



Article

Predicting DDoS Attacks Using Machine Learning Algorithms in Building Management Systems

İsa Avcı ^{1,*}  and Murat Koca ² 

¹ Department of Computer Engineering, Faculty of Engineering, Karabuk University, Kilavuzlar Mahallesi 413, Sokak No. 7, Merkez, Karabuk 78000, Turkey

² Department of Computer Engineering, Faculty of Engineering, Van Yuzuncu Yıl University, Kampüs, Tuşba, Van 65080, Turkey; muratkoca@yyu.edu.tr

* Correspondence: isaavci@karabuk.edu.tr; Tel.: +90-444-0-478

Abstract: The rapid growth of the Internet of Things (IoT) in smart buildings necessitates the continuous evaluation of potential threats and their implications. Conventional methods are increasingly inadequate in measuring risk and mitigating associated hazards, necessitating the development of innovative approaches. Cybersecurity systems for IoT are critical not only in Building Management System (BMS) applications but also in various aspects of daily life. Distributed Denial of Service (DDoS) attacks targeting core BMS software, particularly those launched by botnets, pose significant risks to assets and safety. In this paper, we propose a novel algorithm that combines the power of the Slime Mould Optimization Algorithm (SMOA) for feature selection with an Artificial Neural Network (ANN) predictor and the Support Vector Machine (SVM) algorithm. Our enhanced algorithm achieves an outstanding accuracy of 97.44% in estimating DDoS attack risk factors in the context of BMS. Additionally, it showcases a remarkable 99.19% accuracy in predicting DDoS attacks, effectively preventing system disruptions, and managing cyber threats. To further validate our work, we perform a comparative analysis using the K-Nearest Neighbor Classifier (KNN), which yields an accuracy rate of 96.46%. Our model is trained on the Canadian Institute for Cybersecurity (CIC) IoT Dataset 2022, enabling behavioral analysis and vulnerability testing on diverse IoT devices utilizing various protocols, such as IEEE 802.11, Zigbee-based, and Z-Wave.



Citation: Avcı, İ.; Koca, M. Predicting DDoS Attacks Using Machine Learning Algorithms in Building Management Systems. *Electronics* **2023**, *12*, 4142. <https://doi.org/10.3390/electronics12194142>

Academic Editors: Xiangjie Kong and Giovanni Pau

Received: 7 September 2023

Revised: 24 September 2023

Accepted: 29 September 2023

Published: 5 October 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: cybersecurity; distributed denial of service attacks; internet of things (IoT); intrusion detection systems; slime mould optimization algorithm

1. Introduction

Building Management Systems (BMSs), also known as Building Automation Systems (BASs), Building Management and Control Systems (BMCSs), Direct Digital Controls (DDCs), or building controllers, are intelligent microprocessor-based control networks designed to monitor and manage all electronic and mechanical devices within a building. As the BMS extends its integration across multiple buildings, ensuring comprehensive control and operation as a unified system becomes crucial. With the increasing proliferation of IoT devices within these systems and the diverse communication protocols in use, ensuring their security has emerged as a significant challenge [1,2].

A BMS refers to a control system used for monitoring and managing the mechanical, electrical, and electromechanical services inside a given facility. These services include a range of essential functions, such as power supply, heating, ventilation, air conditioning, physical access control, pumping stations, lifts, and lighting systems. A rudimentary BMS comprises software, a server housing a database, and intelligent sensors that are interconnected inside an Internet-enabled network. Intelligent sensors deployed throughout the premises collect data and transmit them to the BMS where they are then stored inside a designated database. If a sensor detects data that deviate from predetermined circumstances,

the BMS will initiate an alert. In the context of a data center, it is plausible for the BMS to initiate an alert system if the temperature inside a server rack exceeds the predetermined tolerable thresholds.

Recent advancements in BMSs, while beneficial, have concurrently amplified cybersecurity challenges. Particularly concerning are Distributed Denial of Service (DDoS) attacks. These attacks have morphed over time, with some now originating from within the network, adeptly bypassing firewall controls and causing significant damage to interconnected devices. While the problem is well defined, traditional methods focused primarily on mere data monitoring, proving increasingly inadequate against the sophistication of modern DDoS attacks. Recognizing this evolving threat landscape, our study introduces a novel, multi-stage, modular DDoS attack detection system. This system, which stands apart from prevailing solutions, delivers an impressive accuracy of 97.44% in estimating DDoS attack risk factors and a notable 99.19% accuracy in predicting attacks [3].

The promise of machine learning in defense models offers a fresh perspective to this challenge. These models, with their ability to detect and predict an array of network intrusions, have spotlighted potential solutions to vulnerabilities rampant in IoT [4]. Building on this foundation, our proposal amalgamates the Software Defined-Wide Area Network (SD-WAN) packet duplication detection algorithm with a Firewall as a Service (FWaaS). The latter integrates a Support Vector Machine (SVM) modeling resolver to meticulously analyze packets and connections. We conducted an extensive evaluation of these developed models using the reputable Canadian Institute for Cybersecurity (CIC) IoT Dataset 2022.

In terms of cybersecurity, protection measures have become difficult as the attack vectors of cyber threats increase. This issue has become especially important for the security of IoT devices used in smart BMSs. In this respect, taking precautions against DDoS attacks is important for service continuity. In this work, our main contribution is to propose a new algorithm that combines the power of the Slime Mold Optimization Algorithm (SMOA) with an Artificial Neural Network (ANN) estimator and an SVM algorithm for feature selection.

This paper unfolds as follows: Section 2 delves into the background and the compelling motivations behind our proposed system. It emphasizes the pressing need for fortified security measures in BMSs, especially in the face of DDoS threats. Section 3 offers a detailed exposition of our innovative, multi-stage, modular DDoS attack detection system. Here, the intricacies of the SD-WAN packet duplication detection algorithm and the SVM-integrated FWaaS are unraveled. Furthermore, this section delineates the incorporation of Artificial Neural Networks (ANNs) in predicting DDoS attack risk factors.

