data is a heterogeneous mix of all such devices, meticulously designed to stimulate a realistic ASH network. The input, X_{input}, encompasses network traffic patterns, device-specific characteristics, device communication, etc, as shown in Eq. 1. Precisely 80 unique and equally salient features, can be symbolically represented as X_1, X_2, ...X_{80}. Therefore:

$$X_{input} = \Sigma(X_1, X_2, X_3, \dots X_{80}) \tag{1}$$

To diagnose and detect various threats, a predictive multi-class classification model can be used, specifically a one-dimensional CNN, denoted as Λ_{CNN}. The architecture of 1D-CNN is well suited to analyze tabular data, learn patterns and converge on to one of the 9 specific cyber threats represented by Π_1, Π_2, Π_3,...Π_9. Applying our function Λ_{CNN} in Eq. 2, to X_{input}, results in the creation of a distinct output Θ_i. here $\Theta_i \in (\Pi_1, \Pi_2, \Pi_3, \dots \Pi_9)$

$$\Theta_i = \Lambda_{CNN}(X_{input}) \tag{2}$$

The loss function utilized by our model Λ_{CNN} is Categorical Cross-entropy. The loss function, in any model, is responsible for shaping a path through an unfamiliar landscape of optimization, as well as of paramount influence on adjusting parameters. Categorical Cross-entropy yields smoother gradients, leading to effective convergence during training, and therefore deeming it fit for classification into various cyber threats. Our loss value, Ω can be written mathematically as Eq. 3, where Y_i represents the true probability of class i, which we have one-hot encoded, and P_i denotes the predicted probability of class i.

$$\Omega = -\Sigma_i Y_i \cdot \log(P_i) \tag{3}$$

Using the loss value Ω as a guiding principle, we can optimize the model to generate precise and true categorization of malicious cyber intrusions. The final stage of our system demands an established module operating to relay the anomaly detected by Λ_{CNN} to ameliorate user life expectancy. This task can be accomplished through, swift communication with local authorities to address the distress in a home, or transmitting data to a central server to terminate the processes of the device in question if possible.

III. The Proposed Scheme

Fig. 1 depicts proposed approach. *Smart-Sec* comprises three main layers: a smart home IoT module communication layer, DL-layer for threat detection and Alert layer.

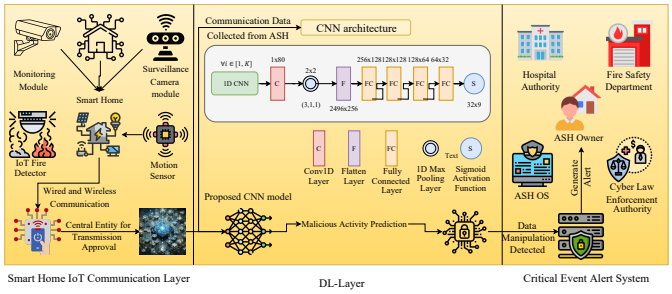


Fig. 1: Proposed *Smart-Sec* Approach.

A. Smart Home IoT Communication Layer

ASH with the facility of wired and wireless automated or semi-automated advance IoT-based sensors establishes a comprehensive and responsive controlling-monitoring system. This advanced set-up ASH is integration of different wireless and wired IoT gear seamlessly collaborating, delivering real-time assistance to end-users ensuring safety, security, and automation, boosting work efficiency. Devices enables data exchange in order to take decisions without any human interruptions. Fire Detector are designed and installed in smart environment as a safety precaution. They conventionally utilize sensors like ionization or photoelectric sensors to determine a peculiar change in zone. Device have different communication protocols as WIFI being one to connect and share facilitating remote surveillance and alerts. Fire detector uses low-powered wireless protocol Z-Wave which have central hub to connect other devices directly in smart environment. It performs anomaly detection with Bayesian networks as seen in Eq. 4.

$$P(A|\mathbf{S}) = \frac{1}{\mathcal{Z}} P(\mathcal{A}) \prod_{i=1}^{n} P(\mathbf{S}_i|\Pr(\mathbf{S}_i)) \tag{4}$$

here, $\mathbf{S}$ is vector of sensor readings and $\mathcal{A}$ is the event of an anomaly. n is total available sensor in ASH and $\Pr(\mathbf{S}_i)$ represents the parent of sensor S_i the Bayesian network. $\mathcal{Z}$ is normalization content to get output in probabilistic range.

