Data Security Model Using Deep Learning and Edge Computing for Internet of Things (IoT) in Smart City

by

Md. Yasin Aziz
17201019
Tanjid Alam Kabbo
17301149
Tasnuva Tahsin
17101432
Nadia Haque Zumme
17301008
Mohammad Sadman Tahsin
17301127

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
BRAC University
September, 2021

© 2021. BRAC University
All rights reserved.
Declaration

It is hereby declared that,

1. The thesis submitted is my/our own original work while completing degree at Brac University.

2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.

3. The thesis does not contain material which has been accepted or submitted for any other degree or diploma at a university or other institution.

4. We have acknowledged all main sources of help.

Student’s Full Name & Signature:

Md. Yasin Aziz
17201019

Tanjid Alam Kabbo
17301149

Tasnuva Tahsin
17101432

Nadia Haque Zumme
17301008

Mohammad Sadman Tahsin
17301127
Approval

The thesis/project titled “Data Security Model Using Deep Learning and Edge Computing for Internet of Things (IoT) in Smart City” submitted by

1. Md. Yasin Aziz (17201019)
2. Tanjid Alam Kabbo (17201019)
3. Tasnuva Tahsin (17101432)
4. Nadia Haque Zumme (17301008)
5. Mohammad Sadman Tahsin (17301127)

Of Summer, 2021 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on September 26, 2021.

Examining Committee:

Supervisor:  
(Member)

Dr. Muhammad Iqbal Hossain  
Assistant Professor  
Department of Computer Science and Engineering  
BRAC University

Program Coordinator:  
(Member)

Dr. Md. Golam Rabiul Alam  
Associate Professor  
Department of Computer Science and Engineering  
BRAC University

Head of Department:  
(Chair)

Sadia Hamid Kazi  
Chairperson  
Department of Computer Science and Engineering  
BRAC University
Abstract

In the current ongoing world of the IoT (Internet of Things) devices, it is absolutely vital to have a safe, secure and reliable cyberspace. A cyberspace or network where it is free from all sorts of unethical activities like hacked systems, data breaches and stolen data. For that, goal to be accomplished we need to have a modern, strong and rigid cybersecurity system so that the information and data stays safe from threats and attacks. Our conducted research includes recent IoT data security issues and a robust security model which ensures the data security of the IoT devices based on a smart city’s perspective. According to the recent research data on the vulnerable IoT devices we propose an intelligent and effective security approach to tackle the modern IoT security issues because our data needs to be protected as the IoT devices or “things” as we call it needs to have proper security. A few areas of future research indicate the use of blockchain to resolve the cybersecurity issues of the IoT devices are the most promising and interesting.

Keywords: IoT, CNN, LSTM, Edge Computer, Smart City, Malware, Internet, Security, IoT device.
Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.
Secondly, to our supervisor Dr. Muhammad Iqbal Hossain sir for his kind support and advice in our work. He helped us whenever we needed help.
And finally, to our parents without their throughout support it may not be possible. With their kind support and prayer we are now on the verge of our graduation.
# Table of Contents

Declaration ................................................................. i
Approval ................................................................. ii
Abstract ............................................................... iii
Acknowledgment ......................................................... iv
Table of Contents ......................................................... v
List of Figures ............................................................. 1

1 Introduction .................................................................. 2
   1.1 Research Problem ................................................. 2
   1.2 Research Objectives .............................................. 3
   1.3 Purpose of Research .............................................. 4

2 Literature Review ....................................................... 6
   2.1 Internet of Things (IoT) ........................................... 6
      2.1.1 IoT Architecture ............................................ 7
   2.2 EDGE Computing ................................................ 8
   2.3 Related Works .................................................... 9

3 Methodology ............................................................... 13
   3.1 EDGE Model and Description ................................. 14
   3.2 Security Requirements .......................................... 15
   3.3 Protocol Stacking ............................................... 16

4 Data ........................................................................... 18
   4.1 Data set Summary and Description ......................... 18
   4.2 Data Pre-Processing ............................................. 18
   4.3 Data splitting and Clustering ................................. 19

5 Implementation & Results .............................................. 20
   5.1 Preparing the model ................................................ 21
   5.2 Results and Accuracy ............................................ 22

6 Conclusion ................................................................ 24

Bibliography ................................................................ 27
List of Figures

2.1 The Visual Representation of the uses of IoT Devices .................. 6
2.2 Hybrid CNN+LSTM Deep Learning Model Architecture ............... 10
2.3 Hybrid CNN+LSTM Deep Learning Model Performance ................. 12

3.1 The flow chart of the proposed DL and Edge model ....................... 13
3.2 The flow chart of the proposed edge computing model (SIEM) ............ 15
3.3 Protocol stack flow of our model ........................................ 17

4.1 Preview of the data set before processing ............................... 18
4.2 Preview of the data set after processing ................................ 19
4.3 Preparation of our input data ............................................. 19

5.1 Flow diagram of a CNN+LSTM DL model ............................... 20
5.2 Architecture of a CNN+LSTM DL model ................................ 21
5.3 Deep Learning model preparation of our proposed CNN+LSTM hybrid model .................................................. 22
5.4 Testing accuracy using our proposed CNN+LSTM hybrid model ... 22
5.5 Plotting the accuracy using our proposed CNN+LSTM hybrid model 23
Chapter 1

Introduction

Internet of Things is a concept with a composition of multiple technological devices or objects which have their own specific purposes. From automation, to providing security, to providing us with information, to making our life easy and better; they do them all. These smart devices all have their respective hardware compartments and software codes as well.