Section 4 meticulously details our experimental setup, the dataset deployed, the evaluation metrics applied, and how our proposition stacks up against existing methodologies. This section also sheds light on the robust performance metrics of our system; chiefly, its accuracy and efficiency in warding off DDoS attacks. Also, Section 4 compares our system against contemporary defense models, underscoring the superiority of our approach in accuracy, robustness, and adaptability to a spectrum of DDoS attacks. This comparative analysis also touches upon the potential of hybrid models, which marry machine learning techniques with time-tested defense mechanisms, enhancing the detection and mitigation prowess of cybersecurity frameworks.

Finally, rounds off the paper, encapsulating the seminal contributions of our research. It also sketches a roadmap for prospective studies, underscoring the pressing need for innovative machine-learning-based defense models. In the ever-evolving cybersecurity domain, particularly within BMSs and similar IT systems, the looming threat of DDoS attacks warrants relentless research. Future endeavors could delve deeper, exploring the amalgamation of advanced machine learning stratagems like deep learning and reinforcement learning. Such exploration holds the key to crafting security systems that can not only match but outpace the rapidly evolving cyber threat landscape.

2. Related Work

Understanding past research and innovations concerning DDoS attacks' analysis and prevention for BMSs offers essential insight into the ongoing challenges and solutions. DDoS attacks in IoT networks typically overload servers using deceptive requests from a myriad of IoT devices, effectively incapacitating them [5,6]. A significant case in point was the 2016 incident where hackers instigated a DDoS attack that disrupted the heating systems of two Finnish apartments [7]. Another seminal episode revolved around the infection of IoT devices via DDoS methodologies, leading to the temporary incapacitation of Dyn, a significant US domain name service provider, thereby affecting various websites across North America [8].

The penetration and popularity of IoT devices have soared over recent years. By 2017, sales figures reached a staggering 22 million units for Amazon Echo and USD 310.4 million for wearables [9]. The count of IoT devices escalated to 30.73 billion, and projections indicate this number might burgeon to 41 billion by 2027 [10]. This rapid proliferation has an attached economic magnitude, with these devices' total cost likely to hit USD 2.4 trillion. Compounding the complexity of this vast landscape is a concerning statistic from 2017, where DDoS attacks accounted for 89% of all potential attack types, underscoring their menace and stealth [11].

Several solutions have been postulated in the recent literature. Singh et al. proposed the Edge-Based Hybrid Intrusion Detection Framework (EHIDF), integrating a machine learning (ML) technique with Mobile Edge Computing (MEC) [12]. Their model achieved an accuracy of 90.25% while maintaining a low False Alarm Rate (FAR) of 1.1%. Wu et al. introduced the Edge Node Firewall (ENFW), crafted specifically for edge computing adaptability [13]. Another significant contribution came from Zhang et al., who designed a DDoS detection and prevention model anchored on Bidirectional Long Short-Term Memory (BiLSTM), boasting 95.96% accuracy [14].

Myneni et al. shed light on the merit of capturing over 90% of DDoS traffic right at the inception point, which substantially amplifies the detection and mitigation efficacy of smart defense [15]. They charted out strategies centered on efficient network traffic management and DDoS flow programming, respectively [16,17].

The study was conducted by Zhang et al. through the implementation of a three-layer back propagation network; the researchers demonstrated that a Neural Network with a dynamic structure may provide identical control parameters within the specified flying circumstances, resulting in consistent responses, as seen before [18]. The use of game theory approaches in conventional artificial intelligence decision-making systems has yielded beneficial outcomes, as shown by the work of Yang et al. These methods are rooted in classical mathematical modeling methodologies [19].

Forestiero et al. conducted an approach based on the multi-agent paradigm and inspired by biological systems, such as ant and termite colonies, for building an efficient information system in Grids. The approach was exploitable in very large networks because it is fully decentralized and self-organizing. Two complex objectives are specifically addressed: reorganization and the discovery of resources [20].

Abualigah et al. studied optimization algorithms, such as particle swarm optimization, harmony search, firefly algorithm, and cuckoo search. They also present a variety of solution techniques for optimization problems, emphasizing concepts rather than rigorous mathematical details and proofs [21].

A pivotal challenge in the IoT realm is the heterogeneity of end-point devices, complicating packet inspection for suspicious DDoS activities. To this end, our method incorporates an edge computing system design, functioning as a firewall, to streamline and optimize detection in intricate device communications. This multi-modular approach affords the flexibility to integrate updates and new functionalities, a feat unattainable in conventional, static firewall systems.

In summary, the reviewed literature accentuates the urgency and significance of sculpting efficient techniques to thwart DDoS attacks in IoT frameworks, especially within BMS.

Advancements leveraging edge computing, machine learning, and multi-modularity herald promising strides toward enhancing the precision and effectiveness of DDoS attack mitigation. As the IoT domain burgeons, so does its associated security vulnerability landscape. Building on the bedrock of extant research, future endeavors should focus on devising increasingly robust and adaptable protective measures for IoT and BMS infrastructures. It is worth noting that research articles containing expansive datasets deposited in publicly accessible repositories should delineate the deposit location and supply the pertinent accession numbers. These numbers should be furnished before publication if they are not available during the manuscript's submission.

3. Materials and Methods

The proposed system aims to tackle the ever-increasing challenge of cyber threats targeting large-scale networks. With a surge in DDoS attacks affecting numerous institutions and industries, our research offers a solution that bridges the gaps identified in existing studies. Primarily, our work consists of two components concerning functionality and technological integration: SD-WAN Packet duplication detection and Firewall as a Service (FWaaS) with SVM modeling resolver.

