I. J. Computer Network and Information Security, 2022, 1, 52-68
Published Online February 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2022.01.05

Mitigation of DDOS and MiTM Attacks using Belief Based Secure Correlation Approach in SDN-Based IoT Networks

Mimi M Cherian, Satishkumar L. Varma
Department of Computer Engineering, Pillai College of Engineering, Navi Mumbai, Mumbai University
E-mail: mcherian@mes.ac.in, vsat2k@mes.ac.in

Received: 28 June 2021; Revised: 11 August 2021; Accepted: 13 October 2021; Published: 08 February 2022

Abstract: In recent years the domain of Internet of Things (IoT) has acquired great interest from the ICT community. Environmental observation and collecting information is one of the key reasons that IoT infrastructure facilitates the creation of many varieties of the latest business methods and applications. There are however still issues about security measures to be resolved to ensure adequate operation of devices. Distributed Denial of Service (DDoS) attacks are currently the most severe virtual threats that are causing serious damage to many IoT devices. With this in mind, numerous research projects were carried out to discover new methods and develop Novel techniques and solutions for DDOS attacks prevention. The use of new technology, such as software-defined networking (SDN) along with IoT devices has proven to be an innovative solution to mitigate DDoS attacks. In this article, we are using a novel data sharing system in IoT units that link IoT units with the SDN controller and encrypt information from IoT unit. We use conventional Redstone cryptographic algorithms to encrypt information from IoT devices in this framework. The Proposed Belief Based Secure Correlation methodology supports the prevention of DDOS attacks and other forms of data attacks. The system proposes new routes for transmission through the controller and communicates with approved switches for the safe transmission of data. To simulate our entire scenario, we proposed the algorithm Belief Based Secure Correlation (BBSC) implemented in SDN–IoT Testbed and verified IoT data is secure during transmission in the network.

Index Terms: Distributed Denial of Service Attacks (DDoS), Software-Defined Networking (SDN), Internet of Things(IoT), Encryption, Decryption.

1. Introduction

The entire world can be considered a vast network of wired and interacting devices in today's rapidly evolving ecosystem of automated and connected devices. The Internet of Things (IoT) is a ubiquitous computing system in which sensors and actuators are interacting with living and non-living 'things,' and all of these, not just computers and smartphones, will be connected to the Internet. However, as the network grows, the problems also grow. The security problems surrounding IoT have a significant effect on the domain's future, raising concerns about the security of devices in use. Meanwhile, distributed denial of service (DDoS) assaults has been increasingly popular in the cyber security world. DDoS attacks have risen dramatically after things are linked over the Internet Since there are now more devices to hack and launch attacks. The resource-constrained systems used in IoT scenarios have made it much easier for an attacker to break in. All these research interests have increased in the recent past in this field of IoT defense. The IoT ecosystem consists of several devices with various capabilities and attributes. It varies from high-end computer systems to low memory and processing capability basic microprocessors. Security solutions must also be formulated at different levels in this diverse climate. Since the capacities of devices at various levels of the Internet of Things vary, the dimensions and properties of enforcing protection measures at each level can differ. In general, there is a variety of distributed denial of service (DDoS) and denial of service (DoS) attacks, and MITM attacks that cause various IoT devices to fail.

The Internet of Things (IoT) is a concept in which physical objects can be linked to the Internet and recognize themselves to various devices [1]. RFID, sensor technologies, and remote advancements are all closely linked to IoT devices. It allows objects to be detected and monitored from a distance using an existing device framework. The web is a network that connects people all over the world for purposes such as texting, gaming, conferencing, and web-based information exchange [2]. The ability for information broadcast, wide-ranging inspection, and planning is distributed among the universal objects. The term "intelligent" is used here to refer to a function that is considered essential. Distributed smart elements such as sensors, actuators, and information centers are made possible by the intelligent

IoT. Smart data acquisition, advanced information retrieval, monitoring, transmission, and intelligent decision support and supervision will all be possible with intelligent devices. Framework models, frameworks, and correspondences, as well as data preparation and ubiquitous processing advances, are critical to the smart IoT. Many administration applications, such as blurring processing, huge information, semantic web, learning coordination, and social registration are expected to support intelligent administration and business-related activities [3]. IoT includes things like sensing a person's temperature and switching the lights off and turning on the AC in a room based on their availability. Without individual communication, the Internet of Things (IoT) communicates information through the internet. A wide range of devices cannot be connected to the Internet by traditional IP. IPv6 is therefore the best option but does not support heterogeneous access to objects. IPv6 is used by SDN to communicate between objects from various systems[4]. One of the most common types of intrusion affecting terminal devices is a Dos attack.

IoT devices are fantastic, the data are sent to the combined framework to screen and transfer as the company provides. IoT can be used in a variety of fields, including transportation, human care, smart homes, control matrices, and smart systems [5]. Safety is especially concerned because of the large number of devices linked to the internet and the vast amount of data associated with it [6]. Most gadgets are effectively interrupted, as they depend on external assets and often go unaddressed. The interruption effectively assaults online devices. In 2020, there will be 200 million gadgets connected to the Network at all times, so programmers will most likely use these gadgets to launch DOS attacks, send malicious emails, and install Trojans. According to a current study, 70% of the IoT devices are useless in the face of attacks. Customers are disappointed to use this innovation because the confidentiality, honesty, and protection of information will be compromised [7]. The safety and security challenges at the leading edge of 5G's flexible IoT developments have long been unaddressed [8]. An IoT arrangement is legally combined with the organizer and divided into regions. It is essential to understand the implementation of distributed SDN IoT systems. To maintain the standard of administration. Figure 1 shows the standard configuration of SDN and IoT.

Man in the middle attack can be abbreviated as (MITM, MIM, MITMA). In this attack, a malicious attacker secretly takes control of the network communication channel. The attacker intercepts or modify can even replace the victim in the network. The victim is unaware of the attacker and believes that the communication channel is protected. The attacker targets the confidentiality and integrity of data in the network. In IoT networks, these data are critical and time-sensitive. Hence the severity of the situation is more critical. The Major Objective of this Work is to provide a Novel Solution for Mitigating both DDoS and MITM attacks.

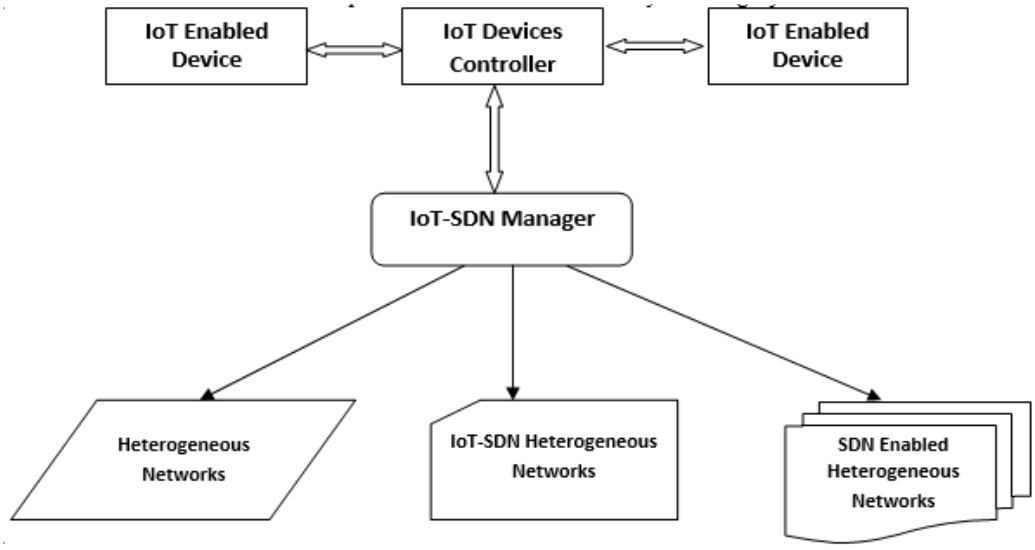

Fig.1. Architecture that combines SDN and IoT.

2. Architecture of SDN-IoT

In SDN-IoT architecture, the IoT network has its backbone network as Software Defined Network and not the traditional network. The integration of SDN and IoT makes the IoT network more programmable and provides a single view of the whole network. The attacks like DDoS and MiMA can happen in any network. But the severity of these attacks is more crucial in IoT networks. Hence the current paper discusses different techniques by which attacks like DDoS and MiM can be mitigated at the earliest by other researchers also the performance of the proposed algorithm is compared with recent mitigation techniques.

SDN will help drive the expansion of IoT-enabled devices, increase the efficiency of network resource sharing and improve IoT service-level agreements. The configuration flexibility that SDN offers can allow both network operators

and enterprises to more flexibly allocate resources to cope with this shift. Because it is software-based, and with recent hardware developments in terms of processing and memory, SDN is more resilient to limited size concerns and capable of handling the MAC addresses for a large number of IoT devices.

