Journal of Administrative and Economic Sciences • Vol 15, Issue 2 (2022) • p 1-16

Challenges Facing IoT Expansion: Security and Energy

Sami Mahfoudhi

Department of Management Information Systems and Production Management, College of Business and Economics,

Qassim University, P.O. Box: 6640, Buraidah 51452 • Kingdom of Saudi Arabia

s.mahfoudhi@qu.edu.sa

Abstract:

The expansion of IoT (Internet of Things) is facing some resistance from organizations' managers fearing security issues as well as technical and operational feasibility obstacles, in particular the energy consumption problem. Despite the legitimacy of these concerns, possible technical solutions exist to face them. These solutions are based on the use of machine learning techniques, namely Random Forest, Support Vector Machines and Artificial Neural Networks, to face the security risk by detecting intrusions at a high accuracy rate. In addition, our approach applies dimension reduction techniques such as Principal Components Analysis to minimize data sending and consumption. Therefore, our proposed solution show promising results in boosting security and quality of services (QoS) in IoT-cloud environments based on machine learning.

Keywords: IoT, cloud, security, QoS, intrusion detection, artificial intelligence, energy, dimension reduction.

1 Introduction

Recently, Internet of things (IoT) has become one of the hot topics of research. These little devices combined with software are taking more importance and are spreading increasingly replacing the human intervention being the better option in term of efficiency, cost and easiness. All the advantages provided by the IoT to companies can lead to the conclusion that IoT must be mass adopted by organizations without any delay. Nevertheless, some obstacles to this worldwide diffusion can be observed; security and energy consumption being the main expansion challenges. Thus, managers are worried about this new technology despite its known benefits.

Firstly, the security problem may have a strong impact on the Internet of Things (IoT) expansion and effect on people's lives, business operations, and government services. In fact, hackers are always on the search for minor security flaws, and they are often successful in their threats to steal identity and financial data. The user can no longer be confident in his anonymity or privacy [1][2].

Traditional security methods are no longer sufficient [1][2]; businesses must evaluate a wide and diverse number of threats and investigate a more active solution to repair network breaches, detect risks, and restore system functioning.

The security challenge facing IoT-cloud expansion is basically composed of two main threats [1][3]:

--The hacking of the cloud server through the internet, which is a potential risk that could pose significant threat to IoT architecture by stealing sensitive secured data, which is the most common risk, or by controlling the IoT devices for the purpose of exploitation.

--The hacking of the cloud server through the IoT sensors themselves, which is possible considering that some IoT sensors are installed in remote non-secured areas.

Accordingly, malicious users' assaults undermine the network's performance by deleting or altering exchanged messages, or by revealing secret information included in these messages. As a result, if an outside attacker gains access to the user's rights and credentials, he or she will be able to intercept transactions, manipulate data, provide false information, and saturate all services and resources. These attacks may have a negative influence on the organization's reputation and productivity [4]. Additionally, these attacks may result in significant income and client losses.

Furthermore, insider attacks are one of the most dangerous threats that face many systems today. An insider attack is carried out by people who are legitimately authorized in the system to perform certain tasks but decide to abuse this trust and harm the organization by causing breaches in the confidentiality, integrity, or availability of the organization's assets.

Data's integrity and accessibility are ensured by designing a secure model such as an intrusion detection system (IDS). Although proposals for new security measures available in the literature are diverse, there are various critical security issues and performance in Cloud-IoT networks that persist [2].

Another challenge facing the IoT expansion is the problem of energy consumption represented in the internet bandwidth consumption and the problem of cloud data storing [2]. In fact, energy efficiency has become a major concern in data centers and IoT sensors due to the environmental impact, cost, and operational expenses. The infrastructure requires resource planning in order to address the issue of energy waste, although this has recently been reduced substantially due to the utilization of best-practice technologies [5].

The high energy consumption of hardware devices, hosts, computation resources, and technologies has increased concerns about their usage [6]. In this context, a datacenter is similar to a farm in that it houses a large number of servers that provide networking, data management, data storage, and recovery services. When it comes to datacenter difficulties, the two primary obstacles are currently energy efficiency and trustworthiness. At the infrastructure level, cooling systems consume half of the energy provided to a datacenter, and systems consume a significant amount of energy when they are idle [4]. According to the research [7], the overall worldwide power usage of datacenters in 2015 was almost 416.2 terawatts, which is more than the energy consumption of the United Kingdom.

According to the research of Gartner [8], cloud datacenters' power usage grew to 12.02 billion kWh by 2020. Both suppliers and consumers suffer from financial losses. If effective power management methods are not used alongside the increasing capabilities of datacenters, then datacenter power consumption will continue to rise.

Therefore, company managers are still dubious about the use of IoT as they fear problems related to security and energy consumption. In fact, most of them lack technical knowledge and may have an inaccurate concept of IoT effects and outcomes, especially on infrastructure. This mindset is a real handicap to IoT expansion. Thus, they keep postponing the integration of IoT and then missing all the benefits provided by this new way of collecting data. Consequently, it is imperative to encourage and motivate managers by explaining and clarifying that infrastructural problems have solutions [5].