Surveillance cameras or camera sensors part of smart home security captures visual data for monitoring and surveillance, usually are integrated with facial recognition for users to safeguard there possession. Camera sensor uses Ethernet as wired communicating protocol ensuring stability and high-bandwidth. This also use Real-Time Streaming Protocol (RTSP) allowing visual information and audio to stream over internet and various platforms. Normally surveillance camera module uses advanced pre-trained inbuilt neural network based architecture to perform facial recognition and authentication using matching score F_{match}. Abstract representation of this task has been shown in Eq. 5.

$$F_{\text{match}} = \mu\left(\mathcal{W} \cdot \mu(\mathcal{V} \cdot \mathbf{F_s} + \mathbf{b}_1) + \mathbf{b}_2\right) \tag{5}$$

here, F_s is the vector of facial feature and μ is the sigmoid activation function. $\mathcal{W}, \mathcal{V}, \mathbf{b}_1$ and $\mathbf{b}_2$ are weight matrices and bias vectors learned during training for that sensor module.

Motion Sensor perceive fluctuations in infrared radiation patterns in line of vision for detection of motion, generating alert signals via wireless zigbee protocol to ensure connection with central hub incorporating additional devices when triggered in unusual situations. Eq. 6 represents the motion sensor activation with Gaussian mixture models (GMM). The data collected from this modules with high number of network parameters will further be used for malicious activity prediction task by proposed Λ_{CNN} model.

$$P(\text{Activate}|\mathbf{M}) = \sum_{k=1}^{K} \pi_k \mathcal{N}(\mathbf{M}|\boldsymbol{\tau}_k, \boldsymbol{\Sigma}_k) \tag{6}$$

where, $P(\text{Activate}|\mathbf{M})$ is the probability of activation given motion. M is the vector of motion sensor readings derived from IoT environment. K is the number of Gaussian components in the mixture. π_k is the weight of the k^{th} component. τ_k and Σ_k are the mean and covariance matrix reading of k^{th} component.

B. DL-Layer

Based on the information relayed by various IoT devices, cyber threats can be detected by incorporating an intelligence layer consisting of a pre-trained DL model. This layer is in control of accepting raw instances, processing the required instances to better suit the model and accurately predicting the degree of risk contained within them.

The training process for the 1D-CNN model, represented as Λ_{CNN}, uses a subset of the ACI IoT Network Traffic Dataset 2023 [12] with 61312 training instances and 85 attributes for each instance. The dataset is entirely created using real-time smart home network in their respective facility. Here, target column has 9 different categories of labels, i.e, Benign, ICMP Flood, ARP Spoofing, OS Scan, DNS Flood, Slowloris, SYN Flood, Port Scan, Vulnerability Scan as part of malicious data prediction. Further preprocessing is applied to dataset to assist training and prediction. Insignificant columns describing IP addresses and time of the instance have been dropped from the dataset. Instances with infinite values in the Flow Bytes/s and Flow Packets/s column indicates the highest possible flow rate, therefore replaced by the general maxima of 10000. The target label column, Ψ, is converted from a string to a numeric value, by applying label encoding to it, which assigns a value from 0 to 8 for each class. Following this, one hot encoded vector is created, for each instance, corresponding to its value in Ψ. Our final target column can be represented as:

$$\Psi = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \& \ldots \& \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \& \ldots \& \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \tag{7}$$

Furthermore in Eq. 8, we use standard-scaler transformation, also known as z-score normalisation, for all features $X_i \in (X_1, X_2, X_3, \ldots, X_{80})$, to achieve a comparable and common scale in our feature set.

$$X_{standardized} = \Sigma_{i=1}^{80} \left(\frac{X_i - \mu_i}{\sigma_i}\right) \tag{8}$$

where μ_i and σ_i are mean and standard deviation respectively.

To eradicate the predicament of over-fitting or under-fitting, the architecture has been developed with rigorous testing, thus curating the best possible 1D-CNN model, Λ_{CNN}. It comprises of exactly one convolutional layer and six fully connected neural network layers. The CNN layer has 64 filters, kernel size of 3 , valid padding, stride equal to one and ReLU activation function as depicted in Eq. 9.

$$\text{ReLU}(x) = \begin{cases} x, & \text{if } x > 0 \\ 0, & \text{if } x \leq 0 \end{cases} \tag{9}$$

To further extract the paramount features and down-sample the input sequence, max pooling layer is used with pool size as 2. The data obtained is of the shape 39 x 64, which is flattened to array of size 2496. This flattened data is passed through 5 fully connected layers with ReLu function and no. of neurons as 256, 128, 128, 64, 32 respectively. These layers use L2 regularization, adding a penalty term to the loss function as shown in Eq. 10, thus affecting the weights in each layer to counteract over-fitting. Regularization strength, ν, of 0.001 is utilised.

$$\text{loss}_{regularized} = \text{loss}_{original} + \frac{\nu}{2}\Sigma_i W_i^2 \tag{10}$$

where, $\text{loss}_{original}$ is loss function before regularization and ν is regularization strength. $\Sigma_i W_i^2$ is summation of squares of all weights in the layer.