3.1. Experiment Setup

The experimental setup and simulation were conducted using Visual Studio Code, utilizing an environment featuring Python 3.10.4 64-bit. The system configuration is as follows:

- Operating System: Microsoft Windows 11 Home, version 10.0.22621 Build 22621, System Type x64-based PC.
- Hardware Specifications: 11th Gen Intel(R) Core (TM) i7-11600H @ 2.90GHz processor, 2918 MHz, 6 Core(s), 12 Logical Processor(s), and an installed total physical memory of 15.7 GB.
- Libraries: Scikit-learn, Matplotlib, NumPy, and Pandas were pivotal in performing various operations and analyses.

3.2. Pseudo-Code of the Proposed Algorithm

The first and foremost step involves the collection and preprocessing of the dataset, as exemplified in Algorithm 1. The data flow connectivity is validated, ensuring each packet in the stream is cross-referenced with the attack dictionary. Packets identified as threats are filtered and blacklisted. The artificial intelligence prediction technique is recurrently applied to subsequent flows, updating the blacklist.

Our proposed algorithm addresses DDoS attacks in BMS using two primary components: Detection_step and Prediction_step. These components, functioning in harmony, offer a comprehensive solution against DDoS attacks by monitoring, analyzing, and predicting potential threats.

3.3. Two Mainstream Proposed Algorithm

The SD-WAN mesh mechanism efficiently determines the communication paths for traffic, targeting internet portals, cloud-based applications, and data centers. With the foundation of overlay architecture, the SD-WAN mesh reduces operational intricacy and optimizes the user experience [22,23]. The system also facilitates the speedy deployment of applications and services, in addition to standardizing and enforcing regulations across various locations. Figure 1 provides a visual representation of the system's prevention mechanism against unprotected internet traffic.

Algorithm 1 Pseudo-code of the proposed algorithm

Inputs: Request flags, Packets count, Packets data, Ti (Period time for the check-up loop), Tj (Maximum allowed period for traffic allocation)

Synchronize threads DS \leftarrow Detection_step() and PS \leftarrow Prediction_step()

Wait Until (DS.is_running == PS.is_running == false)

FilteredAccess \leftarrow (DS.result NOR PS.result) * Packets_matrix(Packet data, Packet count)

Return FilteredAccess

Function Detection_step()

Each Ti seconds

 connections_available \leftarrow Access_control_retriever(Request flags, Packets count, Packets data)

For each connection of connections_available **do**

 selected_features \leftarrow Slime_Mould_Optimization_Algorithm(connection.packetData)

 get_first(connection_dictionary(p=connection.packetData)):Merge(selected_features, connection.packetData), append(connection_dictionary(p=connection.packetData, i=connection.packetCount))

If (get_first(connection_dictionary(p=connection.packetData))>unnorm_traffic) during Tj seconds **then**

 subnet_x \leftarrow Find_SubNet_In_blacklist_dataset(connection)

 insert_SubNet_in_blacklist_dataset(subnet_x, connection)

Move connection to blacklist_dataset

Else

 reset_data(get_first(connection_dictionary(p=connection.packetData)))

End If

End For

End Function

Function Prediction_step()

Each Ti seconds

 connections_available \leftarrow Duplication_detection_retriever(Request flags, Packets count, Packets data)

For each connection of connections_available **do**

 selected_features \leftarrow Slime_Mould_Optimization_Algorithm(connection.packetData)

 get_first(connection_dictionary(p=connection.packetData)):connection_dictionary(p=connection.packetData).packetCount+connection.packetCount,append(connection_dictionary(p=connection.packetData, i=connection.packetCount))

If (get_first(connection_dictionary(p=connection.packetData))>unnorm_traffic) during Tj seconds **then**

 subnet_x \leftarrow Find_SubNet_In_blacklist_dataset(connection)

 insert_SubNet_in_blacklist_dataset(subnet_x, connection)

Move connection to blacklist_dataset

Else

 reset_count(get_first(connection_dictionary(p=connection.packetData)))

End If

End For

End Function

The implemented access control is instrumental in preventing data breaches, malware penetrations, and other cyber threats. Notably, our system incorporates FWaaS with SVM modeling resolver, transforming a conventional physical firewall into a cloud infrastructure. This addition provides an enhanced layer of security, including URL filtering, advanced threat mitigation, and DDoS prevention, among other features. Figure 2 offers an illustrative depiction of the OSI model and system functionalities based on layers.