In response to managers fears toward IoT integration, cloud suppliers have been trying to develop effective cloud services. A number of experts from around the world have proposed algorithm architecture and rules to make the cloud computing environment more secure and energy efficient.

Therefore, the key challenge is to design a complete model for secure data transfer and management with an appropriate solution for best energy allocation between all components. This issue becomes much more critical when considering the performance requirements associated with the IoT-limited Cloud's access latency. To reach this goal, experts should take advantage of the huge amounts of existing data through training effective machine learning models. In fact, rules may be difficult to extract from classic approaches while trained models can learn the right patterns from historical data and continue to improve them through incremental learning over the latest data streams.

In this paper, we address all the above critical issues and propose a secure scheme with a Machine-Learning- based IDS to further enhance the data security and privacy of cloud/IoT networks. Moreover, we design an energy efficient system based on dimension reduction techniques to improve the performance of these environments.

2 Related work

2.1 The security challenge

Recently, researchers have worked to overcome intrusion detection difficulties in IoT networks [9]. These studies employ a variety of methods, including machine learning. This section discusses relevant research dealing with network-based intrusion detection [10].

Hajiheidari et al.[11] presented a Systematic Literature Review (SLR) of the IDSs in the IoT environment. The authors also provided detailed categorizations of the different classic IDSs in the IoT and their benefits and drawbacks.

However, for Zarpelao et al.[12] implementing classic IDS approaches to IoT is challenging and perhaps difficult because to the IoT's unique features, including resource-constrained devices, proprietary protocol stacks, and standards.

Furthermore, Asharf et al.[13] confirmed that the boom of IoT devices, which can be readily expanded in comparison to desktop PCs, has resulted in a surge in cyber-attack instances using IoT devices. To address this issue, it is necessary to create novel approaches for identifying attacks launched by hacked IoT devices.

Sharma et al. [14] describe several IDS detection approaches, such as misuse-based, specification-based, and anomaly detection. The authors of the study make recommendations for sensor networks based on the benefits and drawbacks of IDS. Furthermore, several potential directions for IDS selection are mentioned.

While Wazid et al. [15] present an IDS approach for detecting numerous malicious attack types that occur in an IoT network-based environment. The authors used two classification techniques, namely naive Bayes and KNN, to detect malicious activity.

Also, Moustafa et al. in [16] present an intrusion detection system (IDS) based on a client-based system that exploits anomalies to identify an attacker known as E-Spion. Three-layered security was considered for improved security. However, the higher protection level resulted in greater overhead.

Sun and Yu [17] establish and suggest intrusion detection techniques for detecting the routing attack affecting the environment in Edge-based IoT (E-IoT).

In the other hand, Venkatraman and Surendiran [18] suggest hybrid IDS based on the studied multimedia files. To train the IDS model and detect intruders in Internet of Things (IoT) networks, they used internet resources as repositories. The acquired test findings were up to 99.06 percent accurate for recognizing various attacks in IoT settings such as deny of services (DoS), control hijacking.

However, the security issue is not the only handicap facing IoT expansion and adoption from the managers' point of view. The energy consumption challenge for instance represents another major problem that has to be treated. In the other hand, although technical solutions are available, managers would like to be assured about their efficiencies and reliabilities. Therefore, additional researches emphasizing the accuracy and the precision of intelligent security systems will bring more relief for managers about the security threat and challenge.

2.2 The energy challenge

According to [19], electricity accounts for approximately 70% of total data center running expenses, thereby emphasizing the need to reduce energy use. Researchers have attempted to suggest answers in this field using a variety of techniques, including heuristics and algorithms.

The difficulty with these approaches is that they are not workload-specific, they are unable to handle workload fluctuations due to a lack of dynamicity, and they require previous knowledge of the workload in order to modify parameters. However, some researchers have attempted to tackle the problem using machine learning. Machine learning can manage fluctuating workload behavior since it is workload-specific, and it does not require workload specialization.

As an example, Green IoT aims to minimize the energy usage of IoT devices while also protecting the environment [20]. As a result, it is critical to use an efficient routing strategy for network routing. Multi-hop routing and clustering are two approaches that have been proposed to increase network performance and energy efficiency [21]. One or more intermediary nodes direct data to the base station in multi-hop routing. Direct

data transfer would suddenly discharge the nodes if the source nodes are far from the base station; thus, multi-hop routing can minimize node energy usage [22].

Minimum transmission energy is a multi-hop routing approach. In this approach, each node directs data from other nodes in order to decrease the overall energy of the transfer [23].

Some researchers have employed the weighted sum [24], normalization [25], and normalizing [26] methods to arrive at a single best solution for tackling energy-aware IoT-based strategies in CDC. [27] introduce a new priority, power, and traffic-conscious VM placement algorithm that aims to reduce the energy use of incoming IoT traffic servers. Finally, the authors of [28] provide a safe technique for controlling the impact of IoT device requests on the network. Moreover, an energy-aware algorithm was intimately connected to the energy consumption model, and every energy-saving algorithm was reliant on a certain power model. The accuracy of the power model directly reflects the benefits and drawbacks of an energy-saving method. Specifically, in [29], the authors used deep learning technology to create a unique energy consumption model. Their approach considered 12 energy-related variables and used deep neural network architecture to create an energy consumption model.