2.1. Multi-Layer Sdn-Iot Architecture

IoT four-layer architecture is illustrated in Figure. 2that includes IoT devices that monitor the environment and collect the data. IoT gateways that collect data from different IoT devices, SDN switches to route the packets based on flow rules created by SDN Controller, Cloud servers to store data for IoT-based applications. In the layer of the IoT device, there are two types of data IoT sensor network data and the user's Wi-Fi network. Various protocols such as Bluetooth, ZigBee, and Wi-Fi relay packets are available. IoT gateways add sensor information from a range of sensors.

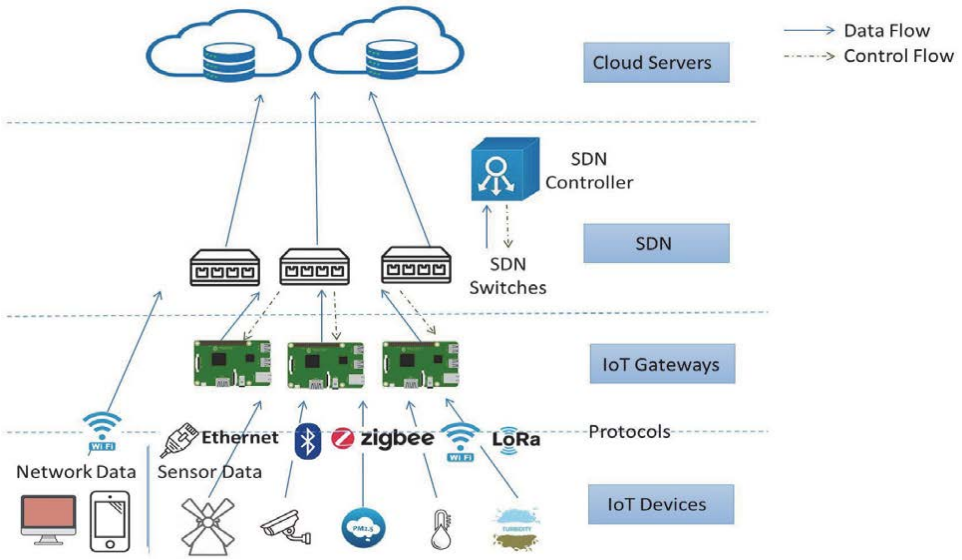

Fig.2. Multilayer SDN-IoT Architecture

For the IoT environment, the system employs a multi-layer DDoS attack detection system. The DDoS sources are divided into two IoT groups. One is the flux of network sensor data and the other is the flux of user equipment network data. To detect and block DDoS attacks the following measures are proposed. First, we design IoT security authentication faster than existing system layer encryption standards. Secondly, we choose the features of the IoT gateway captured packets and the SDN switches according to attack styles. Thirdly, in our system architecture, we incorporate data flow, control flow, and training processes.

3. Organaisation of Paper

In Section 3 we have covered a brief survey on works done in the field of DDoS and MiM attacks. The detection, mitigation techniques, and efficiency of different techniques to resolve DDoS and MiM attacks. In Section 4 we discussed the proposed architecture, methodology, and algorithms used for creating a secure software-defined architecture to make the IoT environment more secure and efficient. In Section 5 based on the proposed methodology, we have implemented the setup architecture and done a detailed result analysis. In this section, simulation results of DDoS and MiM attacks are done, the detection and mitigation time for DDoS and MiM attacks are compared with other systems that we came across during the literature survey in Section 3. The simulation results are tabulated based on a comparison of the accuracy and efficiency of our systemconcerningDDoS and MiM attacks.

4. Related Work

In this section, there are 2 sub-sections 4.1 and 4.2. In section 4.1 a survey of different techniques explored by other researchers to detect and mitigate denial of service attacks in SDN-IoT is done. The time taken for them to detect and mitigate attacks are been considered. In section 4.2 similarly to section 4.1 a broad survey is done on different techniques to detect and resolve MiM attacks in SDN-IoT. The result analysis of this survey is later considered for comparison with our proposed architecture’s implementation and performance evaluation in Section 5.

4.1. DDoS Attacks on SDNand IoT

Various methods are in use to notice and prevent assaults from DDoS because they are behaviorally different. Daoerntu[9] will create a table for the manager during a DDoS attack that tracks packets using the IP address. All latest elements are flagged as guarded, and the flow entry gives them a short timeout value. The number of packets sent over the link is measured against the smallest rate to decide if the application is legitimate otherwise malicious. This approach effectively reduces the flow input of the switch, and according to the simulation, the bandwidth of the regulator switch channel is currently usable through DDoS attacks. Even though if the attacker alters the basis address, this process consumes a lot of controller resources. Because of its randomness calculating ability, Mouhasavin and StHilaeirene [10] suggest the methodology used for DDoSdiscovery.While the proposed techniques can increase detection precision in the actual system, only discovery and solutions are addressed.

Dongen [11] proposed a statistical method called an SPRT that detected DDoS attack but its mitigation was not considered. The DARPA interruption information set [12] was evaluated and presented in a timely and accurate manner. On the other hand, rather than using random variables, the approach is evaluated solely based on mathematical outcomes.

Yanare et[13] suggest a "Multislot" approach for managing requirements on a per-request basis, so that valid users be able to talk with one another correctly during DDoS attacks. Large flow latencies are introduced when the user and the aggressor use a similar switch because the legitimate and malicious requests are placed in a similar line.

Dharmaname[14] proposes using a "flow collector" connecting the controller and switch. If the number of invalid packets goes beyond the limit for some time, the manager will inspect those suspicious packets more closely. This, however, leads to a delay for legitimate users. Moreover, no statistical investigation, simulation is available.

Shnaebr and Chithualehakm[15] established a maximum time and stage of confidence in the defense of data and control aircraft from DDoS attacks. The confidence level of the node is used to determine the priority of the control process when the value is determined based on the behavior in normal times. The manager rejects requests from certain nodules with several requirements that exceed a definite threshold during peak time. The controller responds by switching to a new rule with a shorter time-out for normal nodes. The authors, however, do not demonstrate how to describe the maximum time and its threshold. Furthermore, the suggested procedure is not simulated or evaluated on actual equipment.

To detect connection flood attacks in the SDN, Xiao et al. [16] propose using a Bloom filter. In this model, there are two subsystems: a collector and a detector. If the connection isn't right, the collector scans the switch's flow table for abnormal flows and flags them in the flow entry statistics. The detector uses a controller to keep track of the entire network and sniff packets. Because the related IP characteristics are saved in the Bloom filter, the categorization of such packets is transferred to the Bloom filter to decide whether they are irregular. However, there is no concept of abnormal link usage, and the controller makes no mention of how this problem can be detected.

Koukilaman [17] suggests that DDoS attacks should be detected using the SVM category. The SVM studies the model with training examples and forecasts that the anonymous traffic samples are natural or attackable. SVM is instructed to collect scenario-specific information on the DARPA intrusion in 2000. In comparison to other simulation approaches, the SVM is more accurate and less false. However, the output of SVM depends on the training datasets.

Phanmenor [18] also recommended using SVM and SOM combinations to differentiate DDoS attacks. Until the model is used for research, ready-made datasets will condition SVM and SOM. A special SVM is provided for each protocol to filter aircraft traffic. If a certain flow is indicated by the SVM in the attack field, it is forwarded to the classifier. If the flow is in the trendy area, the decision will be sent to SOM. The simulations show that the SVM-SOM combination works better than individually.

To reduce DDoS attacks, Lim et al. [19] recommend changing the victim's IP address. The DDoSjamming Method (DJM) on the manager uses a protected channel to connect straight to the server. When a server notices metric DDoS attacks, DJMallocates it to the latest IP address and requests that packets be transferred. When the number of packets sent to a host’s default address goes beyond a certain value, the source is tagged as an aggressive one. After the IP address has been updated. DDoS attacks are prevented, according to the simulation results. However, no mention is made of how defense and drop action measures and thresholds are established.

Chin et al. [20] are using the Monitor, Correlator, and Controller to detect DDoS attacks by concert. The monitoring section monitors the anomaly detection network and activates IDS to inspect auxiliary packets. When the IDS detects an assault, it sends the corresponding data to the monitor and notifies the organizer to find the flow table of hubs. The manager initiates the hub to act as per the avoidance behavior when the suspicious factor corresponds to any function associated with the flow table.

Macedomer proposed the DDoS Attack Mitigation Protocol for Multiple regulator SDN Networks [21], which is a multi-controller cluster model. PATMOS is divided into three phases: identifying the overloaded controller through control message delay or stability; selecting the best output regulator to synchronize alleviation, and minimizing the impact of DDoS attacks. PATMOS' efficiency in falling CPU usage, increasing the throughput, and lowering waiting time is demonstrated by the simulation results.