As we advance more towards the future, the Internet of Things is revolutionizing our lifestyle. For example: a smart IoT based robot can clean our house, a smart bulb can turn on or off based on the presence of someone in the room, a smart door can use its sensor to open itself or not, a smart speaker which has an artificially intelligent assistant built-in can talk and interact with us. These are all the objects of the Internet of Things spectrum.

In contrast, they all share a common surface and that is, they have to interact with the internet which involves sharing of valuable information which we know as data. And these can be easily manipulated and stolen. In our instance, a smart city; where people are constantly relying on these Internet of Things devices, they can’t be vulnerable to their personal data. So, a strong, secure and smart security approach is imminent.

IoT devices are different in their own ways, shapes and forms. These devices are interconnected using the internet and diverse types of communication technologies. At present, IoT devices are extensively exploited depending on the existing qualities for several functions for example: smart city, smart home, smart grid, smart traffic system, ad hoc networks of vehicles and power systems that are autonomous. Multiple associations of IoT (IPSO, AllJoyn, OMA, IEEE P2413 etc.) have offered their own quality IoT frameworks among the various developed levels that are out there. Therefore, these lead to the urge of comprehensive security protection and a new security model is eminent which can solve the modern data security vulnerabilities.

1.1 Research Problem

In order to achieve a convincing security measure for our data, we will be using Deep Learning and Edge Computing on our proposed model and framework. In contrast, IoT devices are easy to hack and compromise due to limits than other endpoint powerful devices like the pc and mobiles. So, our primary target is to ensure a solid security environment where we can provide security to the user’s data on their IoT devices. Our main concern is a smart city; where countless IoT devices are being
used constantly. Data security is an absolute must. From a smart assistant at home, to the IoT based surveillance camera, to sensor-based devices like the smart door, bulb, fridge, furthermore, the smart traffic system in the smart city. In all instances in our smart city, we need to provide data security to the users and authorities. We’ll introduce a model of deep learning. In such sectors like healthcare, image processing, speech identification etc., deep learning approaches have been used, which have provided better results compared to other methods of machine learning. In [35], for fog computing, a deep learning approach is presented for the observation of allocated attacks. Deep learning is a wider machine learning sub field, a largely substantial deep neural network which can be used for operated, unmonitored and semi-operated learning. In [11], the deep learning system framework was first introduced. The goal of this paper was to present a new method of deep learning to provide our smart city data with compact cyber security.

In addition, the subsequent domains can split IoT executions: The Internet of Controllers/Sensors, the Internet of Transport, the Internet of Electricity, and communications from system to device/machine to machine. In this case, to provide a good cryptographic solution for our IoT security, we thought of demonstrating some awareness of the current security challenges. Cross-application key management is complicated because for specific security purposes, one and all functions can manage its security keys [8]. In our smart city, when consumers use many IoT based applications, it raises the threat of key manifestation and threatens the protection of services. On resource-strained IoT devices, such as group signatures (GS), modern cryptographic algorithms require to be operated [8][1] for anonymous transmissions and attribute-based encryption (ABE) for approaching to control data. This will be a reason for the IoT application to fail in real time because it is not possible to complete the computation of the advanced algorithms in a pre-defined duration. Furthermore, standard protocols, software, hardware all are significant factors for processing encrypted keys for providing data security as we know not all IoT devices have the same computing power. Therefore, we absolutely need to reconfigure our security system with Edge Computing. Edge computing is a new type of computing model [9], where a near-user computer with a higher computing power supplies the requisite resources for other resource-limited IoT device applications. Found on Edge Computing, our new model will alleviate the challenges of immense computing costs, limited flexibility, and incompatibility in promoting security with modern cryptography.

1.2 Research Objectives

This research aims to develop a standard of the IoT devices in the smart city where the data of the users and devices stay secure and safe. By following our formidable model, securing data security as we know shall have a broader perspective. The objectives of this research are:

1. To deeply understand IoT and how it works.
2. To understand different sorts of deep learning methods.
3. To develop a model for securing the data of the IoT devices in a smart city.
4. To evaluate the model.

5. To understand how Deep Learning and Edge Computing contributes to providing security.

6. To offer recommendations on improving the model.

1.3 Purpose of Research

Data security processes are assigned to minimize data breaches, to mitigate the high risk of data leakage, and to ensure regulatory compliance. Data security’s purpose inside any organization is to ensure the sustained safe and secure usage of private data while reducing exposure risk. Over the years, lack of security caused data breaches in numerous areas.

The goal of this paper is to provide a thorough overview of the present state of the art at the convergence of deep learning and edge computing. It will also cover open issues such as system performance, network technology and management, benchmarking, and privacy. According to [25], this will examine several methodologies for promptly producing deep learning inference across a combination of user devices, edge servers, and the cloud, as well as provide methods to train models of deep learning across numerous edge devices.