The authors of [30] present numerous power models, including mixed load and I/O-intensive demand. While the authors of [31] introduce an energy-efficient work prioritization model in order to create a fairness job-scheduling algorithm in the CDC. Nonetheless, the suggested model in this study focused on the energy model, which was a threshold-based provisioning mechanism that was validated using a real-world workload.

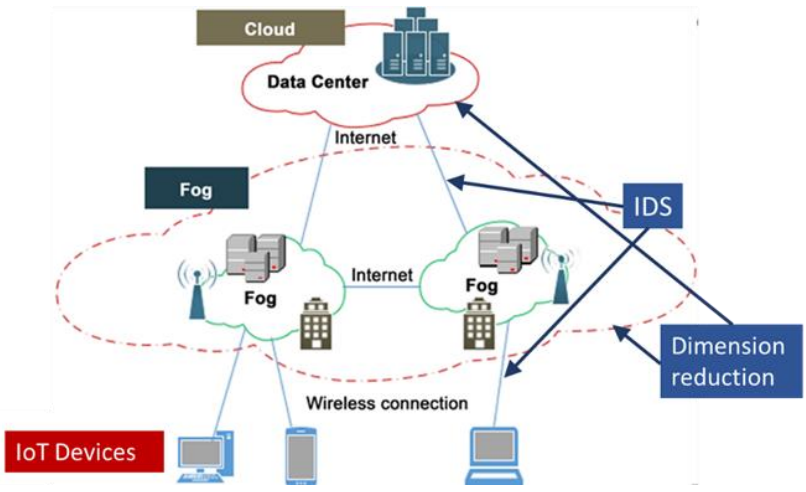
3 Overview of the proposed contribution

There always has been a trade-off between security features and system performance for Cloud-IoT environments. Consequently, maximizing resource utilization while minimizing energy consumption is a big challenge.

Consequently, we propose a system that can:

- Provide high security by encrypting transferred data among IoT-cloud;
- Detect malicious actions and identify network attacks; and
- Optimize energy consumption.

Figure 1: Overview of the proposed architecture



Our proposed system model includes components that will be incorporated in an IoT-cloud system. This generalized model can be used in different scenarios depending upon the application requirements. The proposed architecture contains a model for data security and energy efficiency. In fact, for network attacks, we aim to use IDS. Then, we deploy the dimension reduction strategy to minimize energy consumption in the IoT-cloud environment.

Figure 1 presents the proposed architecture illustrating an overview of our proposal.

3.1 Intrusion detection

Here, maximizing data security is taken as the primary objective. Numerous attacks in the Internet of Things (IoT) and cloud environment are occurring as a result of numerous breaches. In fact, a large portion of these threats is comprised of small variations of recently known cyberattacks. Accordingly, ensuring privacy and security to IoT users is one of the timeliest and urgent research issues.

Therefore, among the widely used data security techniques is the Intrusion Detection System (IDS), a form of detecting system that secures networks by providing all systems with monitoring services. Furthermore, in instances when incursion and other security breaches must be found fast and effectively, an IDS is a key component of network security.

An effective IDS must meet certain needs such as flexibility, real-time, and scalability. These requirements have prompted several studies in an attempt to develop a next-generation IDS that meets all of these needs. IDS is frequently comprised of five components.

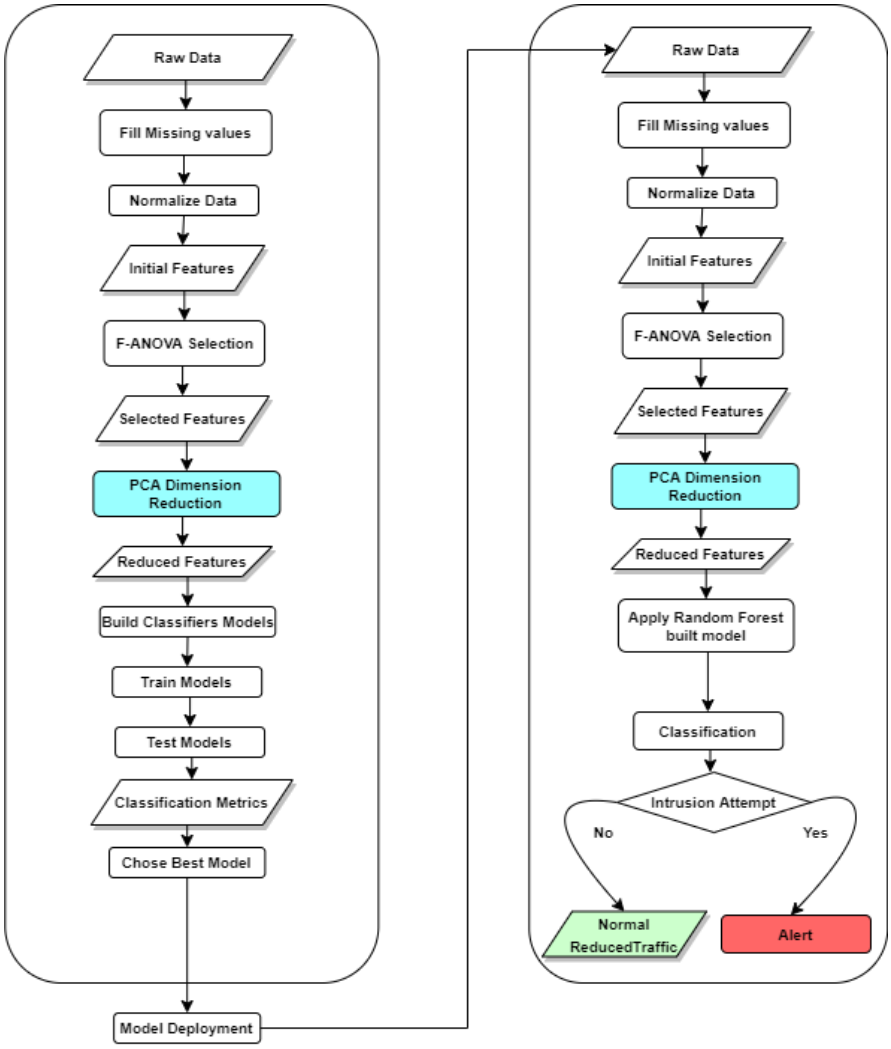
The primary role of the Network Engine is to analyze all network traffic (protocols, ports, subnets, etc.) and interact with the Analysis System, which is the brain of the IDS. The Analysis System is in charge of detecting intruders. The Analysis System is made up of five parts: a pretreatment module, a rule knowledge base, a protocol analysis module, a data analysis module, and a secure communication module. Its function is to examine data from the Network Engine. When an incursion is discovered, the Response System must take the appropriate action of either an alarm or a defensive measure. These metrics are transmitted to the Console so that they may be shown to users.