The sixth layer has highest significance, with nine neurons for classification into nine categories. The sigmoid activation function is used to predict the label, shown in Eq. 11, where $\sigma(x)$ is output of sigmoid function with input x and e is base of natural logarithm (approximately 2.7183).

$$\sigma(x) = \frac{1}{1 + e^{-x}} \tag{11}$$

The model, Λ_{CNN}, is compiled using four optimizers– RMSprop, SGD, Adam and Adagrad, however, with conclusive and satisfactory results, both RMSprop and Adam show superior performance. RMSprop flaunts adaptive learning rate, by dividing the learning rate with the square root of the mean of the squared gradients for that weight. This is achieved by maintaining squared gradients through a running average, τ, for each weight.

$$\tau = \gamma \cdot \tau + (1 - \gamma) \cdot \left(\frac{\partial Loss}{\partial W}\right)^2 \tag{12}$$

here, γ is contribution of previous squared gradients, also known as decay factor. $\frac{\partial Loss}{\partial W}$ is the gradient.

The weights are updated by Eq. 13, resulting in an efficient and effective convergence to optimum output.

$$W_{new} = W_{old} - \frac{\rho}{\sqrt{\tau + \epsilon}} \cdot \frac{\partial Loss}{\partial W} \tag{13}$$

where, ρ is the learning rate. ϵ is a constant to avoid division by zero. W is the weight. The prominence of the layer increases further as we understand the risks associated with these cyber threats, substantially decreasing human life. Address Resolution Protocol (ARP) spoofing is a type of Man in the Middle (MitM) attack where the communication between two devices is disrupted by a malicious attacker.

Upon network access by an intruder, forgery of Media Access Control Address (MAC) of destination device occurs, such that the attacker's machine is connected rather than the initial two devices. In the case of a security camera, or any other privacy-sensitive device, through ARP spoofing an unauthorised third party device can invade the privacy of a user and endanger their livelihood. A Domain Name System (DNS) flood causes large traffic in a network, often disguised as normal heavy traffic due to near perfect queries for real records and generation from innumerable unique locations. Such Distributed Denial-of-service (DDoS) attacks may cause detectors to degrade their ability to detect other legitimate attacks, predict a higher number of false negatives and in turn compromise security of the resident. A SYN flood is another DDoS attack responsible for exhausting all obtainable server resources, thus diminishing the ability to respond to authorized traffic. All ports on a targeted device are swamped due to repetitively receiving initial connection request (SYN) packets. IoT devices like thermostats, lighting systems and hubs, become unable to communicate with web or cloud servers, degrading quality of life and thus eventually decreasing life expectancy in the long run.

C. Critical Event Alert System

These attacks are terrifically threatening once they enter the ASH network and compromise our health, security, and privacy. After detection of such malignant cyber threats, appropriate precautionary measures are needed to amortize the magnitude of loss and resume operation swiftly. On the arrival of a critical event, detected by the previous layer, suitable action must commence and for severe threats, relevant local authorities must be notified. Devices safeguarding the privacy of a resident, like security cameras, must use Two-Factor Authentication (2FA), secure local network settings and a Virtual Private Network (VPN) making it virtually invisible. Thermostats, fire detectors, motion sensors, air purifiers monitor physical elements, like temperature, human presence, air quality and etc. Breach in their conventional functionality generating a critical event, alerts the home owner and other individuals in a certain radius, through visual and auditory indicators. Distress signals are sent to fire stations, emergency department in hospitals and other rapid response teams for expert assistance. For attacks on devices used for communication, like phones and laptops, a critical event is reported to cyber authorities aswell as notified to the user immediately with an appropriate descriptive warning message. For any kind of DDoS or MitM type of attack, the critical alert event system shall, isolate the affected device from the network for security of remaining devices, scrutiny of network traffic to find any anomalies and discrepancies. Specifically for DNS flooding, SYN flooding and other DDos attacks, rate limitation and load balancing algorithms are initialised to reduce the intensity of the attack. This last layer gives a unique and effective solution in the larger proposed approach of tackling threats posed by such countless malicious attacks.