In 2016, North Korean hackers attempted a 1 billion dollars attack on the central bank of Bangladesh. The transactions were stopped by only one fluke, all except $81 million in 2015. Bangladesh Bank is the country’s central bank, in charge of the country’s valuable currency reserves. It all began with a malfunctioning printer. The printer was important. It was kept on the tenth floor of the bank’s main headquarters in Dhaka, the capital, in a very secure chamber. It’s function was to print out records of the bank’s multi million-dollar transactions in and out. When employees discovered it wasn’t functioning, they assumed it was a previous issue. Hackers had gained access to it’s computer networks and were carrying out the most sophisticated cyber-attack ever undertaken at the time. To steal the money, the heist team would use fake bank accounts, charities, casinos, and a vast network of collaborators.

In October 2016, on the U.S. east coast, an onerous distributed denial of service (DDoS) attack remained much of the internet unreachable. The Mirai Botnet, which initially had fewer grand ambitions, grew more powerful than it’s creators ever dreamed possible. This attack was originally intended to make money off of Mine craft fans’ hard-to-crack investment in the game. An IoT botnet is a network of internet-connected devices, usually routers, that have been infected with malware and taken over by malicious actors. Mirai’s first big wave of attacks launched on September 19, 2016, was targeted against OVH, which was at the aggravated assault as the host for the popular anti-DDoS tool that Minecraft server hosts utilized. Furthermore, Mirai was also posted a few days later, which provided malware authors with plausible deniability since they knew that other malware copycats would utilize the code, and so the waters would be muddled to who exactly invented it.

Dyn is indeed a business that provides DNS services to many popular sites, and on October 12, they came under assault from an external source, who used a major vulnerability in their infrastructure to unleash an enormous - scale shared denial of service (DDoS) attack. According to the FBI, this incident was an attempt to
target Microsoft’s 4 gaming servers.

A vulnerability in the Trendnet security cameras has the potential to expose thousands of consumers to unauthorized access. A blogger who goes by “someLuser” exposed the problem in January, explaining how he was proficient to locate unprotected cameras online by using the Shodan search engine, which permits users to discover the devices which are connected to internet operating basic search terms. Even with a password, users may set up cameras with an IP address, and anybody who knows the camera’s net address can watch the video stream from the address regardless of whether the stream is password protected. He was skillful to finding 350 vulnerable Trendnet cameras in this manner. After his unveiling, internet users had discovered more than 600 web addresses with webcams, which were discovered in business offices and inside children’s bedrooms. Over time, many cameras that were uncovered were coupled with pictures from those cameras as well as photos from Google Maps identifying the required details of those cameras.

A study team was expert to gain complete control of a Jeep SUV by exploiting the vehicle’s CAN system. They gained control of the car through the Sprint cellular network by exploiting a software update vulnerability and found they could cause it to accelerate, decelerate, and even swerve off the road. It serves as an evidence of hypothesis for newly discovered Internet of Things hacks, while companies often overlook the security of peripheral appliances or networks, the results may be catastrophic.

Cybersecurity experts declared 2015 “The year of the health care hack” in February, and they were correct. The breach of more than 11 million data at Premera Blue Cross started in January. Along with particular informations such as, mail addresses, bank account information and Social Security numbers, attackers targeted sensitive insurance claims data. Further investigation by the firm revealed that the first breach occurred in May 2014, providing enough time for attackers to scan the system for valuable data.

To conclude, considering how vulnerable IoT devices are which we shall get to, in a moment a secure and sustainable way to provide the security to these devices were the primary key purpose of this research.
Chapter 2

Literature Review

2.1 Internet of Things (IoT)

In recent days, one of the most trending and enjoyed technologies is the Internet of Things (IoT). Basically, IoT describes the network between some hardware which consist of various sensors, software and other technologies. These devices mainly read from the embedded sensors and other mechanisms, then transfer it to another device or cloud storage. Usually, these devices are mainly connected to a smartphone or a computer from which the user can see the data and also can control the devices if needed. In present days, it has been greatly used in smart homes, hospitals, offices, industries etc. As a result, preserving the security of IoT has become an important issue.

![Figure 2.1: The Visual Representation of the uses of IoT Devices](image)

The Internet of Things (IoT) is a special addressing network system with various degrees of perception, process and keep in motion potentialities which share the
potentiality to interwork and communicate through the web and can be narrated as the contact network, connects particulars to data as their joint manifesto [4]. Though, the foremost aim of the Internet of Things is to make it feasible for nodes to be joined with the other nodes, particulars, using any kind of network, service or path at anywhere and any time. Today’s internet evolution, IoT is being considered as the succeeding period. It has been said that, in 2020, more than 50 billion devices have internet connection [9]. But approximately 0.6% devices which can be the part of IoT has been associated so far [14]. With the advancement of the Internet, it has become more than just a computer network, it is now a network of multiple devices, whereas IoT, as a network of numerous “connected” devices, provides a network of networks [20] as shown in Figure 2.1. Currently, technological devices like smartphones, automobiles, technical systems, buildings, cameras, house applications and countless others can all share information through the internet. Nevertheless, their size and performances, devices can fulfill real-time monitoring, keep track on controlling, smart restructuring, tracking and many more. However, the most remarkable trading consequence has been distinguished in the purchaser electronics fields. As an example, the revolution of smartphones and absorption for wearing wearable devices like (smartwatch, wireless headphone etc.), the biggest movement for the people towards the digital and physical worlds.