The principal aim of machine learning systems is to simplify open communication between humans and computers. Indeed, improved environmental awareness is made possible by an intelligent analytical approach that increases network performance primarily in terms of latency and energy consumption metrics.

In fact, owing to its highest extraction capability, machine learning algorithms have introduced numerous benefits in different security fields. In this context, we propose the use of classification techniques to deal with the problem of intrusion detection. Specifically, we applied a set of classification tools on a real IoT dataset to detect intrusion. Figure 2 displays the detailed steps of our proposal.

Therefore, we install an intelligent intrusion detection system (IIDS) on the IoT-cloud network to monitor the whole network, oversee traffic, and analyze transferred data. When a new assault is discovered and identified by new signatures, the IIDS classifies the traffic as normal or anomalous. To make up for the lack of a monitoring system and to avoid potential risks, the proposed attack detection model could be implemented.

Figure 2: Overview of the proposed intelligent intrusion detection system



This activity is responsible for arranging the IIDS in order to acquire the basic information that will be utilized for the learning phase. To be effective, the IIDS must be able to recognize network attributes such as the presence of different types of services, components, architecture, type, memory capacity and operating systems on a network, as well as vulnerabilities.

After gathering the essential information, the IIDS analyzes and categorizes traffic flows as normal or malicious. It can identify abnormal traffic by comparing it to regular traffic using an ML technique after analyzing a large amount of data. Then, it employs network audit technologies to produce alarms. To this end, several well-known ML techniques for their high performance were applied mainly Random Forest, Support Vector Machines and Artificial Neural Networks.

The proposed smart attack detection system consists of three phases: data preparation, feature selection and extraction, and the attack classification. To begin, the first phase is data preparation which is a treatment process to ensure high-quality data. Second, feature extraction is required to extract and bring out several types of characteristics as vectors from data. In the last phase, the goal of this step is to create

classifiers that employ the characteristics of the attack to distinguish attacks from regular data.

Our intelligent system has significant potential in attack detection, and it may be ideal for real-time applications in IoT-cloud computing.

3.2 Energy efficiency

In the IoT-cloud environments, the phase of analyzing and treating heterogeneous data obtained from many sources is difficult and time-consuming. The management of these data is difficult without ignoring duplication, irrelevant, and unneeded data. Moreover, these environments consume a large amount of energy to provide efficient and reliable services to users.

To this end, we aim to reduce energy usage in the IoT-cloud by eliminating superfluous data with Artificial Intelligence (AI) technologies. Indeed, the application of AI techniques allows for the separation of superfluous data gathered by IoT devices in order to prevent overloading storage and data processing. Ignoring unneeded or duplicated data will aid in avoiding an overflow of objects, internet connections, and servers. Furthermore, this enables the optimal functionality of IoT devices. Our findings are analyzed using PCA (Principal Component Analysis) as a feature extraction method.

In this context, to improve machine learning performance and reduce dimension, two frequently utilized approaches are used: feature selection and feature extraction as we have shown in Figure 2.

Feature selection is a dimension-reducing method used as an advanced step in machine learning. It is effective in removing irrelevant data, lessening changes, increasing learning accuracy, enhancing predictor performance, improving understanding of results, providing faster and lower-cost predictors, and emphasizing the most crucial process generating the data. Feature selection is classified into three types: wrappers, filters, and embedding. Wrappers are superior to filters since they were optimized for the classifier employed. As a result, wrapper techniques have a high computational cost; thus, they are expensive and sluggish when employed for big features.