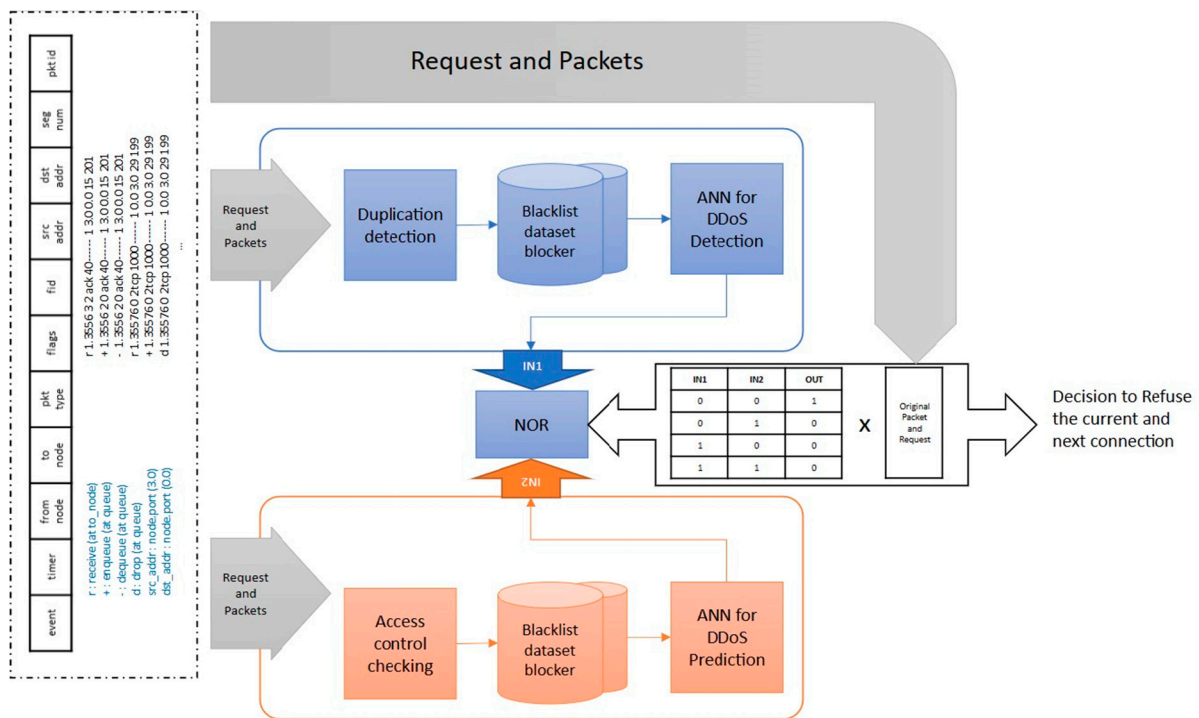


Figure 1. The proposed algorithm consists of two main streams.

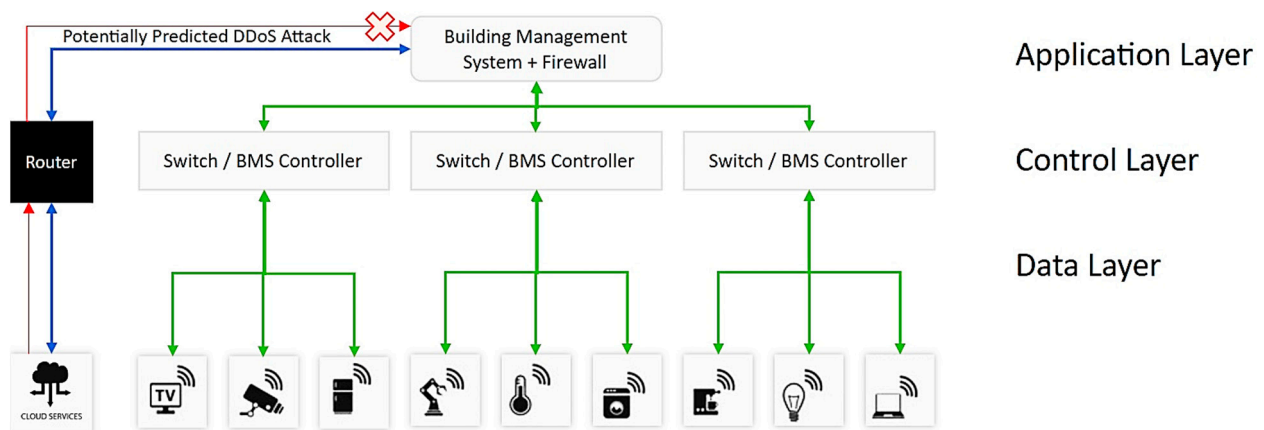


Figure 2. OSI model to demonstrate the system functionalities and sections based on layers.

3.4. Dataset Justification

The choice of the Canadian Institute for Cybersecurity (CIC) IoT Dataset 2022 for evaluation in our study requires clarification [24]. Although the dataset primarily comprises Denial of Service (DoS) attacks, it provides valuable insights into attack patterns, network behavior, and system vulnerabilities that contribute to understanding the problem of DDoS attacks in BMS. The dataset, despite its focus on DoS attacks, enables us to gain knowledge applicable to the development of effective defense mechanisms against DDoS attacks in the BMS context. Building upon the existing pseudo-code, we modified it to integrate the SMOA for feature selection. The enhanced pseudo-code provided a step-by-step representation of our algorithm, incorporating SMOA within the feature selection process. This modification improves the clarity and replicability of our proposed approach. Although the dataset used for evaluation in our study primarily focuses on DoS attacks rather than DDoS attacks, it still contributes significantly to understanding the challenges posed by DDoS attacks in BMSs. The dataset's relevance stems from the following justifications:

- **Similar Attack Patterns:** Despite the distinction between DoS and DDoS attacks, they share fundamental similarities in terms of their objectives and impact [8]. Both attack types aim to overwhelm system resources, leading to service disruption or unavailability. By studying DoS attacks, which are extensively documented in existing datasets, we can gain valuable insights into attack mechanisms, traffic patterns, and mitigation techniques that can be adapted to address DDoS attacks in BMSs.
- **Detection and Response Strategies:** The detection and response strategies employed to counter DoS attacks can serve as a solid foundation for developing effective countermeasures against DDoS attacks. While the scale and complexity of DDoS attacks may differ, understanding the principles of detection and response can facilitate the adaptation and enhancement of existing techniques to mitigate DDoS attacks in BMS effectively [25].
- **Resource Utilization and Performance Evaluation:** DoS attacks often target specific system resources or services, resulting in abnormal resource utilization and performance degradation. By analyzing DoS attacks within the BMS context, we can gain insights into the impact of such attacks on critical resources, system performance, and overall operational efficiency. This understanding can inform the design of robust defense mechanisms and resource allocation strategies to mitigate the effects of DDoS attacks.
- **Algorithm Validation:** Although an ideal dataset specifically tailored to DDoS attacks in BMS would be preferable, the availability of comprehensive and well-labeled datasets is limited. Thus, the DoS attack dataset utilized in our study serves as a foundation for validating the effectiveness and performance of our proposed algorithm in detecting and mitigating attacks. Conducting experiments with a realistic attack dataset, even if not DDoS-specific, allows us to assess the algorithm's robustness, accuracy, and scalability within a relevant context.