According to [31], the functions of IoT covered a wide area such as smart cities, securities, health care, agriculture and emergencies among many others. Some other IoT functions creating smart cities include smart building [17], smart lighting, smart parking, waste management, traffic obstruction, intelligent transportation systems and rural maps [19][22]. This may cover unlike features such as; monitoring accessible parking, sensitive parts of the cities as well as monitoring any vehicle conditions.

2.1.1 IoT Architecture

Basically, IoT architecture is the scheme of legionary elements such as: protocols, sensors, actuators, cloud services, and layers. The base layer device architecture consists of IoT devices that include all components, such as sensors with the ability to detect, calculate, and connect to other devices. In the second layer, the IoT Aggregation Layer, which significantly aggregates information from various sensors, these two layers form the definition machine and determine the rules for data aggregation. The next layer is cloud-based; it is known as the Processing Engine or the Event Processing Layer. It has multiple algorithms and data processing components that are finally shown on a dashboard. This layer essentially processes the data received from the sensor layer. The last layer is known as the Application Layer or API Management Layer. It behaves like an interface between the devices and the third-party infrastructure, the entire scheme supported by the users of the device, and looks for administrators who are useful for the security of the IoT reference architecture and access them.

To establish a safe IoT implementation, several security standards need to be enforced at each tier. The future of the IoT framework is contingent upon addressing and resolving the security concerns connected with it. Numerous researchers have tried to decrease the security risks related to IoT layers and devices by developing
appropriate remedies. This article discusses security fundamentals, technical and security problems, suggested treatments, and prospects for IoT security [3]. The author of this paper [15], began by discussing the fundamental security needs for securing an IoT environment. Additionally, they discussed the threat model and various attacks that could occur in an IoT environment. Then, they proposed a taxonomy of safety protocols for the IoT environment, including critical security measures such as user and device authentication, access control, key management, identity management, and data protection. Additionally, the author compared newly suggested state-of-the-art IoT related security protocols regarding the additional security and functionality aspects they offer. Finally, they highlighted some of the potential difficulties facing IoT security standards.

The evolution and importance of IoT in regular life, the communal architecture, vast used protocols, and the tremendous possible applications, security and privacy concerns connected to IoT, practical implementation of IoT schemes using tools like Arduino and upcoming propensity. The Internet of Things is likely to become one of the most popular networking ideas since it can provide many advantages. Internet of Things (IoT) needs technological adoption patterns, and recommends a reference design for e-commerce enterprises [2][5].

In this article [26], the author analyzes the security concerns and possible sources of risk connected with IoT applications in detail. After discussing security concerns, several new and established solutions are explored to establish a higher level of trust in IoT applications. Four different technologies are analyzed to improve the degree of security in IoT: block chain, fog computing, edge computing, and machine learning.

### 2.2 EDGE Computing

Edge computing is known as an open and distributed IT architecture including a decentralized power system, qualified mobile computers, and technologies for the Internet of Things (IoT). By including edge computing, the device can process data on its own or use a nearby computer or server instead of being transmitted to a knowledge center. Edge computing enables efficient processing in the sense that large amounts of information are processed close to the source, reducing the use of Internet bandwidth. This saves costs and ensures that applications in remote locations are used efficiently. Additionally, the flexibility to process data without having to put it in a public cloud provides a useful layer of security for exquisite data. With edge computing, individual distributed nodes can transmit data where nodes are connected via the web and therefore require specialized encryption techniques, which are independent of the cloud. Edge nodes can also be devices with limited resources with limiting options in the sector of security procedures.

On the other side, when storing and processing data, expanding privacy is possible by minimizing the transfer of impresssible information to the cloud. Due to the proximity of analytical resources to users who write, delicate analysis tools and calculation tools can be run on the system. This location on the stinger helps to increase efficiency to operate and many other benefits of the system. Avoiding transmission over the network leads to considerable bandwidth savings and thus increases efficiency. Edge application actions mitigates the amount of knowledge to transfer, the resulting data traffic, and also the distance travelled by that data.
leading to lower latency times and lower transfer charges. Computer offloading for real-time implementations, such as identity verification algorithms, resulted in significant improvements in response times, as shown in early research. Subsequent research showed that, the use of resource-rich machines called Cloudlets close to mobile users providing services normally found in the cloud resulted in improved execution time when a number of tasks were outsourced to sting nodes. On the other hand, outsourcing any task can cause a slowdown due to the transmission times between the device and the node, so an optimal configuration can be demarcated taking into account the workload.

Another application of Edge Computing is cloud gaming, where important prospects of a game can be played in the cloud and then the rendered video is streamed to clients running on devices such as cell phones, virtual reality glasses, etc. This type of transmission is also known as pixel transmission. Other prominent applications are connected cars, autonomous cars, smart cities, smart industry, and automation systems for residential buildings.