Feature extraction is the process of applying some transformation to important characteristics in order to create more significant features. Features extraction, which treats each feature variable as a linear mixture of relevant input variables, is used to minimize complexity and simplify data representation. Principal component analysis (PCA) and linear discriminant analysis (LDA) are the two primary feature extraction approaches that have been widely employed in various fields.

4. Results and Discussion

In this section, the evaluation of our contribution is outlined. Please note that the proposed approach was implemented on google Colab using Python programming language. Preprocessing, training, testing, dimension reduction operations was developed using well known python packages such as Pandas, Scikit-learn and Keras.

4.1 Performance evaluation of the Intelligent IDS

As previously mentioned, we propose the application of an intelligent IDS in the IoT-cloud environment. Then, we aim to evaluate our proposal by the application of a set of classifiers on a real dataset [32] for intrusion detection.

To measure the performance of our intelligent system, we adopt the following steps.

Following the collection of managed data, data preparation occurs. The data is cleaned and formatted for the next stage of the information process in this step, which is frequently referred to as "pre-processing." The purpose of this preparation is to eliminate low-quality data that may be missing, redundant, or wrong, and to begin creating data that will assure the high quality of the intelligent model chosen. In fact, the raw dataset is meticulously scrutinized for errors of any type. We turn the input data into a vectorizable matrix in this stage. The classifier then determines whether or not there is an attack in the network traffic. As a result, we use the intelligent IDS to select the best classifier by combining a number of them.

Researchers in the security domain have employed a variety of datasets to train and evaluate their systems' performance. The NSL-KDD dataset [32] is the most often utilized. The data was heavily processed in order to eliminate duplication and/or missing records. The traffic distribution of the NSL-KDD dataset is shown in Table 1 [2]. The NSL-KDD dataset is derived from the KDDCUP'99 dataset, which itself is derived from data collected during the DARPA'98 IDS evaluation program [33]. The KDDCUP'99 training dataset contains roughly 4,900,000 single connection vectors, each of which contains 41 features and is categorized as normal or an attack, with each attack type being unique. The various attack types are classified as probing (Probe), Remote to Local (R2L), Denial of Service (DoS), and User to Root (U2R).

The learned features have been used to the labeled test dataset to identify it as an attack or regular traffic.

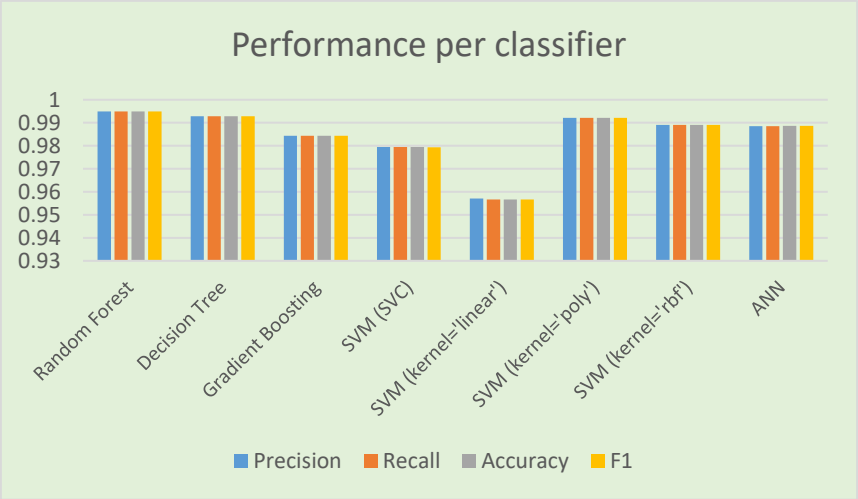
Table 1: Traffic Distribution of the NSL-KDD

Traffic	**Training**	**Test**
Normal	67343	9711
Dos	45927	7458
Probe	11656	2754
R2L	995	2421
U2R	52	200
Total Attack	58630	12833
Total Traffic	125973	22544

To evaluate the intelligent IDS, we use a number of machine/deep learning classifiers in the context of intrusion detection, using the NSL-KDD dataset to choose the best model. Numerous metrics can be used in this test, such as accuracy (Ac), recall, detection rate (DR), positive predictive value (PP), and negative predictive value (NP). These factors are evaluated with the help of true positive (TP), true negative (TN), false positive (FP), and false negative (FN). However, we will essentially rely on two main metrics: accuracy and the F-measure which represents the harmonic mean of recall and precision [34].

Table 2 summarizes the evaluation measures and shows that the Random Forest (RF) classifier outperforms standard models in terms of accuracy. In reality, the value of accuracy has been estimated to be 99.49 percent (Figure 3).