Hameedullaha et al. [22] recommended a secure protocol (C-to-C) regulator to control the implementation of a collaborative DDoS mitigation process. The most important are the files, certificates, and signature parts of the C-to-C protocol. The certificate part establishes a chain to verify the authenticity and honesty of the controller. When a controller recognizes a DDoS threat, it modifies the data plane policy and sends to the controller next door a list of malicious IP addresses. such packets are therefore stopped in diverse networks. Simulation results in evidence that it acquires a very small time to notify adjacent managers and overcome attacks.

Sahayamer.[23] recommended ArOMA to mitigate malicious traffic on aircraft, a DDoS protection system. ArOMA uses streamID to classify network courses and the detection engine determines whether the traffic run to the service provider is suspected. The flow status is passed on to the ISP controller through the customer's controller. The ISP controller selects the direction in which the malicious flow to the filter is being inspected. Correspondence between controllers must, however, also be protected.

BhavikaPande[24] proposed SDN based setup to prevent DDOS attacks from occurring in the same and different domains. They used a Mininet based setup for topology creation that consists of RYU Controller and OpenFlow protocol. The DDoS Prevention Mechanism is simulated and for an average of 50 nodes the detection time is 4.23 ms and the Detection accuracy is 89%.

YinqiYang[25] suggested a promising network architecture for dropping malicious traffic in the propagation path to avoid an avalanche effect on the victim server in a traditional network. A significant amount of time and effort has been invested in the existing works. Using the SDN controller wastage of resources and detection of attacks can be done in less time. they consider the characteristics of IoT traffic and employ the edge. computing to provide local services through the use of detection and mitigation methods into the IoTOpenFlow (OF) switches. The DDoS Detection and Mitigation Framework are simulated and for an average of 50 nodes the detection time is 6.9 ms and the Detection accuracy is 85%.

DDoS attacks in SDN, as mentioned in the previous section, are a well-studied subject that still requires attention to progressDDoS detection and mitigation. Security[24] is the most important issue in the IoT system as a result of IoT device flaws. The security of IoT networks can be improved by combining SDN and IoT networks, particularly next toDDoSattacks[26-27].

Tortonesisedc [28] proposed SPF as an SDN-based design for reducing data bursts in IoT, which was similar to the DDoS attack situation. The processing and distribution element, which includes a programming unit, replaces the data plane in the SDN. This module allows you to get instructions from the SPF controller. The processing module divides user application requests into categories based on the type of service requested and then assigns a priority to each request as a point of reference for dissemination. The expertise of SDN controllers is used to make informed decisions.

To identify and overcome DDoS attacks on an IoT network's edge node, Ozçelikmanl. [29] use a scheme called Border centered Software-Defined IoT Defense (BCESID). The discovery calculation relies upon the suspicions (i) a kind association is bound to prevail over a malicious association, and (ii) association demands from a contaminated host are more normal than demands from a typical host. Thus, the number of connection endeavors and disappointment checks over the long run can be utilized to decide if a host is contaminated. From the SDN regulator to the switch, altered stream rules are embedded to hinder all streams from that malicious host.

Based on IoT paradigms, Sarwar.[30] suggested a trust framework for defending SDN controllers against DDoS attacks. Each network user's historical record is assigned a trust value, which means that a superior trust rate represents the manager will give the request higher priority, whereas a low confidence level means the user will discard packets. In addition, the controller has a queue buffer request; if such storage is overloaded, the appeal with a small confidence level is crashed in favor of a more reliable inquiry.

To recognize DDoS assaults in the IoT organization, Ravi and the remaining [31] utilize semi-administered AI calculations. Learning-driven recognition relief is a progressive control plane component that sorts IoT gadgets into two gatherings: fixed and versatile. A nearby regulator is accountable for a solitary organization fragment, while an all-inclusive regulator is responsible for all neighborhood regulators. LEDEM distinguishes DDoS assaults dependent on approaching parcel highlights, and an AI model is prepared with both named and unlabeled information to decide if an IoT framework has been settled.

According to Sharma et al. [32], machine learning should be used to detect DDoS attacks, and cloud networks and wireless SDN should be used in tandem to safeguard IoT networks from DDoS attacks. When the latest node joins the network, the OpCloudSecsystem analyses it using a deep brief network to determine whether it is attacked or not. Regular traffic will be transferred, but identified assault traffic will be sent to the manager for additional directions. if the attack is latest, OpCloudSecpermits administrators to add it to the attack catalog, making it an imminent attack for the subsequent time it occurs.

According to Nobnmerkht[33], IoT-IDM is a smart home-dependent method for intrusion detection in IoT networks that employs machine learning. IoT-IDM relies on the number of times in control and reply packets, as well as the inter-packet interval, as detection indicators because smart home IoT devices must be switched on and off physically. The precision rate from actual implementation could reach over 91 percent if mutually linear and nonlinear logistic regression methods of machine learning are used. In the survey different detection and mitigation techniques of DDOS attack and their accuracy is noted for furthers comparisons.

4.2. Literature on Man-in the Middle Attack

Man in the middle attack happens in a network when an attacker tries to intercept the packets that are sent between two legitimate nodes. The communication channel is less secure due to which attackers can intrude on the network. U. Meyer and S. Wetzel discussed the man-in-the-middle attack on mobile communication which they presented in a report in the year 2014,[34]. In 2016, the author published his research on an encryption method of MITM using Kirchhoff-loop-Johnson in a master listed journal [35]. In paper [36] the authors have researched secure Bluetooth communication along with the implementation of a system that was capable of preventing MITM attacks. Sun et al., 2018 and Saif et al., 2018; discussed new techniques to prevent MITM in two-party communication and made similar research on an updated version of Bluetooth networks security[37].

Sounthiraraj et al., (2014) found MITM as a very serious threat and discussed various prevention techniques while researching HTTP security issues[38].

Tung et al. (2019) published their researches on different prevention methods of MITM [39]. Wallace and Miller (2017) tested multiple prevention methods for MITM and patented their research about endpoint-based MITM [40].

Conti et al. (2016); worked on effects on the economy due to MITM[41]. Howell et al. (2018) discussed several effective measures on the prevention of MITM from on-net communication and made identical researches on the prevention of MITM mainly for internet communication[42]. Kuo et al. (2019) discussed WLAN security for 2-way communication and published their review reports on MITM[43]

FarouqAliyu[44] proposed a system to resolve Man in the Middle (MitM) attack at the fog layer. These systems are Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) The IDS consists of IDS nodes that periodically interrogate nodes one hop away. The IPS uses lightweight encryption to preventsMiMA. The solution in this work is the IPS-IDS System framework which is evaluated and the detection time and detection accuracy is 4.5ms and 90% for an average of 50 nodes

Cheng Li,[45] specifically investigated the potential threats of Man-in-the-Middle attacks on the OpenFlow control channel. They first introduced a feasible attack model in an IoT-Fog architecture, and then implemented attack demonstrations to show the severe consequences of such attacks. Additionally, they proposed a lightweight countermeasure using Bloom filters. They implemented a prototype for this method to monitor stealthy packet modifications.

YiLi[46] proposed a system that can provide a global view of a network so that the Wifi network can be managed. The SDN controller is deployed with two components detection and mitigation. Once the attack is detected the mitigation module will update the flow rules and redirect the packets. These attack packets are stored to perform further analysis of the attack pattern. Extensive experimental results demonstrate that the proposed framework can efficiently detect and mitigate KRACK framework. For 50 nodes the attack detection time and accuracy are 6.3ms and 86% respectively. A survey on different recent techniques to mitigated MiMA and its time duration is noted for further comparisons.

5. Proposed Architecture and Methodology

In this section, we will discuss the proposed secure defined architecture for IoT networks and its implementation. The secure SDN-IoT architecture in Figure 3, has an IoT environment from which data is collected and send through the IoT gateway. The IoT Gateway is part of a Software-Defined Network along with many other hosts, gateways, SDN Controller and OpenFlow enabled switches. The SDN controller has a northbound API in which the proposed methodology of section 4 is implemented. The API helps in detecting and mitigating different attacks like DDoS and MiM attacks. SDN-enabled IoT network makes the network more scalable and adaptable as per dynamic traffic compared to the traditional network used for IoT. The cloud platform used to store IoT data is Thingsboard.

We developed the Belief Based Secure Correlation (BBSC) algorithm. Clients can connect to enabled networks thanks to the SDN architecture represented by BBSC. To provide users with contact to a verification check, the BBSC scheme employs ciphertext-policy attribute-based encryption. Overall, ciphertext policies, which will be implemented as both SDN controllers and information plane OpenFlow switches, are used to power the device.