Our choice of the Canadian Institute for Cybersecurity (CIC) IoT Dataset 2022 is not arbitrary. While the dataset predominantly focuses on DoS attacks, it provides invaluable insights into attack trends, system vulnerabilities, and network behaviors. This knowledge is paramount for understanding and tackling DDoS threats in BMS.

3.5. Recorded Data Distribution

For the training and testing of our model, we employed the CIC IoT Dataset 2022 [24]. This dataset sheds light on DDoS attacks' impact on server resources, firewalls, and other communication devices. For a visual representation of these distributions, histograms were created, as depicted in Figure 3.

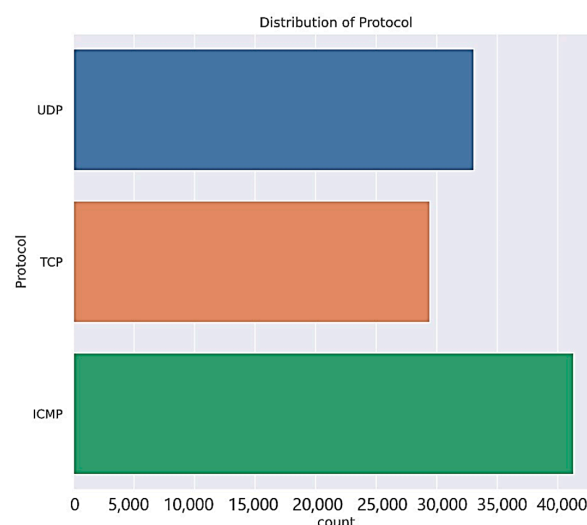


Figure 3. Data distribution.

3.6. Artificial Intelligence (AI) Model Elaboration

The vulnerability of IT and OT endpoints in IoT is a rising concern, especially given that DDoS traffic often mimics regular traffic. Addressing this, our method uses multiple AI techniques to formulate a dynamic machine-learning-based model. This model, using an SVM classifier, efficiently classifies DDoS attack traffic and detects potential threats.

Table 1 provides a comprehensive view of the AI model's structure, highlighting the output model/shape, layer type, and number of parameters.

Table 1. Extracted model structure with parameters.

Output Model and Shape	Layer Type	Parameter Number
(Sequential, 28)	Dense	1596
(Sequential, 10)	Dense	290
(Sequential, 01)	Dense	11
Total params: 1897	Trainable params: 1897	Non-trainable params: 0

Further testing revealed the efficacy of our proposed model. Using SVM, KNN, and LR classifiers, we observed that our model outperformed alternative classifiers in detecting and mitigating attacks. Table 2 presents a comparative analysis of these results.

Table 2. Comparison of proposed method using classifiers.

Classifier Algorithms	Model Testing Accuracy
SVM	97.44%
KNN	96.46%
LR	83.69%

4. Results and Discussion

Following a comprehensive literature review and the development of machine learning models using the NN DDoS detection method, we obtained our results. Our algorithm contrasts the NN outputs with a specialized SVM to authenticate the findings. We performed an analysis using the CIC IoT Dataset 2022 attack data combined with the NS-2 network simulation to validate the functionality and efficacy of the proposed algorithm. Figure 4 illustrates the data results distribution based on packet counts, flows, and byte counts. Additionally, the attacked data are labeled with 1 and an orange color, and the normal data traffic is labeled with 0 and a blue color, as shown in Figure 4 below. Data are displayed graphically according to traffic flows, the byte count, the density of the traffic, and the count of the packets.

Simulation assessments of the implemented algorithm revealed that the proposed method outperformed single NN projects in detecting intricate DDoS techniques, such as combinational attacks using UDP flood, SYN flood, Zero-day, fragmented packets, and ping of death attacks. Whereas single NN projects reported accuracies of 73% and 76% [25], our algorithm, incorporating SVM and multiple layers of Neural Networks, achieved an impressive accuracy of 99.19% with the CIC dataset, as documented in Table 3. Figure 5 visualizes the training and validation accuracy over various epochs.

Table 3. Extracted model structure with parameters.

Precision Factors	Recall	F1 Score ¹	Val-Accuracy
Accuracy	0.9923	0.9920	0.9919
Value loss	0.0195	0.9920	0.9919

¹ F1 Score = $2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})$.