Figure 3: Performance per classifier



The results of the experiments reveal that the implemented intrusion detection system performs well in detecting attacks in IoT-cloud scenarios. A number of categorization metrics are used to evaluate our suggested method. It has been demonstrated that our scheme's attack detection rates increase to more than 99 percent when the RF classifier is used. In addition, Table 2 compares the RF's overall statistical evaluation values to those of other classifiers such as [35]: Decision tree, SVM (different kernels), Gradient Boosting and ANN. The collected findings reveal that, in terms of precision, recall, and F1 score, the RF outperforms the others. Therefore, the RF has the highest attack detection rates. Please note that used metrics are defined as follows:

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN)$$

$$\text{Recall} = TP / (TP + FN)$$

$$\text{Precision} = TP / (TP + FP)$$

$$F1 = (2 * \text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision})$$

Table 2: Performance metrics

Classifier vs Metric value	TP	FN	FP	TN	Precision	Recall	Accuracy	F1
Random Forest	17635	100	88	19154	0.9949	0.9949	**0.9949**	0.9949
Decision Tree	17624	148	213	19090	0.9928	0.9928	**0.9928**	0.9928
Gradient Boosting	17411	111	152	18991	0.9844	0.9844	**0.9844**	0.9844
SVM (SVC)	17227	508	250	18992	0.9795	0.9795	**0.9795**	0.9794
SVM (kernel='linear')	16629	1106	496	18746	0.9571	0.9566	**0.9566**	0.9566
SVM (kernel='poly')	17613	122	165	19077	0.9922	0.9922	**0.9922**	0.9922
SVM (kernel='rbf')	17529	206	196	19046	0.9891	0.9891	**0.9891**	0.9891
ANN	18853	389	871	16864	0.9662	0.9885	**0.9887**	0.9886

The performance of the RF classifier slightly surpasses the DT classifier and the SVM classifier with the poly kernel. The RF classifier, in fact, is based on building numerous decision trees during the training phase. As a result, in most cases, the RF classifier outperforms the DT classifier, as seen in this instance. Therefore, our intelligent intrusion detection system (IIDS) on the IoT-cloud network will be based on using the model constructed through the RF classifier to monitor the whole network, oversee traffic, and analyze transferred data. When a new assault is discovered and identified by new signatures, the IIDS classifies the traffic as normal or anomalous with an accuracy rate of 99.94%.

4.2 Performance evaluation for dimension reduction

We first discuss the dataset that was used. Following that, to illustrate and analyze our findings, we utilize PCA to extract features from this dataset.

Various approaches for dealing with dimension reduction [36]–[37] in AI have been presented in the literature. In this work, we select the PCA technique to perform on a real-world dataset. PCA was chosen because of its various benefits. For instance, PCA can aid in minimizing data size without losing critical information. Furthermore, it lowers the data dimension by creating additional variables known as main components. The most significant benefit of PCA is that it is considered an unsupervised approach, which means that it does not utilize knowledge about the group when completing dimension reduction tasks.

We conclude that reduction approaches improve energy consumption by removing superfluous data. Only the most critical and meaningful data is then processed.

The dataset [38] utilized is a collection of air pollution measurements. The data was collected using a carbon dioxide sensor. For each sensor, a starting value between 25 and 100 is set. Following that, values are changed in accordance with the following rules:

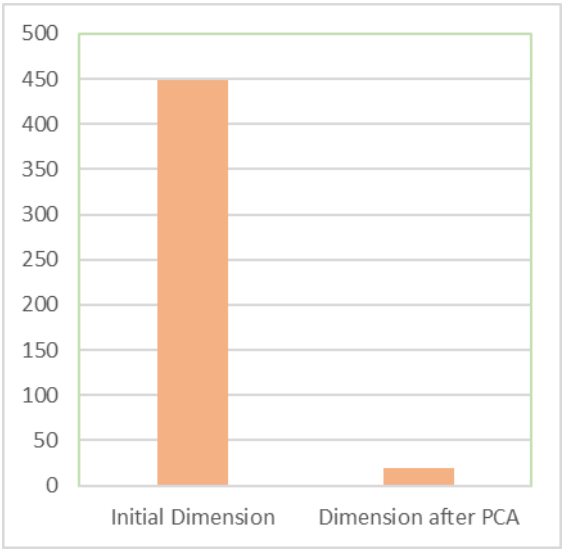
$$value = \begin{cases} value + random\ integer\ in\ [1..10]\ if\ value \leq 20 \\ value + random\ integer\ in\ [1..10]\ if\ value \geq 210 \\ value + random\ integer\ in\ [-5..5]\ elswhere \end{cases}$$

These rules give the stream a realistic behavior by limiting measurement jumps between low and high values.

449 observation sites were used to collect data using the Air Quality Index [39].

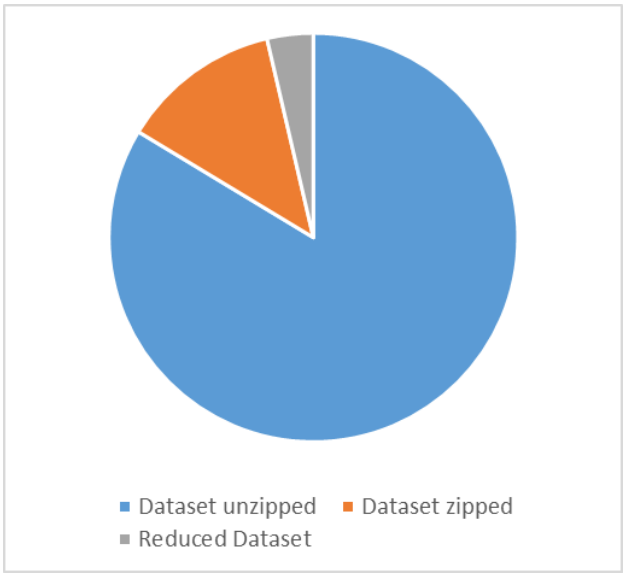
Figure 4 depicts the outcome of using PCA, an artificial intelligence technique, to minimize data size. Before using PCA, there were 449 features; after using PCA, there are just 20. This reduction is empirically acceptable knowing that the total variance explained is 75.69%. The overall amount of decrease is 95.55%, which is a substantial and noteworthy reduction. This reduction will definitely assist in the reduction of resource consumption and allocation in the future.