2.3 Related Works

Previously, we have seen many Machine learning and AI approaches towards the fields of IoT. For an example, in [6], to identify abnormalities in an IoT system, they suggested using machine learning including an IOT gateway. We were able to train the network to recognize erroneous data points and then retrain it to detect legitimate data points using artificial neural networks (ANN) and genetic algorithms. Artificial neural networks (ANN) are basically computer programs that imitate the brain’s neurons and synapses to convey data for connection, acquaintance, and decision-making. In IoT systems, ANNs are used to monitor the condition of connected devices and make educated perceptions about how to best use them. But we want a deep-learning approach that includes Edge computing, that can secure the IoT devices in a smart city.

According to [30], they showed a dependable method for enhancing security in edge computing based on AI. The combination of mobile edge computing with AI opens up endless possibilities in everyone’s daily life, thanks to the prosperity of artificial intelligence (AI) applications. A security-enhanced trace back (SET) system is proposed to increase the security of wireless networks. In order to save energy, nodes further away from the sink adopt a greater marking probability while nodes closer to it adopt a lower marking probability. To compensate for the storage space of the nodes, the probability of marking the data packets is stored in the nodes and transmitted to the nodes far from the sink.

This paper offers an intelligent architecture that combines Complex Event Processing (CEP) and Machine Learning (ML) techniques to identify various IoT security threats in real-time. Such an architecture, in particular, is capable of efficiently handling event patterns whose criteria are determined by machine learning algorithms. Additionally, a model-driven graphical tool for defining security attack patterns and automating code creation is given, abstracting away from domain experts all the complexity resulting from implementation specifics. The proposed architecture was validated against a hospital IoT network to demonstrate its capacity to identify assaults initiated by rogue devices. The collected findings show that this design meets its goals adequately. IoT architecture is addressed in this survey study, along with
the significance of IoT security in terms of many kinds of potential threats, after a thorough literature analysis on machine learning methods. Additionally, machine learning-based possible solutions for IoT security have been highlighted, as well as future difficulties [32][34].

Here, we used a new CNN+LSTM deep learning model. It’s basically a hybrid model where both CNN and LSTM is implemented. Figure 2.1 illustrates the architecture of this proposed model. This model includes the first 1-d CNN layer pursuing a relu-activation feature, and then an Adam-activation LSTM layer. The remaining parameters are similar to those used in the CNN and LSTM models [9].

Figure 2.2: Hybrid CNN+LSTM Deep Learning Model Architecture

This Paper [29] is based on the comparison between Machine Learning and Deep Learning regarding cyber security when the main focus is DDoS attacks. It is seen that, the main problem in cyber security is these DDoS attacks where the system crashes for a while, also the users cannot access the system. Keeping this as the major issue, IDS is an effective technique to detect cyber-attack. Keeping the attacks in mind they have introduced models like CNN, LSTM and hybrid CNN+LSTM. Here one model is designed with Autoencoder combined with SVM for malware detection in the network (both for binary and multiclass classification). Another model – Bidirectional Long Short-Term Memory based Recurrent Neural Network (BLSTM-RNN). The main focus is mirai, udp, dns and ack attack vector.

In this paper [23], they talked about various issues on secrecy related to the compilation, dispatch, and data storage in the Cloud. Additional security measures have been implemented to strengthen security and privacy protection. In this project, MAC addresses had to be collected because MAC addresses can be very sensitive instead of collecting MAC addresses to use a hash function that generates a hash value according to the MAC address and instead maintains that value. A hash function takes any message size as input and generates a fixed message digest, the so-called hash value. This property assures that the stored Hash value of MAC addresses does not compromise user privacy.

In this era, IOT devices are being used all over the world and the number is increasing to another level. It also raises the probability of attackers to hack into the IOT devices. These days IOT devices are connected through a FOG network instead of cloud. FOG computing is faster and reduces energy consumption and storage. Here, it consists of 3 layers which includes an Application layer, FOG layer and IoT sensor layer and FOG layer is the most important component of the smart city architecture. In this paper, the author proposed the AD-IOT system which relies
on machine learning which can unroll threats with reducing the false positive rate [7]. For intrusion detection they have considered both Host Based IDS and Network Based IDS. Furthermore, the host based IDS only detects any suspicious activities on the host computer connected to the network. This method is not suitable for IoT devices as it requires more computational power. On the other hand, the NIDS methods are more significant for IoT devices though it has a high false positive rate. AD-IoT method significantly reduces the false alert rate by using anomaly based machine learning methods. This AD-IoT system has 3 major components:

- IoT Devices
- Gateway and
- AD-IoT security Gateway IDS System.