The primary goal of the BBSC working procedure is to make communication among users and switches easier. It connects to the network's platform and performs access authentication for client individuality. The SDN controller controls the decision to accept users and prevents unauthorized users from accessing the network through an access authentication service. We used a reliable method that is essentially ciphertext-policy attribute-dependent encryption [49]. The BBSC method is maintained by the SDN controller process, and the access authentication service is checked by the SDN controller process. Following that, the SDN IoTadmissionmachine validates each request and grants the right of entry as per the rule. The validation method is encrypted with one SDN controller's public key to prevent an unauthorized client from gaining access to it. When a user first joins the architecture, it checks the user's uniqueness as well as the access platform.

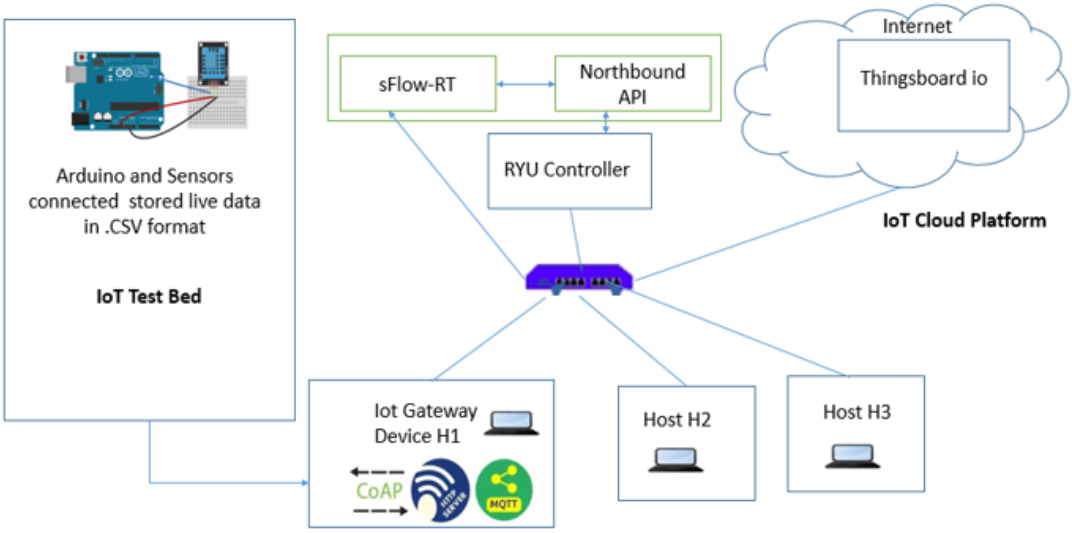

Fig.3. SDN-IoT Architecture

An output containing the public key and its corresponding private key. The publish and delivery systems are implemented using the trusted authority scheme. The public key is connected to the published system, and the master secret key is connected to the delivery system. The authentication process is depicted in Figure 4.The client's authorization is experienced throughthe network platform and uniqueness during the verification process, and the access method is embedded in that method. The authentication mechanism and the encrypted access policy both keep track of a division of characteristics.

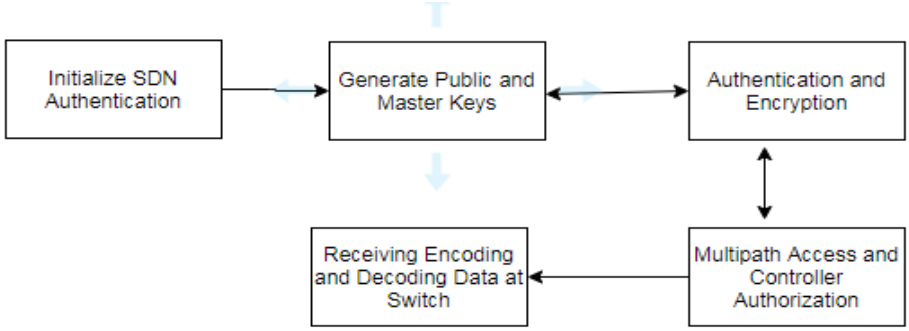

Fig.4. BBSCbasedIoTWorking Procedure

In Figure 4 the steps involved in BBSC based IoT working procedure are as follows:

1. Initialization: 1.1 initializes the SDN Authentication
   1.2Assign attribute for users
2. Public Key Generation
   2.1 Generate Public and Master Secret Keys
   2.2 Implement Distribution System
3. Encryption Process
   3.1 Initiate Encryption Process after proper Authentication
   3.2 Receive Request from users
   3.3 Send Request to Switches
4. Create Multi path access
   4.1 Switches Receive requests from Users and access the multipath from SDN Controllers
   4.2 Controller authorizes switches and accepts the users
5. Communication
   5.1 Multipath secure data is happening
   5.2 Authorized switches receive the encoded data
   5.3 Switches decode the encoded data

A request from an IoT access system is received by the authorization method's core, which then transfers it to SDN switches. SDN switch is excluded from the SDN network if it fails to maintain security or service efficiency. In this case, the SDN controller in our proposed system creates a new multicast route and enhances multicast protection by generating keys that are broadcast to switches. To turn at the primary phase in the series, the process controller must be approved and authenticated. As a result, the Controller devised new forwarding paths between source and destination that were previously difficult to locate using the traditional scheme. Approved switches are installed on the routes during data transfers to ensure that data is effectively protected against attacks. As shown in Algorithm. 1, the Redstone algorithm encrypts user data so that it can only be accessed by authorized switches. The data is readable after it has been decrypted, as shown in Algorithm 2. . After that, the access strategy is applied to the obtained user data, which has been encrypted using the public key principle used in the authentication process. The data is processed, decrypted with a secret key, and the client's individuality, as well as system characteristics, are verified in the last step of the access strategy. The verification tool, which is built on top of the controller, generates the flow table. Multi-access privileges are granted to customers who effectively complete the validation process. It will also take into account the characteristics of the network platform as well as the individuality of each client.

Algorithm 1: EncryptionAlgorithm

Encryption Algorithm

1. Start
2. Generate Encryption Key
3. For(i=0;i<n;i++)
   {
4. Identify various incidences of key
5. Eliminate the entire replicas of Key

}

Eliminate non-alphabetic typescripts

If input length < 5

Affix the string

{

Identify the location of the Key

Append the string

Create the secret message

}

6. Stop

Algorithm 2: DecryptionAlgorithm

Decryption Algorithm

1. Start
2. Receive the Secret Message
3. Generate Square of the key
4. Eliminate the Non Alphabetic Typescripts
5. Calculate the length of the Secret Text
6. For (i=0;i<length; i++)

{

Remove Non Alphabetic Typescripts

If input length < 5

Join the string

Identify the location of the key

Join the string

Generate Decrypted Text

}

7. Stop

When compared to previous approaches, this is a vastly improved definition. The proposed approach would provide greater versatility while also lowering costs. The authentication method in BBSC-based SDNs ensures a secure communication of data in combination with an authorization access policy. Sections 4 and 5 go over the system's performance in detail, including a description of the simulation, as well as simulation environments and graphs that show the system's advantages.

For client access, multi-point access has been integrated, making the multi-client authentication process easier for users. The authentication cryptography principle has also been completed. This is an important feature of our proposed system because many network providers are not able to provide it, which compromises both the availability of authentication and approval aspects. The authentication procedure for the BBSC-based SDN network is depicted in Algorithms 1 and 2 . Since the controller can limit acts that violate the SDN network's security, the SDN network was tested with crypt-analysis attacks. MININET testbed was used to validate the proposed procedure. We were able to monitor the results and check the progress in this manner.