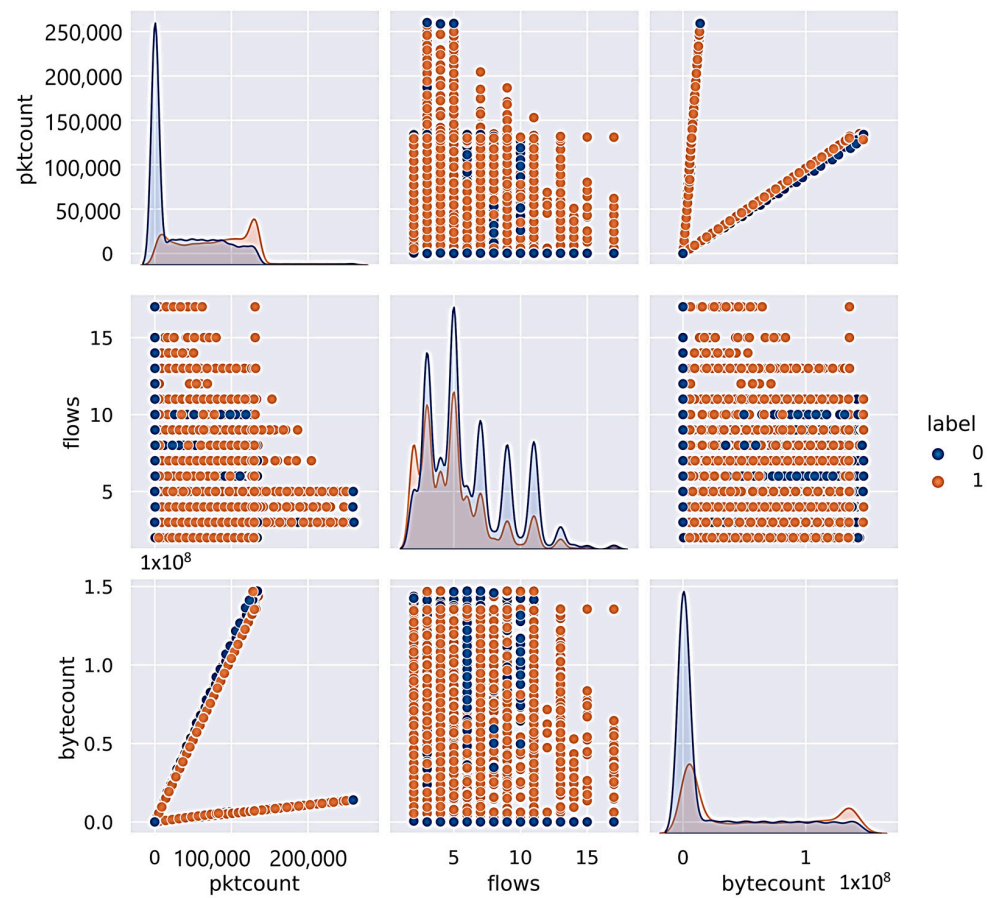


Figure 4. Data result distribution based on packet counts, flows, and byte counts.

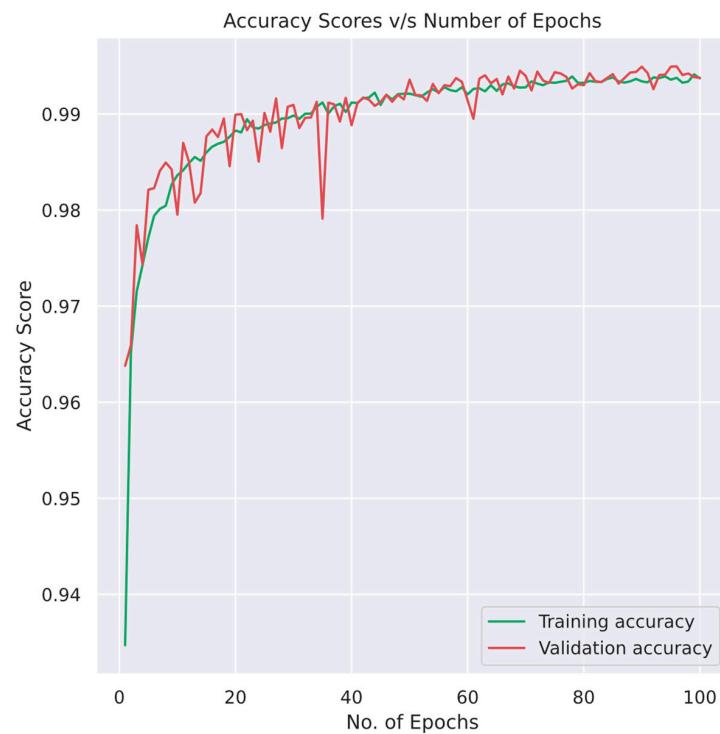


Figure 5. Training and validation accuracy demonstration for different numbers of epochs.

DDoS attacks can instigate significant technical and infrastructure disruptions, resulting in substantial damage or compromised system operations [25]. Traditional IoT

protocols, such as the Message Queuing Telemetry Transport (MQTT) protocol, are often inadequate in warding off advanced DDoS assaults [26,27]. A myriad of studies have delved into DDoS attack detection in IoT systems utilizing machine learning techniques; however, a majority report sub-optimal detection accuracy for sophisticated DDoS strikes [28,29].

In comparison to existing methods that prioritize features based on top scores from multiple classifiers, our proposed method stands out. Despite leveraging a reduced set of features, our methodology delivered enhanced accuracy, as showcased in Table 4. Parameters, such as classification type, feature count, and algorithms used, were taken into account for this comparison.

Table 4. Extracted model structure with parameters.

Method	No of Features	Classifiers	Accuracy
R.J. Alzahrani and A. Alzahrani [30]	24	KNN, SVM, NB, DT, RF, and LR	99%
M. Aamir and S.M.A. Zaidi [31]	25	KNN, SVM	98%
Sekar et al. [32]	18	DT	96.25%
Khanday et al. [33]	20	Linear SVM, NB, LR, ANN, LSTM	99%
Proposed Method	21	SVM, KNN, LR + Parallel Synchronized 2-step algorithm (Detection and Verification Using Predictor)	99.19%

When the evaluation of our suggested technique is conducted using the relevant articles, methodologies, and datasets used in our literature review, our research exhibits divergence in terms of the dataset and methodology employed. The primary distinction in our approach is in the use of hybrid modelling techniques. The correctness of the model is verified by the F1 Score, as shown in Tables 3 and 4. Furthermore, it is widely acknowledged that the metric of Recall, which quantifies the proportion of transactions correctly identified as positive, indicates that our mistake tolerance stays at a minimal threshold. Through the implementation of a three-layer back propagation network, Zhang and colleagues demonstrated that a Neural Network with a dynamic structure is capable of producing identical control parameters within the specified flight circumstances, resulting in consistent responses, as seen before. The methods used in game theory are well-established mathematical modelling tools. Notably, game theories have been effectively implemented in conventional artificial intelligence decision-making systems, as shown by the successful outcomes achieved.