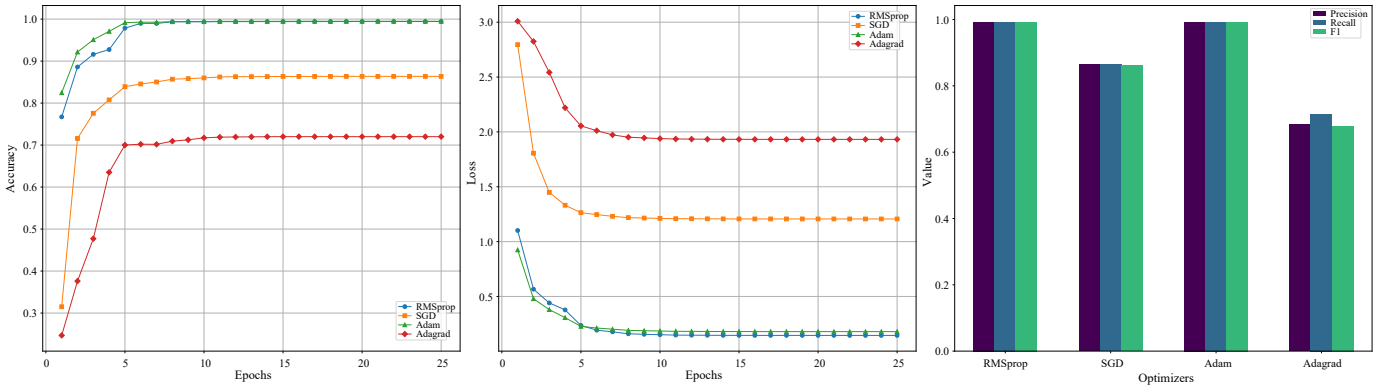
IV. Performance Evaluation

This section emphasises on the analysis of the CNN model to detect cyber threats in ASH networks,with respect to different optimizers.

To achieve consistency and precision during training, the experimental setup included a single computer system with a clock speed of 1.10 GHz and 7.77 GB usable RAM. The hyper-parameter epochs is set to 25, batch-size is set to 128 and an adaptive learning rate to adjust with fall or rise in accuracy of the model. The 'Categorical Crossentropy' loss function has been utilised for training the proposed model. To fine-tune our model, four distinct optimizers–RMSprop, SGD, Adam and Adagrad have been carefully selected due to their numerous advantages in various DL applications. RMSprop changes the learning rate based on the average of squared gradients for each parameter individually. SGD updates the parameters in the opposite direction of the gradient with respect to the loss function. Adam is a step up of the RMSprop optimizer as it tracks running average of both gradients and square gradients. Finally, Adagrad accumulates squared gradients of each parameter and applies square root to this to alter the learning rate. It is worth noting that the below findings were obtained by keeping no of epochs, the batch size and overall model architecture constant

Fig. 2a presents the change in accuracy of the model with respect to no. of epochs for all four optimizers. Accuracy is measured by the percentage of rightly predicted labels as compared to the total labels for the target column. RMSprop and Adam show significantly higher accuracy's outperforming SGD and Adagrad optimizers. Adagrad shows the least accuracy of 0.6802, highlighting its weakness to provide a high accuracy, while SGD has a better accuracy of 0.8807, this result is still sub-par in converging to an optimal classification as compared to the other optimizers. Both Adam and RMSprop reach a remarkable accuracy of 0.9941 and 0.9944 respectively, while RMSprop edges out Adam by the smallest of margins, both optimizers prove their relevance in the problem at hand by traversing optimization productively. Fig. 2b displays the value of the loss function, namely 'Categorical Crossentropy', as no. of epochs increase for all 4 optimizers. Categorical Cross-entropy loss function measures the difference between true and predicted label probability, with the objective of minimizing the difference between the predicted and true probability distributions. SGD and Adagrad optimizers maintain an undesirably high loss value of 1.1723 and 1.9359 respectively, depicting unfavourable convergence patterns. In contrast both Adam and RMSprop, consistently exhibit favourable loss values of 0.1925 and 0.1419, notably RMSprop, the leading optimizer in minimizing the loss metric.

Based on Fig. 2c, we indulge in extensive analysis of Precision, Recall and f1 scores by the way of a bar chart, presenting a comprehensive interpretation of optimizer behavior on test data. Both RMSprop and Adam achieve near perfect f1 score standing at, 0.9926 and 0.9913, precision of 0.9926 and 0.9914, and recall at 0.9926 and 0.9913 respectively. Such impeccable result indicates that we achieved accurate positive predictions and a satisfactory trade-off between precision and recall. Contrary to the above, SGD obtained a f1 score of 0.8755 and Adagrad with a mere 0.6562 f1 score, proving once again, their incapability in this context. Fig. 3 illustrates the confusion matrix for the test data using RMSprop optimizer. It imparts a more nuanced