Using NIDS and utilizing it with Machine learning algorithms this can analyze statistics to predict and identify cyber-attacks with less False Positive rate [24]. Kalra and Sood [18], came up with an authentication design representing elliptic curve cryptography (ECC) which serves IoT and cloud servers and exclaimed that, it gratifies all security needs and is unassailable to a wide variety of threats. This scheme is vincible to offline password rates and insider attacks and has yet to come close to device anonymity, agreements of session key, and mutual authentication. According to the document, the embedded device must be configured with the TCP / IP protocol stack. HTTP is basically a request-response protocol in the client / server communication model. A novel IT paradigm where Cloud and IoT, two fulfilling system fused together as CloudIoT, is expected to bring about an unprecedented increase in current and upcoming Internet as CloudIoT solves most impedance providing additional facilities like ease-of-access, ease-of-use, and decreased deployment costs. Before accessing cloud services, attached devices like HTTP client and HTTP-enabled cloud server like HTTP server should be authenticated mutually. For efficient usage of power and memory, it is more likely to be suitable to use ECC (Elliptic Curve Cryptography), one kind of public key cryptography [18].

In contrast, in the paper [29], it was shown that, we can achieve higher accuracy using the CNN+LSTM model in our pursuit of providing security on our IoT based network than the other conventional machine learning and deep learning model we have. Because, according to the structures of the models (CNN LSTM), Deep feature extraction is made possible with CNN and with the extracted features, detections are done with LSTM in the process. However, a strong rigid framework or model is also required since we are trying to achieve the utmost security we can provide to our IoT network.

Furthermore, in [28], the authors proposed a security model based on the edge computing framework, to secure the IoT network space from malicious attacks. However, since modern problems require modern solutions, we need to have a Machine or Deep learning model as well with our Edge Computing network, to secure a convincing, rigid and trustworthy security solution. That is where our “SIEM” model comes in. It not only consists of a hybrid Deep learning model which, according to [29], has a better accuracy than the standard MLP, LSTM, CNN models but also the framework is based on the edge computing model as well.
Again, this paper [33], intends to provide an overview of overall existing IoT security composition at the edge layer. It also provides inspiration for further edge-based IoT security concepts. It begins by presenting an IoT architecture that is centered on the edge. Then it focuses into security architectural designs, firewalls, intrusion finding systems, authentication and authorisation protocols, and secrecy-preserving procedures in depth for edge-based IoT security investigation.

Basically, our model is a combination of the hybrid Deep Learning model and the Edge Computing model. In the nutshell, we expect to not only get a solid trustworthy accuracy in terms of predictions of attacks on our IoT network but also maintain a sustainable, efficient and stable key encryption as well to provide the highest level of security on our network.

Figure 2.3: Hybrid CNN+LSTM Deep Learning Model Performance
Chapter 3
Methodology

The proposed model follows below:

Figure 3.1: The flow chart of the proposed DL and Edge model
We shall handle the data of the IoT devices using these steps as mentioned in the model [16]. It consists of several major stages:

1. Input data will be preprocessed. Then the hybrid deep learning model shall be applied for predictions. If our deep learning prediction gives us the green signal of moving forward (i.e., no attack / threats were found) then we shall move forward to our Edge computing process.

2. Then our protocol stacking framework will manage the data and manage keys for authentication of the data.

3. Thereafter, the data shall be sent to undergo the Edge Computing process. As we know, Edge Computing is a computing model where the higher-powered devices which are near to our target device (i.e., the IoT devices) do the computing job of key management of encryption so that our data stays safe.

4. Now it is possible to simplify key management from the implementation level to the user level. Since, we now have a stronger computational capability from the edge devices like the AAA-key management system, and the Global key management system, our low powered low-end devices like most IoT devices will also stay secured.

5. As we can compute higher computational processes for all of our devices regardless of what power the devices come in, we can now use our deep learning model to detect possible attacks and also have the power to manage and compute keys for encryption of the IoT devices as well.

6. If we compare this solution to the current cloud-based solutions that are out there, then we’ll see a significant improvement not only in security measures but also in time for fully processing our data for the IoT devices.

### 3.1 EDGE Model and Description

As we know, in edge computing, higher powered computers are needed for computing to provide better security, not only for the higher-powered devices but also for the lowered powered devices like our IoT devices. Our proposed model is a security framework which will provide the security solutions to our IoT devices. We will utilize high-performance IoT application servers in our edge computing architecture, which will be required for deep learning. This server will also be used for key management for performing end-to-end data encryption. Furthermore, we will have key management systems and AAA key management systems as well for the management of the keys to improve performance in an overall spectrum as dedicated key management servers are key for a rigid edge computing system’s architecture. Further security requirements procedures will be explained below:

The following is the basic architecture of our proposed Edge computing model.
3.2 Security Requirements

Owing to the reality that, IoT has become an essential component and complements the future of the internet with its enlarged consumption, it is needed to sufficiently address security and assurance purposes [27]. Though IoT is built on wireless sensor networks (WSNs), it assumes the security features that WSNs have architecturally [10][12]. Attacks and vulnerabilities in Internet of Things (IoT) systems demonstrate the need for comprehensive security setup. Numerous attacks substantially exploit weaknesses in particular devices in-spite-of acquiring access into their system and in consequence, making secure devices insecure [13][14].