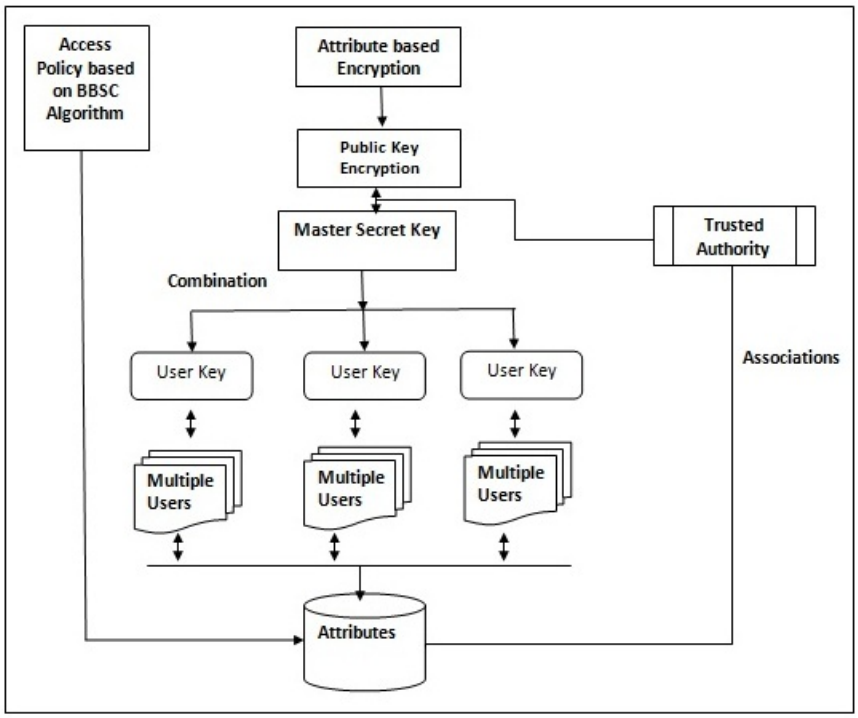

Fig.5. Safe Authentication Procedure in BBSC dependent SDN Network

6. DDoS and Man in the Middle Attacks Simulation in SDN-Based IoT Architecture

A MININET simulation was used to carry out the research. An experimental network was used to start the evaluation. The controller in the SDN network is responsible for the multicasting module's execution. The development of a safe path was combined with the use of dependable switches to determine the multicast transmission path. The mechanism for establishing trust among the switches and controller is critical. The controller is responsible for sending the information of the devices that create the multipath to the trust establishment. The trust establishment mechanism can detect any suspicious behavior by the switches, allowing the switches to be isolated and the multicast path's efficiency to be improved. The encoding and decoding of the vector were combined with the network communication overhead. The time-consuming computation mechanism ensures that stable switches are maintained. The controller addresses the trusted switches and initiates contact along with network specifications. By default, the switches receive the session key with broadcast encryption. The controller allocates to the network the keys generated in the network. The switches serve as a non-recipient storage point.

Mininet (accessible at: http://mininet.org/) is used to test the performance of the SDN-dependent IoT DDOS algorithm BBSC, and the simulation is run on Ubuntu 12 with an Intel i3 CPU and 4 GB RAM. The configuration of the practical network is shown in Figure 6. This network has 05 switches (s1–s5) connected to the same controller, each with two subordinate hosts (h1–h8), for a total of 16 hosts (h1–h8). The bandwidth of every connection among switches and hosts is restricted to 2 GB. From h1 to h18, the iPerf tool (Traffic generator, available at: https://iperf.fr) is in use to calculate accessible bandwidth, allowing us to compare performance when the network is regular, when an attack occurs, are covered. Here, h1 represents a new client, and h18 represents a server. There are 05 IoT attackers among the remaining 17 hosts; these compromised hosts produce malicious traffic to use network resources. A new user is represented by h1, and a server is represented by h18. Among the remaining 17 hosts, 05 attackers produce malicious traffic to use network resources.

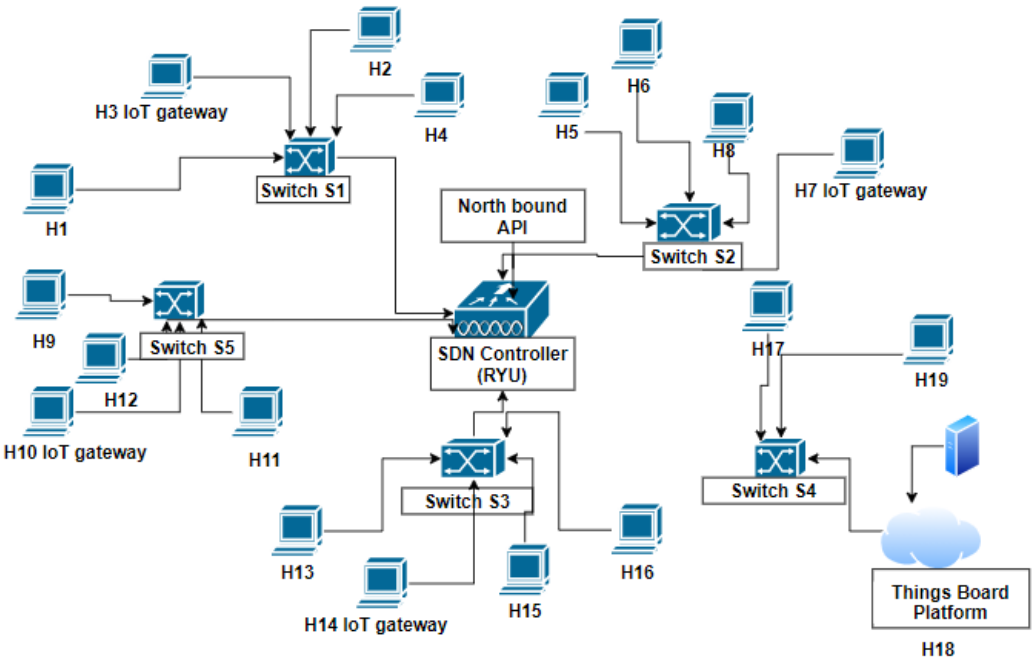

Fig.6. Testbed Setup in the mininet

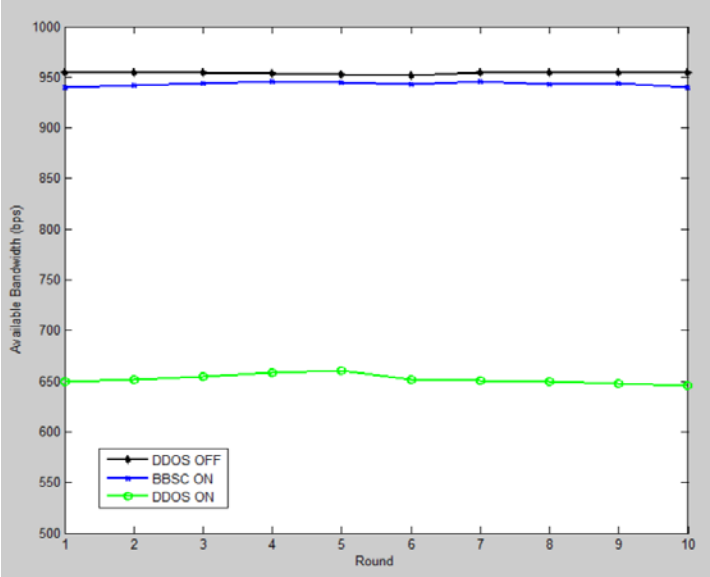

Fig.7. Bandwidth Accessibility with and without DDOS Attacks

The usable bandwidth in normalandDDoS attack states is compared to confirm the output of BBSC. Figure 7 depicts the results of ten runs for each scenario. The total available bandwidth on the network is 1850 Mbps when it is in a normal state, but it drops to 753 Mbps during DDoS attacks. The average bandwidth is 1835 Mbps when BBSC is activated in response to a DDoS attack. As a result of the findings, it is clear that BBSC can protect the network from DDoS attacks coming from a variety of directions. Figure 7 is a graphical representation of bandwidth utilization in the network during the attack. It is found that due to DDOS attack utilizes maximum bandwidth of network thus accessibility to legitimate resources are less. Hence by implementing the proposed algorithm the bandwidth utilization is less even when the network is under attack as the detection and mitigation of the attack was more efficient comparatively.

Detection Time:

In the detection process, the running device needs analysis to detect malicious traffic leading to DDoS attacks Detection entails using a sophisticated method to detect vast amounts of illegal GET request traffic directed at a web server. Pattern matching, clustering, deviation analysis, associations, and correlations are only a few of the detection strategies that have been used to detect DDoS attacks. Detection time in this work refers to the total time taken to detect the DDOS attack. Here we will compare the algorithm for our BBSC with two other related DDOS, namely DDOS.

Prevention Mechanism [24] and DDoS Detection and Mitigation Framework [25]. Here we compare our BBSC algorithm. The attack detection time is measured in milliseconds. In this time we will consider both the time taken to send the packets from switches to servers and vice versa as well as the total time taken for the attack to happen for the network. The algorithms are evaluated on mininet and the acquired results are in Table 1:

Table 1. Evaluation of Detection Time

Number of Packets	Detection Time (ms)		
	BBSC	DDOS Prevention Mechanism	DDoS Detection and Mitigation Framework
10	1.15	1.45	2.32
20	1.96	2.32	3.35
30	2.32	3.32	4.36
40	2.69	3.96	5.36
50	2.96	4.23	6.89
60	3.64	5.36	7.93
70	4.23	6.89	8.35
80	5.45	7.36	9.36
90	6.59	8.96	10.36
100	8.06	9.53	11.56

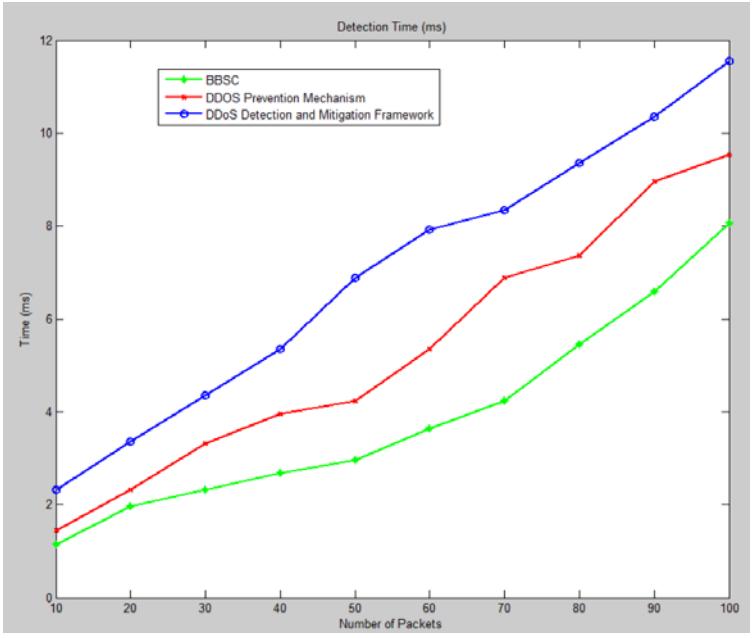

Fig.8. Performance Evaluation of Attack Detection Time

Figure 8 illustrates the attack detection time of three different algorithms. here the attack detection time is directly proportional to the number of packets. As the traffic in the network increases automatically detection time also will be increased. but the results show that when compared to the remaining algorithms our BBSC security algorithm has very little detection time because of its security mechanism used. Hence the detection time using the BBSC security algorithm is reduced by 26% compared to [24] and 43% compared to [25].