Figure 4: Dimension reduction using PCA



The size of the dataset is shown in Figure 5. The initial zipped dataset is approximately 80MB, but after unzipping it, it becomes approximately 527MB. Without zipping, the new size of the dataset after PCA is approximately 23MB. As a result, we can deduce that using PCA has a significant influence on data size reduction. Lowering dataset size verifies the prior conclusion of feature minimization.

Figure 5: Dataset sizes



5. Conclusion

The data security and system performance challenges in IoT-cloud are investigated in this study. Many existing approaches with significant complexity in terms of storage

and time cannot be implemented due to the nature of IoT devices as restricted resources. As a result, using lightweight techniques is strongly advised in this situation. Therefore, for data security, we proposed the use of an intelligent intrusion detection system. Then, we compared a variety of classifier approaches as strong learning tools for dealing with IoT IDS. Moreover, we suggested the use of an encryption protocol to further ensure confidentiality, integrity, and non-repudiation services. For energy efficiency, we proposed the application of the dimension reduction technique to reduce energy consumption and optimize the IoT-Cloud systems. This may be accomplished by decreasing the amount of the dataset. We demonstrated that this reduction may be accomplished in two ways using an artificial intelligence tool: feature selection or feature extraction. In fact, PCA considerably decreased the amount of data via experimental investigation. We demonstrated the efficacy of our proposal in terms of intrusion detection and energy performance in an experimental study.

***Funding Statement*:** This work was supported by the Deanship of Scientific Research, Qassim University.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Ben Daoud, A. Meddeb-Makhlouf and F. Zarai, "A model of role-risk based intrusion prevention for cloud environment," *International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 530–535, 2018.

[2] W. Ben Daoud and S. Mahfoudhi, "SIMAD : secure intelligent method for iot-fog environments attacks detection," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2727–2742, 2022.

[3] N. Hu, Z. Tian, H. Lu, X. Du and M. Guizani, "A multiple - kernel clustering based intrusion detection scheme for 5G and IoT networks," *International Journal of Machine Learning and Cybernetics*, vol. 12, pp. 3129–3144, 2021.

[4] W. Ben Daoud, M. S. Obaidat, A. M. Makhlouf, F. Zarai and K. F. Hsiao, "TACRM : trust access control and resource management mechanism in fog computing," *Human-centric Computing and Information Sciences*, vol. 9, no. 28, pp. 1–18, 2019.

[5] S. Mahfoudhi, M. Frehat and T.Moulahi, "Enhancing cloud of things performance by avoiding unnecessary data through artificial intelligence tools," *International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 1463–1467, 2019.

[6] S. Saraswat, H. P. Gupta, T. Dutta and S. K. Das, "Energy efficient data forwarding scheme in fog-based ubiquitous system with deadline constraints,"

IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 213–226, 2020.

[7] Q. Duy, M. V Ngo, T. Quang, T. Q. S. Quek and H. Shin, "Enabling intelligence in fog computing to achieve energy and latency reduction," *Digital Communications and Networks*, vol. 5, no. 1, pp. 3–9, 2019.

[8] L. Goasduff, "Gartner says 5.8 billion Enterprise and automotive IoT endpoints will be in use in 2020," *https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io*, 2019.

[9] W. Ben Daoud, M. Rekik, A. Meddeb-Makhlouf, F. Zarai and S. Mahfoudhi, "SACP : secure access control protocol," *International Wireless Communications and Mobile Computing (IWCMC)*, pp. 935–941, 2021.

[10] G. Kalnoor, "IoT-based smart environment using intelligent intrusion detection system," *Soft Computing*, vol. 25, no. 17, pp. 11573–11588, 2021.

[11] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of things: A comprehensive investigation," Comput. Netw., vol. 160, pp. 165–191, Sep. 2019, doi: 10.1016/j.comnet.2019.05.014.

[12] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017, doi: 10.1016/j.jnca.2017.02.009.

[13] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions," Electronics, vol. 9, no. 7, Art. no. 7, Jul. 2020, doi: 10.3390/electronics9071177.

[14] V. Sharma, I. You, S. Member and K. Yim, "BRIoT : behavior rule specification-based misbehavior detection for iot-embedded cyber-physical systems," *IEEE Access*, vol. 7, pp. 118556–118580, 2019.

[15] M. Wazid, P. R. Dsouza, A. K. Das, V. Bhat, N. Kumar et al., "RAD-EI : A routing attack detection scheme for edge-based internet of things environment," *International Journal of Communication Systems*, pp. 1–20, 2019.