(a) Accuracy Curve (b) Loss Curve (c) Precision, Recall, F1 Score

Fig. 2: Performance on training: (a) Accuracy curve for different models during training, (b) Loss curve for different models during training, (c) Bar plot for comparing Precision, Recall, F1 Score for different optimizers on Test Data

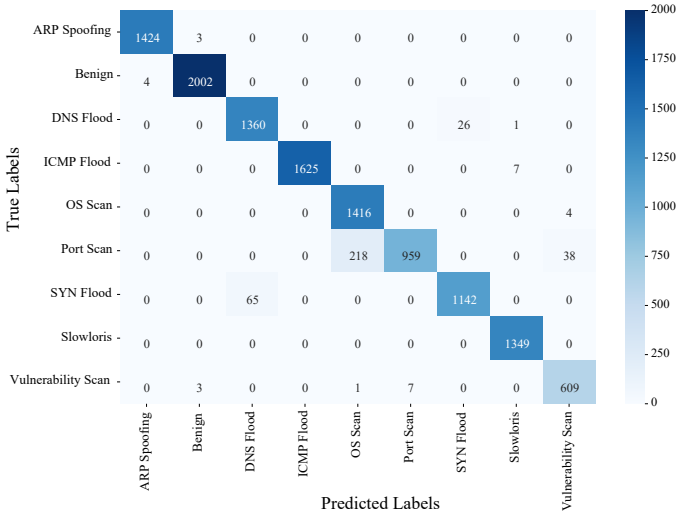


Fig. 3: Confusion Matrix for RMSprop optimizer on test data

overview of the classification by imparting how well instances are classified into-true positive, true negative, false positive, false negative. The diagonal represents no. of true positives for every class, and non-diagonal cells depict misclassifications. RMSprop got the better of remaining optimizers during exploration and subsequent classification.

V. Conclusion and Future Scope

Our proposed approach, i.e., *Smart-Sec* mitigates the concerns related with cyber security and malicious user innervation in ASH environment. Large number of inter-intra communication IoT modules are involved in automation, control and data exchange process for ASH. We have identified eight distinct types of possible malicious attack in smart home environment, capable of causing catastrophic effects. Our utilized CNN architecture with RMSProp optimizer has shown highest performance among all the other model-optimizer combination. Looking ahead, future scope involves optimization of CNN model architecture and curation of dynamic threat modeling. Model compression for DL architecture to minimize resource consumption using knowledge distillation in ASH. Utilization of federated learning to build more centralize and generalize cyber threat defence system in ASH integrated sophisticated urban ecosystems.

References

[1] N. K. Jadav, R. Gupta, M. D. Alshehri, H. Mankodiya, S. Tanwar, and N. Kumar, "Deep learning and onion routing-based collaborative intelligence framework for smart homes underlying 6g networks," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 3401–3412, 2022.

[2] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-preserving mechanism in smart home using blockchain," *IEEE Access*, vol. 9, pp. 103651–103669, 2021.

[3] Z. Zhang, T. Yu, X. Ma, Y. Guan, P. Moll, and L. Zhang, "Sovereign: Self-contained smart home with data-centric network and security," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13808–13822, 2022.

[4] Y. Li, Y. Zuo, H. Song, and Z. Lv, "Deep learning in security of internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22133–22146, 2022.

[5] M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan, and S. O. Hwang, "Blockchain-based smart home networks security empowered with fused machine learning," *Sensors*, vol. 22, no. 12, 2022.

[6] S. AlJanah, N. Zhang, and S. W. Tay, "A survey on smart home authentication: Toward secure, multi-level and interaction-based identification," *IEEE Access*, vol. 9, pp. 130914–130927, 2021.

[7] P. Illy, G. Kaddoum, K. Kaur, and S. Garg, "Ml-based idps enhancement with complementary features for home iot networks," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 772–783, 2022.

[8] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for iot systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020.

[9] B. Ahmed, M. Shuja, H. M. Mishra, A. Qtaishat, and M. Kumar, "Iot based smart systems using artificial intelligence and machine learning: Accessible and intelligent solutions," in *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, pp. 1–6, 2023.

[10] Y. Wan, K. Xu, G. Xue, and F. Wang, "Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, pp. 874–883, 2020.

[11] J. S. Edu, J. M. Such, and G. Suarez-Tangil, "Smart home personal assistants: A security and privacy review," *ACM Comput. Surv.*, vol. 53, dec 2020.

[12] N. Bastian, D. Bierbrauer, M. McKenzie, and E. Nack, "Aci iot network traffic dataset 2023," 2023.