5. Conclusions

The advent of intelligent building applications has the potential to provide cybersecurity vulnerabilities for both individuals and organizations, as well as the technologies they rely on. One of the significant risks that deserves attention is the DDoS assaults perpetrated by botnets targeting BMSs. The objective of these DDoS attacks is to compromise both websites and the whole BMS infrastructure by inundating connections with a substantial volume of data. Despite the emergence of several machine-learning-supported detection systems, our work presents a novel defense approach. The present research used a machine learning model with a focus on Neural Networks to detect DDoS threats.

Additionally, SVM was utilized to enhance the accuracy of the detection process. The SMOA algorithm is used for feature selection to enhance the efficacy of DDoS detection in BMSs, hence reinforcing its sensitivity. The model effectively identifies and mitigates

intrusion attempts by offering robust defense mechanisms against DDoS assaults. The findings obtained in this study confirm the significant efficacy of the algorithm suggested, particularly in its ability to identify intricate DDoS assaults. One notable limitation is the incongruity between the research emphasis of our work, which centers on DDoS assaults, and the assessment dataset, which mostly focuses on DoS attacks. Furthermore, a discrepancy exists between the system model described in our research work and the testing conditions of the dataset. Moreover, the system model does not comprehensively represent the SDN-enabled smart building environment. The existence of this difference raises concerns about the suitability of the dataset for use in BMS situations. Notwithstanding these constraints, our study indicates significant advancements in the identification and alleviation of DDoS attacks in BMSs. The use of NN, SVM, and SMOA enhances the efficacy of our approach in mitigating DDoS attacks. The accuracy of the suggested model was found to be 99.19% when assessed using the CIC dataset and using modular MVP coding paradigms.

After overcoming the highlighted limitations, our technique is positioned to achieve even higher efficacy, offering a bright outlook for the advancement of smart buildings. Our forthcoming endeavors include completing the necessary tasks to enhance the degree of security protection in BMSs by implementing several layers of defense against various cyber-attack techniques.

Author Contributions: Conceptualization, İ.A. and M.K.; methodology, İ.A.; software, M.K.; validation, İ.A. and M.K.; results analysis, İ.A. and M.K.; writing—original draft preparation, İ.A.; writing, reviewing, and editing, İ.A. and M.K.; supervision, İ.A. and M.K.; funding acquisition, İ.A. and M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Our experimental data are all open-source datasets.

Acknowledgments: This research utilized the IoT Dataset 2022 provided by the Canadian Institute for Cybersecurity (CIC). The researchers would like to express gratitude to Sajjad Dadkhah, Hassan Mahdikhani, Priscilla Kyei Danso, Alireza Zohourian, Kevin Anh Truong, and Ali A. Ghorbani for their collaboration in profiling the realistic, multi-dimensional IoT dataset.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shang, W.; Ding, Q.; Marianantoni, A.; Burke, J.; Zhang, L. Securing building management systems using named data networking. *IEEE Netw.* **2014**, *28*, 50–56. [CrossRef]
2. Cauteruccio, F.; Fortino, G.; Guerrieri, A.; Terracina, G. Discovery of Hidden Correlations between Heterogeneous Wireless Sensor Data Streams. In *Internet and Distributed Computing Systems. IDCS 2014*; Fortino, G., Di Fatta, G., Li, W., Ochoa, S., Cuzzocrea, A., Pathan, M., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2014; Volume 8729. [CrossRef]
3. Nugent, E.; August, M.R. SCADA Cybersecurity in the Age of the Internet of Things: Supervisory Control and Data Acquisition (SCADA) Systems' Traditional Role Is Changing as the Industrial Internet of Things (IIoT) Continues to Take a Larger Role. SCADA Systems Need to Adjust, Control Engineering. Available online: <https://www.controleng.com/articles/scada-cybersecurity-in-the-age-of-the-internet-of-things/> (accessed on 20 March 2023).
4. Heino, J.; Hakkala, A.; Virtanen, S. Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity* **2022**, *5*, 25. [CrossRef] [PubMed]
5. Vishwakarma, R.; Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun. Syst.* **2020**, *73*, 3–25. [CrossRef]
6. Taherian-Fard, E.; Niknam, T.; Sahebi, R.; Javidsharifi, M.; Kavousi-Fard, A.; Aghaei, J. A Software Defined Networking Architecture for DDoS-Attack in the Storage of Multimicrogrids. *IEEE Access* **2022**, *10*, 83802–83812. [CrossRef]
7. Anwar, Z.; Malik, A.W. Can a DDoS attack meltdown my data center? A simulation study and defense strategies. *IEEE Commun. Lett.* **2014**, *18*, 1175–1178. [CrossRef]
8. Mahjabin, T.; Xiao, Y.; Li, T.; Chen, C.L.P. Load Distributed and Benign-Bot Mitigation Methods for IoT DNS Flood Attacks. *IEEE Internet Things J.* **2020**, *7*, 986–1000. [CrossRef]