Detection Accuracy:

While transferring the packets in the network some DDOS attacks may happen in the network. When an attack happens we will classify the packets as attack packets and normal packets. It is characterized as the system's ability to classify a packet as an "attack packet" and "normal packet." It describes the ratio of the right prediction for all samples. It is expressed mathematically in the following equation:

$$Accuracy = \frac{TP+TN}{TP+FN+TN+FP} X\ 100 \quad (1)$$

In equation 1, the notations are as follows: TP-True Positive, TN-True Negative, False Positive, and FN-False Negative depending upon the classification of packets into these categories we evaluate the detection accuracy of the algorithm. As mentioned in the preceding section we compare our BBSC algorithm Detection accuracy with two more similar DDOS algorithms namely DDOS Prevention Mechanism [24] and DDoS Detection and Mitigation Framework [25]. Detection accuracy is measured in terms of percentage(%). The evaluated results of the three algorithms detection times are present in Table 2:

Table 2. Evaluation of Detection Accuracy

Number of Packets	Detection Accuracy (%)		
	BBSC	DDOS Prevention Mechanism	DDoS Detection and Mitigation Framework
10	98.23	95.12	92.36
20	95.23	93.23	90.36
30	93.08	92.12	88.36
40	92.85	90.12	86.56
50	91.23	88.92	84.23
60	90.85	86.55	82.56
70	89.56	85.36	80.56
80	88.63	84.08	79.56
90	87.55	82.23	78.16
100	86.23	81.53	77.05

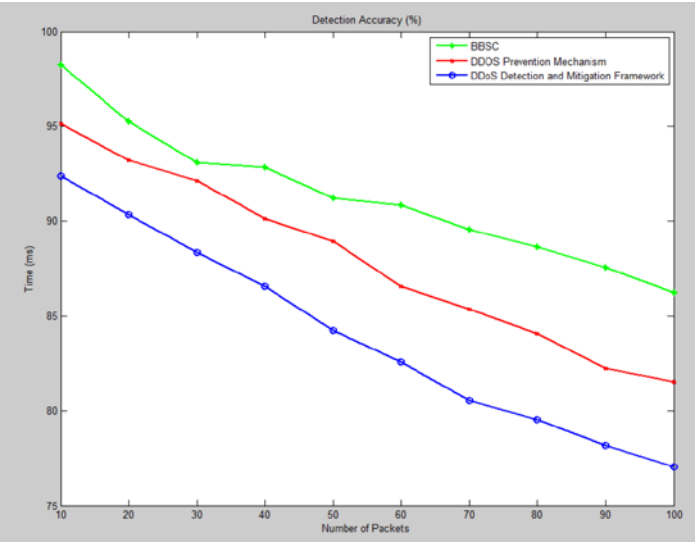

Fig.9. Performance Evaluation of Attack Detection Accuracy

The Figure 9 graph illustrates the attack detection accuracy of three different algorithms. here the attack detection accuracy is very high when we have a few packets. As the traffic in the network increases automatically detection accuracy will be decreased when the packets are more automatically traffic will be more and there is a loss of packets due to DDOS attacks. Hence, the results show that when compared to the remaining algorithms our BBSC security algorithm has very high detection accuracy because of its novel algorithms used in the BBSC security mechanism. Hence the detection accuracy using the BBSC security algorithm is improved by 6% compared to [24] and 15% compared to [25].

Simulation of Mitm Attack:

In this Section Man in the middle attacks are being simulated. Our proposed system BBSC is capable ofsolving Mitm attacks also.In this section, we are going to compare the BBSC algorithm with the IPS-IDS System framework[44] and KRACK mitigation Framework[46].We will simulate the BBSC in terms of detection time and detection accuracy and the results are as follows:

Detection Time for MitM:

The attack detection time is measured in milliseconds. In this time we will consider both the time taken to send the packets from switches to servers and vice versa as well as the total time taken for the attack to happen for the network. The algorithms are evaluated on mininet and the acquired results are in Table 3.

Table 3. Evaluation of Detection Time for MItM attack

Number of Packets	Detection Time (ms)		
	BBSC	**IPS-IDS System frame work**	KRACK mitigation Framework
10	1.53	1.69	2.45
20	2.01	2.56	3.12
30	2.39	3.18	4.53
40	2.96	4.01	5.63
50	3.01	4.56	6.23
60	3.96	5.86	7.23
70	4.23	6.89	8.21
80	5.12	7.23	8.96
90	6.32	8.23	9.94
100	7.26	8.56	10.25

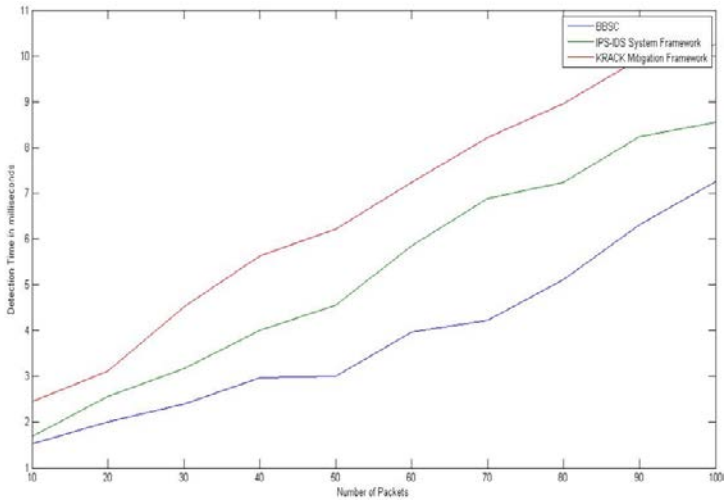

Fig.10. Performance Evaluation of Attack Detection Time for solving MItM attacks

Figure 10 graph illustrates the attack detection time of three different Frameworks for solving MItM attacks. here also the attack detection time is directly proportional to the number of the packet. If the data traffic increases which increases the detection time as the number of defective packets are more. but the results show that when compared to the remaining algorithms our BBSC security algorithm has very little detection time because of its security mechanism used. Hence the detection time using the BBSC security algorithm is better by 31% compared to [44] and 39% compared to [46].

Detection Accuracy for MItM attacks:

Detection accuracy is measured in terms of percentage(%). The evaluated results of the three frameworks detection times are in Table 4:

Table 4. Evaluation of Detection Accuracy

Number of Packets	Detection Accuracy (%)		
	BBSC	**IPS-IDS System frame work**	**KRACK mitigation Framework**
10	99.53	96.23	95.36
20	97.23	95.23	93.36
30	95.08	93.12	90.36
40	92.85	90.12	89.56
50	91.23	89.92	85.23
60	90.85	88.55	83.56
70	89.56	87.36	82.56
80	88.63	85.08	80.56
90	87.55	84.23	79.16
100	86.23	83.53	78.05

Figure 11 graph illustrates the attack detection accuracy of three different algorithms. here the attack detection accuracy is very high when we have fewer packets similar to the previous section. As the traffic in the network increases automatically detection accuracy will be decreased because more number of vulnerable packets when traffic increases. Hence, the results show that when compared to the remaining algorithms our BBSC security algorithm has very high detection accuracy because of the BBSC security mechanism. Hence the detection accuracy using the BBSC security algorithm is improved by 12% compared to [44] and 10% compared to [46].