[16] N. Moustafa, K. R. Choo, I. Radwan and S. Camtepe, "Outlier dirichlet mixture mechanism : adversarial statistical learning for anomaly detection in the fog," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 1975–1987, 2019.

[17] T. Sun and W. Yu, "A formal verification framework for security issues of blockchain smart contracts," *Electronics*, vol. 9, no. 2, pp. 255, 2020.

[18] S. Venkatraman and B. Surendiran, "Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems," *Multimedia Tools and Applications*, vol. 79, pp. 3993–4010, 2020.

[19] N. Hasan, R. N. Toma, A. Nahid, M. M. M. Islam and J. Kim, "Electricity theft detection in smart grid systems : A CNN-LSTM based approach," *Energies,* vol. 12, no. 17, pp. 3310, 2019.

[20] Y. Chen, S. Hao and H. Nazif, "A privacy-aware approach for managing the energy of cloud-based iot resources using an improved optimization algorithm," *IEEE Internet of Things Journal,* pp. 1–12, 2021.

[21] M. Sadrishojaei, N. J. Navimipour, M. Reshadi and M. Hosseinzadeh, "A new preventive routing method based on clustering and location prediction in the mobile internet of things," *IEEE Internet of Things Journal,* vol. 8, no. 13, pp. 10652–10664, 2021.

[22] J. Huang, Y. Hong, Z. Zhao and Y. Yuan, "An energy-efficient multi-hop routing protocol based on grid clustering for wireless sensor networks," *Cluster Computing,* vol. 20, no. 4, pp. 3071–3083, 2017.

[23] M. Bagheri, V. Nurmanova, O. Abedinia, M. S. Naderi, N. Ghadimi et al.,"Renewable energy sources and battery forecasting effects in smart power system performance," *Energies,* vol. 12. no. 3, pp. 373, 2019.

[24] E. Parvizi and M. Hossein, "Utilization-aware energy-efficient virtual machine placement in cloud networks using NSGA-III meta-heuristic approach," *Cluster Computing,* vol. 23, no. 4, pp. 2945–2967, 2020.

[25] X. Xu, Q. Liu, Y. Luo, K. Peng, X. Zhang et al., "A computation offloading method over big data for IoT-enabled cloud-edge computing," *Future Generation Computer Systems,* vol. 95, pp. 522-533, 2019.

[26] F. Ruan, R. Gu, T. Huang and S. Xue, "Open access a big data placement method using NSGA-III in meteorological cloud platform," *EURASIP Journal on Wireless Communications and Networking,* no. 143, 2019.

[27] S. Omer, S. Azizi, M. Shojafar and R. Tafazolli, "A priority, power and traffic-aware virtual machine placement of IoT applications in cloud data centers," *Journal of Systems Architecture,* vol. 115, 2021.

[28] M. Ghahramani, R. Javidan, M. Shojafar, R. Taheri, M. Alazab et al., "RSS : an energy-efficient approach for securing IoT service protocols against the DoS attack," *IEEE Internet of Things Journal,* vol. 8, no. 5, pp. 3619–3635, 2021.

[29] Y. Liang, Z. Hu and K. Li, "Power consumption model based on feature selection and deep learning in cloud computing scenarios," *IET Communications,* vol. 14, no. 10, pp. 1610 – 1618, 2020.

[30] W. Lin, Y. Zhang, W. Wu, S. Fong and L. He, "An adaptive workload - aware power consumption measuring method for servers in cloud data centers," *Computing,* 2020.

[31] M. Hussain, L. Wei, A. Lakhan, S. Wali and S. Ali et al.,"Energy and performance-efficient task scheduling in heterogeneous virtualized cloud computing," *Sustainable Computing: Informatics and Systems,* vol. 30, pp.

100517, 2021.

[32] Dataset: https://www.unb.ca/cic/datasets/nsl.html

[33] "KDD CUP 99 [online] available:," http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 1999.

[34] D. M. Powers, Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness and Correlation, 2011.

[35] J. Rahman, H. S. Suri and M. Abedin, "Accurate diabetes risk stratification using machine learning : role of missing value and outliers," *Journal of Medical Systems*, vol. 42, no. 92, pp. 1–17, 2018.

[36] R. Gupta and A. Saxena, "Nonlinear dimension reduction : edge computing data analytics in IoT networks," *International Conference on Intelligent Technologies & Science*, 2021.

[37] J. Carreras, Y. Y. Kikuti, M. Miyaoka, S. Hiraiwa, S. Tomita et al., "A combination of multilayer perceptron , radial basis function artificial neural networks and machine learning image segmentation for the dimension reduction and the prognosis assessment of diffuse large b-cell lymphoma," *AI*, vol. 2, no. 1, pp. 106–134, 2021.

[38] Dataset: http://iot.ee.surrey.ac.uk:8080/datasets.html#pollution

[39] B. Pardamean, R. Rahutomo, T. W. Cenggoro, A. Budiarto and A.S. Perbangsa, "The impact of large-scale social restriction phases on the air quality index in Jakarta," *Atmosphere*, vol. 12, no. 7, pp. 922, 2021.