9. Press, G. 22 Million Amazon Echo Smart Speakers to Be Sold in 2017, Driving US Smart Home Adoption, Forbes. Available online: <https://www.forbes.com/sites/gilpress/2017/10/29/22-million-amazon-echo-smart-speakers-to-be-sold-in-2017-driving-us-smart-home-adoption/?sh=1c0e1b72481a> (accessed on 23 March 2023).
10. Panda, P. OWASP's Top 10 IoT Vulnerabilities and What You Can Do—Intertrust Technologies, Intertrust. Available online: <https://www.intertrust.com/blog/owasps-top-10-iot-vulnerabilities-and-what-you-can-do/> (accessed on 23 March 2023).
11. Kaspersky Lab Team. DDoS Intelligence Report: Long-lasting Attacks, Amplification Attacks and Old Botnets Make a Comeback | Kaspersky, Kaspersky Lab. Available online: https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-ddos-intelligence-report-long-lasting-attacks-amplification-attacks-and-old-botnets-make-a-comeback (accessed on 26 March 2023).
12. Singh, A.; Chatterjee, K.; Satapathy, S.C. An edge based hybrid intrusion detection framework for mobile edge computing. *Complex Intell. Syst.* **2022**, *8*, 3719–3746. [\[CrossRef\]](#)
13. Wu, G.; Chen, Y.; Zhang, G. ENFW: An Industrial Firewall for Edge Computing. In Proceedings of the 12th International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Baishan, China, 27–31 July 2022. [\[CrossRef\]](#)
14. Zhang, Y.; Liu, Y.; Guo, X.; Liu, Z.; Zhang, X.; Liang, K. A BiLSTM-Based DDoS Attack Detection Method for Edge Computing. *Energies* **2022**, *15*, 7882. [\[CrossRef\]](#)
15. Myneni, S.; Chowdhary, A.; Huang, D.; Alshamrani, A. SmartDefense: A distributed deep defense against DDoS attacks with edge computing. *Comput. Netw.* **2022**, *209*, 108874. [\[CrossRef\]](#)
16. Zhou, L.; Guo, H.; Deng, G. A fog computing based approach to DDoS mitigation in IIoT systems. *Comput. Secur.* **2019**, *85*, 51–62. [\[CrossRef\]](#)
17. You, W.; Jiao, L.; Li, J.; Zhou, R. Scheduling DDoS Cloud Scrubbing in ISP Networks via Randomized Online Auctions. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020. [\[CrossRef\]](#)
18. Zhang, P.; Yang, X.; Chen, Z. Neural network gain scheduling design for large envelope curve flight control law. *J. Beijing Univ. Aeronaut. Astronaut.* **2005**, *31*, 604–608.
19. Yang, X.; Gong, G.; Tian, Y. Generalized Optimal Game Theory in virtual decision-makings. In Proceedings of the 2008 Chinese Control and Decision Conference, Yantai, China, 2–4 July 2008; pp. 196–1964.
20. Forestiero, A.; Mastroianni, C.; Spezzano, G. Reorganization and discovery of grid information with epidemic tuning. *Future Gener. Comput. Syst.* **2008**, *24*, 788–797. [\[CrossRef\]](#)
21. Abualigah, L.; Elaziz, M.A.; Khodadadi, N.; Forestiero, A.; Jia, H.; Gandomi, A.H. Aquila Optimizer Based PSO Swarm Intelligence for IoT Task Scheduling Application in Cloud Computing. In *Integrating Meta-Heuristics and Machine Learning for Real-World Optimization Problems. Studies in Computational Intelligence*; Houssein, E.H., Abd Elaziz, M., Oliva, D., Abualigah, L., Eds.; Springer: Cham, Switzerland, 2022; Volume 1038. [\[CrossRef\]](#)
22. Fujita, H. Assist-iot: A reference architecture for next generation internet of things. In *New Trends in Intelligent Software Methodologies, Tools and Techniques: Proceedings of the 21st International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT_22)*; IOS Press: Amsterdam, The Netherlands, 2022; p. 109.
23. Wang, J.; Zheng, L. SD-WAN: Edge Cloud Network Acceleration at Australia Hybrid Data Center. In *Advanced Information Networking and Applications*; Barolli, L., Hussain, F., Enokido, T., Eds.; Lecture Notes in Networks and Systems; AINA 2022; Springer: Cham, Switzerland, 2022; Volume 450. [\[CrossRef\]](#)
24. Dadkhah, S.; Mahdikhani, H.; Danso, P.K.; Zohourian, A.; Truong, K.A.; Ghorbani, A.A. Towards the Development of a Realistic Multidimensional IoT Profiling Dataset. In Proceedings of the 19th Annual International Conference on Privacy, Security & Trust (PST), Fredericton, NB, Canada, 22–24 August 2022. [\[CrossRef\]](#)
25. Jaszcz, A.; Połap, D. AIMM: Artificial Intelligence Merged Methods for flood DDoS attacks detection. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 8090–8101. [\[CrossRef\]](#)
26. Ali, M.H.; Jaber, M.M.; Abd, S.K.; Rehman, A.; Awan, M.J.; Damaševičius, R.; Bahaj, S.A. Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT). *Electronics* **2022**, *11*, 494. [\[CrossRef\]](#)
27. Husnain, M.; Hayat, K.; Cambiaso, E.; Fayyaz, U.U.; Mongelli, M.; Akram, H.; Ghazanfar Abbas, S.; Shah, G.A. Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System. *Sensors* **2022**, *22*, 567. [\[CrossRef\]](#) [\[PubMed\]](#)
28. Ibtissam, K.; Abdelrahman, M.S.; Alrashide, A.; Mohammed, O.A. Assessment of Protection Schemes and their Security under Denial of Service Attacks. In Proceedings of the IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Prague, Czech Republic, 28 June–1 July 2022. [\[CrossRef\]](#)
29. Yaser, A.L.; Mousa, H.M.; Hussein, M. Improved DDoS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder. *Future Internet* **2022**, *14*, 240. [\[CrossRef\]](#)
30. Alzahrani, R.J.; Alzahrani, A. Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic. *Electronics* **2021**, *10*, 2919. [\[CrossRef\]](#)
31. Aamir, M.; Zaidi, S.M.A. DDoS attack detection with feature engineering and machine learning: The framework and performance evaluation. *Int. J. Inf. Secur.* **2019**, *18*, 761–785. [\[CrossRef\]](#)

32. Sekar, R.R.; Jenny, A.M.; Sreshta, D.; Vikas, M.; Ajay, D.B.N.; Ganesh, M. Prediction of Distributed Denial of Service Attacks in SDN using Machine Learning Techniques. In Proceedings of the 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubballi, India, 23–25 June 2023; pp. 1–5. [\[CrossRef\]](#)
33. Khanday, S.A.; Fatima, H.; Rakesh, N. Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks. *Expert Syst. Appl.* **2023**, *215*, 119330. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.