The first priority of our model is to provide security, confidentiality and integrity. Thus, building the overall framework or model will be challenging. But our proposed framework rises up to the occasion as we will use two agents for detection of malicious devices or data. Embedded in the IoT application server we shall have multiple flag agents (variables in programming convention). For instance, after finishing our deep
learning method to detect anomalies or malware; if we detect any anomalies, we shall stop that data to even enter our IoT domain. However, our prediction will be made more stronger because of the agents (flag variables) that we shall use. Their job is to detect and mark the malicious devices as malicious. For that, we get more accuracy on our prediction to whether the data should enter our IoT domain or not. Authenticity therefore will be verified each time we try to process / pass data to our IoT domain as we have our agents to remember, mark and with the help of deep learning, predict as well as whether it’s safe or not. Therefore, it adds an extra layer to the security measure to our framework. The agents will have the information of the IoT devices in that domain and every time any sort of edge computing starts it shall be able to help. Furthermore, we shall have a re-configurable security function to our model as well. This function will be made available for key management and encryption every time when needed. It will directly interact with the server computers, our AAA and key management systems who are responsible for key management.

3.3 Protocol Stacking

The following figure is the basic flow of our proposed protocol stacking feature (Figure 3.3).

It shows us the protocol stacking flow of our model. After the completion of our deep learning prediction and getting the green light to proceed further in transferring the data from the internet to the IoT device, we first have to go through the process of Protocol Stacking.

As discussed earlier we shall conduct our security measure with our security agents, which will help us in providing a more compelling security measure. If we conduct our explanation from layer to layer wise it will be easier to understand.

Firstly, we get our intended data as now that we know through our deep learning data that it’s not malicious data, then we send our data to the datagram transport layer security panel. From there, it goes to the IoT connectivity protocol phase. A common protocol for example: xmpp or mqtt which are used for the protocol of IoT devices. After following the protocols, the connectivity abstraction layer sends the data to the resource stacking manager. Here, this manager manages and stacks the resources throughout our IoT domain.

Secondly, like we mentioned earlier the manager will send the data to the re-configurable security function. Which will hand the processed data to our security agent. Our security agent based on the validity, integrity of the data will proceed the data from the security layer to the application layer’s resources.

Finally, then from the server side the data will be made available for the edge computing processes and key management and encryption process as well. In an overall nutshell, with the added benefits of having the compute power to run powerful and resource demanding deep learning algorithms for predictions thanks to the powerful local servers like our IoT application security server and being able to complete our edge computing processes and providing end to end encrypted security quickly with the help of the AAA and Key management servers and local router; not only the pressure on low end devices like the IoT devices themselves has reduces drastically and data processing time will decreases rapidly; but also, with the added benefits of deep learning, protocol stacking and edge computing, our entire IoT domain should
have a rigid, safe, confidential and integrity based network security environment and setup.
Chapter 4

Data

4.1 Data set Summary and Description

The data set we used was The BoT-IoT data set. It was made by constructing a realistic network environment in the UNSW Canberra Cyber Center’s Cyber Range Lab. There is a mix of normal and botnet traffic in the environment. The data set has caught pcap files which are 69.3 GB in size, eventually more than 72,000,000 records. The extracted flow traffic is 16.7 GB in size in csv format. DDoS, DoS, OS and Service Scan, Key-logging, and Data Exfiltration attacks are included in the data set, with DDoS and DoS assaults being further categorized based on the protocol utilized. The default full data set comprises 47 columns as well.

Here, “proto” refers to Textual representation of transaction protocols present in network flow. Source and destination address (“addr”) and port (“port”) are self-explanatory. Seq is the Argus sequence number. Stddev is for Standard deviation of aggregated records which is a very important record for making predictions. N_In_Conn connection we used for the inbound and outbound connection per source IP. Srate is the Source-to-destination packets per second. Min Max comprises the min/max duration of the aggregated records. Finally, Attack, category and subcategory describes the attack true or false, the category of the attack (DDoS, DoS etc.) and the subcategory based on tcp, udp.

Figure 4.1: Preview of the data set before processing

It’s 5% of the entire data set. The full raw data set can be downloaded from: [13][14]. All of the feature details that are on the data set also can be retrieved from the URL.

4.2 Data Pre-Processing

In terms of the given (before data), which is too large; we obviously cut it down to make a more valid data set for the preparation phase of our deep learning algorithm. The screenshot given below shows 10 columns which are the best 10 features
described in [28]. So, our input data after processing will look like this.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 3542788 udp 150.100.10.10 8551 150.100.10.10 25 25384 1.003963 100 0 4 2.67519 100 0.45450 4.05161 1.10005 UDP |
| 2042288 tcp 150.100.10.10 7512 150.100.10.10 80 257204 0.789053 38 3.85953 3 3.94927 100 0.25690 4.01250 1.00005 TCP |
| 1497010 tcp 150.100.10.10 27965 150.100.10.10 80 263015 0.986666 100 2.9761 3 3.16424 100 0.24804 3.63905 1.00005 TCP |
| 930876 tcp 150.100.10.10 48719 150.100.10.10 80 99100 1.221605 63 0 4 3.22323 63 0.41645 4.85202 1.00005 TCP |
| 315996 tcp 150.100.10.10 22441 150.100.10.10 80 105463 0.821632 100 3.79995 4 3.93122 100 0.56099 4.34942 1.00005 TCP |
| 409620 tcp 9123100 150015000 80 144299 1.755321 100 0 3 1.01505 100 0.31766 4.05430 1.00005 TCP |
| 3496840 udp 150.100.10.10 31712 150.100.10.10 80 235932 1.509211 100 0 4 2.73469 100 0.49976 3.47040 1.00005 UDP |
| 597172 tcp 150.100.10.10 189644 150.100.10.10 80 179446 1.143512 100 0 4 2.13280 100 0.39226 4.32263 1.00005 TCP |
| 1429327 tcp 150.100.10.10 168 150.100.10.10 80 25264 0.282957 100 4.05280 4 4.64880 100 0.24782 4.98252 1.00005 TCP |