In the paper [47] we had done an extensive Survey on Security threats in IoT and Emerging Countermeasures form which we had concluded that major security issues in IoT networks are denial of service (DoS) attack, distributed denial of service (DDoS) attack and Man in the Middle attack which was not effectively mitigated and resolved with a traditional network. Later in our paper [48], we understood the need of replacing the traditional IoT network paradigm with SDN to detect and mitigate network DDoS thus in the paper we implemented a testbed to resolve DDoS attacks. In our current proposed system, we have designed secure software-defined architecture for IoT networks that can detect and mitigate network attacks like DDoS and MiMA effectively. The implemented architecture is adaptable and easily configurable, scalable as the number of nodes increases.

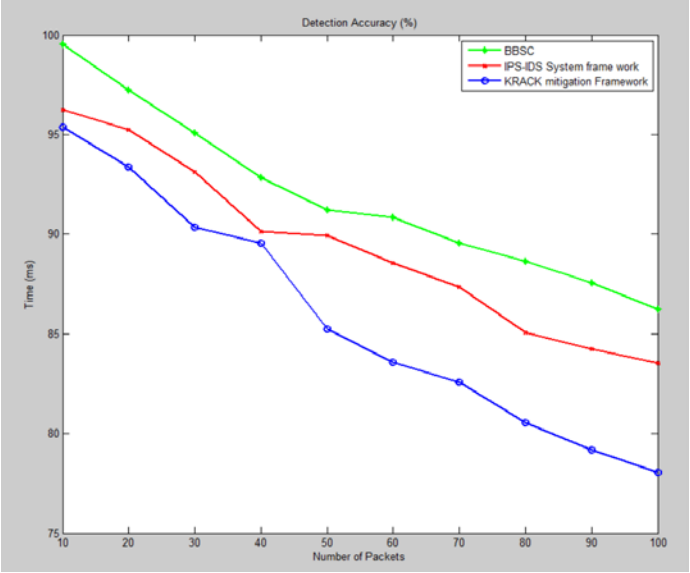

Fig.11. Performance Evaluation of Attack Detection Accuracy

7. Conclusion

In the current paper, we proposed a BBSC multipoint access SDN broadcast encryption method for a securely improved IoT-dependent SDN network. The proposed system will offer safe authentication access using BBSC based SDN Network. The routers are regulated by IoT multicast-protected transmission, which ensures data protection during transmission by transmitting the keys parallel to the SDN switches. The multi-client verification access requests meet a cryptography authentication system. The BBSC algorithm is tested and analyzed to secure the IoT network based on SDN in real testbeds to detect and mitigate DDoS and MiTM attacks. Since IoT has a wide range of applications in diverse areas, IoT is vulnerable to DDoS attacks, which have a significant effect on SDN-based IoT networks. Periodic and random IoT traffic is simulated and tested in the actual MININET testbed. We have evaluated the available bandwidth, compared our BBSC algorithm with two more popular DDOS Security algorithms in terms of detection time and detection accuracy, and shown that our algorithm performs well in terms of both parameters. This SDN-based architecture is easily adaptable, scalable in any IoT network also can detect and mitigate DDoS attacks efficiently. Currently, the testbed has considered periodic data transmission from IoT devices in the future would like to improvise the algorithm further such that even for random data generation from IoT devices the attacks will be detected and mitigated efficiently.

References

[1] Chuah, J.W.: The Internet of Things: an overview and new perspectives in systems design. In: International Symposium on Integrated Circuits (2019). 978-1-4799-4833-8/14

[2] Agrawal, S., Das, M.L.: Internet of Things – A Paradigm Shift of Future Internet Applications, Institute of Technology, Nirma University, Ahmedabad 382 481, 08-10 (2011)

[3] Guest Editorial: IEEE Systems Journals Special Issue on “Intelligent Internet of Things”.IEEE Syst. J. 10(3) (2018).

[4] Jararweh, Y., Al-Ayyoub, M., Darabseh, A., Benkhelifa, E., Vouk, M., Rindos, A.: SDIoT: a software de*fi*ned based Internet of

Things framework. Springer, Heidelberg (2018). Print ISSN 1868-5137, Online ISSN 1868-5145
[5] Shin, S., Gu, G.: Attacking software-de*fi*ned networks: a *fi*rst feasibility study. In: Proceedings of the 2nd ACM SIGCOMM Workshop Hot Topics Software De*fi*ned Networks, New York, NY, USA, pp. 165–166 (2017)
[6] Xu, X.: Study on security problems and key technologies of the Internet of Things. In: International Conference on Computation and Information Sciences (2019)
[7] Kanuparthi, A., Karri, R., Addepalli, S.: Hardware and embedded security in the context of Internet of Things. In: CyCAR 2013: Proceedings of the 2013 ACM Workshop on Security, Privacy and Dependability for Cyber Vehicles, pp. 61–64 (2018)
[8] Zhou, J., Cao, Z., Dong, X., Vasilakos, A.V.: Security and privacy for cloud-based IoT: challenges, countermeasures, and future directions, impact of next-generation mobile technologies on IoT: cloud sconvergence.,2018
[9] Dao, N.N.; Park, J.; Park, M.; Cho, S. A feasible method to combat against DDoS attack in SDN network. In Proceedings of the 2015 International Conference on Information Networking (ICOIN), Siem Reap, Cambodia, 12–14 January 2017; pp. 309–311. doi:10.1109/ICOIN.2015.7057902.
[10] Mousavi, S.M.; St-Hilaire, M. Early detection of DDoS attacks against SDN controllers. In Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC), Anaheim, CA, USA, 16–19 February 2017; pp. 77–81. doi:10.1109/ICCNC.2015.7069319
[11] Dong, P.; Du, X.; Zhang, H.; Xu, T. A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 23–27 May 2017; pp. 1–6. doi:10.1109/ICC.2016.7510992
[12] Laboratory, M. Intrusion Detection Attacks Database. Available online: https://archive.ll.mit.edu/ideval/data/index.html
[13] Yan, Q.; Gong, Q.; Yu, F.R. Effective software-defined networking controller scheduling method to mitigate DDoS attacks. *Electron. Lett.* **2017**, *53*, 469–471.
[14] Dharma, N.I.G.; Muthohar, M.F.; Prayuda, J.D.A.; Priagung, K.; Choi, D. TDMSC:Time-based DDoS detection and mitigation for SDN controller. In Proceedings of the 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), Busan, Korea, 19–21 August 2017; pp. 550–553. doi:10.1109/APNOMS.2015.7275389
[15] Shoeb, A.; Chithralekha, T. Resource management of switches and Controller during saturation time to avoid DDoS in SDN. In Proceedings of the 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, India, 17–18 March 2018; pp. 152–157. doi:10.1109/ICETECH.2016.7569231.
[16] Xiao, P.; Li, Z.; Qi, H.; Qu, W.; Yu, H. An Efficient DDoS Detection with Bloom Filter in SDN. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2018; pp. 1–6. doi:10.1109/TrustCom.2016.0038.
[17] RT, K.; Selvi, S.T.; Govindarajan, K. DDoS detection and analysis in SDN-based environment using support vector machine classifier. In Proceedings of the 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2019; pp. 205–210.
[18] T.Phan.; Bao, N.; Park, M. A Novel Hybrid Flow-Based Handler with DDoS Attacks in Software-Defined Networking. In Proceedings of the IEEE Conferences on UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld, Toulouse, France, 18–21 July 2019; pp. 350–357.
[19] Lim, S.; Ha, J.; Kim, H.; Kim, Y.; Yang, S. A SDN-oriented DDoS blocking scheme for botnet-based attacks. In Proceedings of the Conference on Ubiquitous and Future Networks, Shanghai, China, 8–11 July 2019; pp. 63–68. doi:10.1109/ICUFN.2014.6876752.
[20] Chin, T.; Mountrouidou, X.; Li, X.; Xiong, K. An SDN-supported collaborative approach for DDoS flooding detection and containment. In Proceedings of the IEEE Military Communications Conference, Tampa, FL, USA, 26–28 October 2018; pp. 659–664. doi:10.1109/MILCOM.2015.7357519.
[21] Macedo, R.; de Castro, R.; Santos, A.; Ghamri-Doudane, Y.; Nogueira, M. Self-Organized SDN Controller Cluster Conformations against DDoS Attacks Effects. In Proceedings of the IEEE Global Communications Conference, Washington, DC USA, 4–8 December 2017; pp. 1–6. doi:10.1109/GLOCOM.2016.7842259.
[22] Hameed, S.; Khan, H.A. Leveraging SDN for collaborative DDoS mitigation. In Proceedings of the 2017 International Conference on Networked Systems, Gottingen, Germany, 13–16 March 2018; pp. 1–6. doi:10.1109/NetSys.2017.7903962.
[23] Sahay, R.; Blanc, G.; Zhang, Z.; Debar, H. ArOMA: An SDN based autonomic DDoS mitigation framework. *Comput. Secur.* 2018,*70*, 482–499.
[24] Bhavika Pande,et.al: Detection and mitigation of DDoS in SDN.In Proceedings of 2018 Eleventh International Conference on Contemporary Computing (IC3), 2-4 August, 2018, Noida, India.
[25] Yang Y., Wang J., Zhai B., Liu J. (2019) IoT-Based DDoS Attack Detection and Mitigation Using the Edge of SDN. In: Vaidya J., Zhang X., Li J. (eds) Cyberspace Safety and Security. CSS 2019. Lecture Notes in Computer Science, vol 11983. Springer, Cham. https://doi.org/10.1007/978-3-030-37352-8_
[26] Al Shuhaimi, F.; Jose, M.; Singh, A.V. Software defined network as solution to overcome security challenges in IoT. In Proceedings of the IEEE Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), Noida, India, 7–9 September 2019; pp. 491–496.
[27] Ahmed, M.E.; Kim, H. DDoS Attack Mitigation in Internet of Things Using Software Defined Networking. In Proceedings of the IEEE Conference on Big Data Computing Service and Applications, San Francisco, CA, USA, 6–9 April 2018; pp. 271–276. doi:10.1109/BigDataService.2017.41.
[28] Tortonesi, M.; Michaelis, J.; Morelli, A.; Suri, N.; Baker, M.A. SPF: An SDN-based middleware solution to mitigate the IoT information explosion. In Proceedings of the IEEE Symposium on Computers and Communication, Messina, Italy, 27–30 June 2017; pp. 435–442. doi:10.1109/ISCC.2016.7543778.
[29] Özçelik, M.; Chalabianloo, N.; Gür, G. Software-defined edge defense against IoT-based DDoS. In Proceedings of the 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 21–23 August 2017; pp. 308–313.
[30] Sarwar, M.A.; Hussain, M.; Anwar, M.U.; Ahmad, M. FlowJustifier: An optimized trust-based request prioritization approach for mitigation of SDN controller DDoS attacks in the IoT paradigm. In Proceedings of the 3rd International Conference on

Future Networks and Distributed Systems, Paris, France, 1–2 July 2019; pp. 1–9.
[31] Ravi, N.; Shalinie, S.M. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet Things J.* 2020, *7*, 3559–3570.
[32] Sharma, P.K.; Singh, S.; Park, J.H. OpCloudSec: Open cloud software defined wireless network security for the Internet of Things. *Comput. Commun.* 2018, *122*, 1–8.
[33] Nobakht, M.; Sivaraman, V.; Boreli, R. A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2019; pp. 147–156.
[34] Meyer, U., and Wetzel, S. (2014, October). A man-in-the-middle attack on UMTS. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 90-97). ACM.
[35] Kish, L. B. (2016). Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson (-like)-noisecipher and expansion by voltage-based security. *Fluctuation and Noise Letters*, *6*(01), L57-L63.
[36] Hypponen, K., and Haataja, K. M. (2017, September). "Nino" man-in-the-middle attack on bluetooth secure simple pairing. In *Internet, 2017. ICI 2017. 3rd IEEE/IFIP International Conference in Central Asia on* (pp. 1-5).IEEE.
[37] Sun, D. Z., Mu, Y., and Susilo, W. (2018). Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5. 0 and its countermeasure. *Personal and Ubiquitous Computing*, *22*(1), 55-67.
[38] Sounthiraraj, D., Sahs, J., Greenwood, G., Lin, Z., and Khan, L. (2018). Smv-hunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps. In *In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'18)*.
[39] Tung, Y. C., Shin, K. G., and Kim, K. H. (2016, July). Analog man-in-the-middle attack against link-based packet source identification. In *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*(pp. 331-340). ACM.
[40] Wallace, Brian Michael, and Jonathan Wesley Miller. "Endpoint-based man in the middle attack detection using multiple types of detection tests." U.S. Patent 9,680,860, issued June 13, 2017.
[41] Conti, M., Dragoni, N., and Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys and Tutorials*, *18*(3), 2027-2051.
[42] Howell, C., Statica, R., and Coppa, K. L. (2018). *U.S. Patent No. 9,906,506*. Washington, DC: U.S. Patent andTrademark Office.
[43] Kuo, E. C., Chang, M. S., and Kao, D. Y. (2018, February). User-side evil twin attack detection using time-delay statistics of TCP connection termination. In *Advanced Communication Technology (ICACT), 2019 20th International Conference on*(pp. 211-216). IEEE.
[44] Farouq Aliyu, Tarek Sheltami, Elhadi M. Shakshuki, A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing, Procedia Computer Science,Volume 141,2018,Pages 24-31,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2018.10.125.
[45] C. Li, Z. Qin, E. Novak and Q. Li, "Securing SDN Infrastructure of IoT–Fog Networks From MitM Attacks," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1156-1164, Oct. 2017, doi: 10.1109/JIOT.2017.2685596.
[46] Li, Y., Serrano, M., Chin, T., Xiong, K. and Lin, J.A Software-defined Networking-based Detection and Mitigation Approach against KRACK.DOI: 10.5220/0007926202440251 In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019), pages 244-251.ISBN: 978-989-758-378-0
[47] Mimi Cherian and Madhumita Chatterjee, "Survey of Security Threats in IoT and Emerging Countermeasures", Springer SSCC 2018: Security in Computing and Communications pp 591-604
[48] Mimi Cherian and Satishkumar Varma, " Integration of IoT and SDN to mitigate DDoS attack with RYU Controller", Springer, ICCBI 2020 International Conference on Computer networks, Big Data and IoT
[49] Ali Alshahrani, Khaled Suwais and Basil Alkasasbeh ,Authentication method in software –Defined Network based on Ciphertext –Policy At- tributes Encryption.,International Journal of Innovative Computing, In- formation and Control, 2018.
[50] Wang, S.; Chandrasekharan, S.; Gomez, K.; Kandeepan, S.; Al-Hourani, A.; Asghar, M.R.; Russello, G.; Zanna, P. SECOD: SDN sEcure control and data plane algorithm for detecting and defending against DoS attacks. In Proceedings of the NOMS 2018—2019 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2019; pp. 1–5.
[51] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communications Review*, vol. 34, no. 2, pp. 39-53, 2015.
[52] Z. He, T. Zhang, and R.B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," *Proceedings of the IEEE 4th International Conference on Cyber Security and Cloud Computing* (CSCloud), New York, NY, USA, July 2019
[53] Yi-Wen Chen, Jang-Ping Sheu, Yung-Ching Kuo, and Nguyen Van Cuong," Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning", *2020 European Conference on Networks and Communications (EuCNC): Vertical Applications and Internet of Things (VAP).*
[54] Yang Y., Wang J., Zhai B., Liu J. (2019) IoT-Based DDoS Attack Detection and Mitigation Using the Edge of SDN. In: Vaidya J., Zhang X., Li J. (eds) Cyberspace Safety and Security. CSS 2019. Lecture Notes in Computer Science, vol 11983. Springer, Cham. https://doi.org/10.1007/978-3-030-37352-8_1.
[55] Longe Olumide Babatope, Lawal, Babatunde, Ibitola Ayobami,"Strategic Sensor Placement for Intrusion Detection in Network-Based IDS", International Journal of Intelligent Systems and Applications, vol.6, no.2, pp.61-68, 2014.

Authors' Profiles

Mimi Cherian received ME from Pillai College of Engineering under Mumbai University. B.E from K.C College of Engineering Mumbai University. Currently pursuing a Ph.D. from Pillai College of Engineering under Mumbai University. Published paper on Game theory-based network selection in 4G in ICCCCIT-2015 conferences. Firewall Optimization with Traffic Awareness using BDD in IJCIS 2016. Survey of Security Threats in IoT and Emerging Countermeasures", Springer SSCC 2018. Integration of IoTand SDN to mitigate DDoS attack with RYU Controller", Springer, ICCBI 2020.

Satishkumar L. Varma has completed his Ph.D. in Computer Science and Engineering under the guidance of Dr. S N Talbar from SGGS I E & T, SRTMU, Nanded, India in March 2013. He received B. Tech and M. Tech degrees in Computer Engineering from DBAT University at Lonere, Maharashtra, India in June 2000 and January 2004 respectively. He has over 19 years of the academic experience at Mumbai University, India. He is a reviewer in various Conferences and Journals including IEEE Transaction on Image Processing, Springer Signal, Image and Video Processing, Wiley ETRI Journal, etc. With 1 copyright, he has published 7 Book Chapters, 31 Journal papers, and more than 36 papers in referred National as well as International Conferences including IEEE, Springer, and IET with a second-best paper award at National level paper presentation competition in Threshold–2000. His research activities involve Digital Image and Video Processing, Medical Imaging, AI and Machine Learning, Soft Computing, Data Mining, and Information Retrieval.

How to cite this paper: Mimi M Cherian, Satishkumar L. Varma, "Mitigation of DDOS and MiTM Attacks using Belief Based Secure Correlation Approach in SDN-Based IoT Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.1, pp.52-68, 2022. DOI: 10.5815/ijcnis.2022.01.05