Figure 4.2: Preview of the data set after processing

### 4.3 Data splitting and Clustering

After preparing our training data, we split our data for the preparation of our prediction. As per our target we are taking all of the columns (as x) in order to have the most accurate results in terms of detecting an attack or not and the category of the attack (as y) as well. Also, we used the train size and test size of 0.7 and 0.3 respectively. Furthermore, we then scale our values at ‘x’ and start preparing our data to fit in for our proposed CNN + LSTM hybrid DL model.

```python
# pseudo code of data splitting and clustering

# allocating and splitting data for train and test
trainX, trainY = train_size (0.7)
testX, testY = test_size (0.3)

# scaling
min_max_scaler = scaler()
scale_X = min_max_scaler.fit_and_transform (x)

# convert to arrays
trainX, trainY = array (scale_X), array (trainY)
testX, testY = array (testX), array (testY)

# reshaping for our CNN + LSTM model
trainX = reshape (trainX)
testX = reshape (testX)
```

Figure 4.3: Preparation of our input data
Chapter 5
Implementation & Results

To begin with, a convolutional neural network comprises an input layer, followed by hidden layers, and finally an output layer. As the activation function and final convolution cover their inputs and outputs, any middle layers in a feed-forward neural network are dubbed hidden. Convolutional neural networks have layers that conduct convolutions in their hidden layers too. Furthermore, this usually offers a layer which performs a dot product with the input matrix of the layer of the convolution kernel. Usually ReLU is the activation function of this layer and it’s also generally the Frobenius inner product. As the convolution kernel slides along the input matrix for the layer, it forms a feature map, which then avails to the input of the subsequent layer. After that, more layers including pooling layers, fully linked layers, and normalizing layers are added. Coming down to an LSTM deep learning network, LSTM networks are a type of recurrent neural network capable of adapting new order dependency in sequence prediction applications. LSTM is also a slight improvement over RNN as well. When it comes to building a hybrid CNN and LSTM model, the below two figures explain it.

![Flow diagram of a CNN+LSTM DL model](image)

Figure 5.1: Flow diagram of a CNN+LSTM DL model
5.1 Preparing the model

In terms of coding, our deep learning model we followed the flow diagram shown above. A code snippet is given below:

In the process of building the CNN model, we took 2 layers of convolution 1D with the filter size of 64, kernel size of 3 and followed by 4 layers of LSTM layer with the unit size of 15 for each. After our completion of each LSTM, as mentioned in the figure no. 2.2, we use the dropout function to prevent our neural network from over-fitting as well. Finally, in the final stage, we use the Dense function as 1 since we have a 1D data and predict that if there’s a possible attack on our IoT network and the category of the attack with the help (activation) of the sigmoid function.
5.2 Results and Accuracy

After all of our preparation of the data and model is done, we ran tests. The figures given below will explain.

In terms of getting an accuracy score, in the process of compiling and fitting the model we used the ‘sgd’ optimizer and using our acquired train data of x and y we validated them with our test data of x and y to finally fit the model. Then we evaluated the model in terms of our test data and the outputs were satisfactory. In contrast, as we can see, we get a test accuracy of around 95%, that can be considered as a very good and standard result for a hybrid deep learning model.
Figure 5.5: Plotting the accuracy using our proposed CNN+LSTM hybrid model
Chapter 6

Conclusion

To summarize, just as most important events have advantages and disadvantages, our method of ensuring appropriate security for IoT devices has certain disadvantages and issues. The first issue that needs to be mentioned is the price. Managing server machines that will be used to compute the sophisticated deep learning models sustainability will be complicated due to their high cost. As a result, our first goal is to deploy the model across a network of smart cities. Future work will focus on organizing and designing the computation of the deep learning model and edge computing framework in a cost-effective way that enables them to be utilized in various circumstances and locations.

Through parallel acceleration, quantization, and model pruning, deep learning capability on the IoT edge can be greatly optimized for faster and better results. If we want to see the optimization benefits, we need to take into account a variety of factors. When doing model quantization, for example; we must transfer the model with reduced precision parameters [21].

To Conclude, it can be said that, implementing a smart security model for IoT devices in a smart city may take several forms. Nevertheless, cryptography is not possible for all IoT devices, and not all IoT devices have increased computing capacity. Thus, by combining our hybrid deep learning model’s prediction capability for detecting attacks with the proposed technique framework and edge computing model for computing and managing end-to-end encryption with the least amount of loss and delay possible using our IoT application servers and key management servers, we truly establish a new perspective on how we can secure data for our consumers.
Bibliography


