A short study on SDN-Based IOT, Security challenges and its solutions

Mohammad Saeed Ansari [a,1], Somayeh Jafarali Jassbi [a,2,*]

[a] Department of Computer Engineering, Science and Research Branch,

Islamic Azad University,Tehran,Iran

[1]ms.ansari@srbiau.ac.ir
[2]s.jassbi@srbiau.ac.ir

.

Abstract

The Internet of Things[1] has grown exponentially with many applications from industrial systems to smart homes. Heterogeneous networks with different needs that traditional networks are not able to meet. Software defined networks[2] have come to help meet the needs and challenges of this network, and the main challenges in this area, security and reliability, are solved with the help of new ideas. Different methods, such as using blockchain, have all been proposed to detect, prevent, and eliminate IoT attacks. In this paper, we review some of these methods.

Keywords: : IoT, SDN, Blockchain, Network security, Reliability

[1] IoT
[2] SDN

1. Introduction

[1] The Internet of Things is an evolving technology in which any device can be connected over a network and controlled remotely through a station. IoT devices are limited devices that have limited processing power, memory, and battery life. [2] The Internet of Things has found many applications in all fields today (Figure 1). Numerous applications have also created a Big Data due to:

- Volume: A large number of devices that generate and send a large amount of information.
- Velocity: Very high transmission rate of equipment such as sensors that are located in an environment.
- Variability: Changing a situation, such as an attack on equipment, causes changes in the pattern of sending information at different intervals.
- Veracity: Data, unlike other structures where processed data is transmitted, are transferred raw and unencrypted.
- Variety: Covers data types from a sensor temperature information to a factory control system.

Therefore, data is valuable and require proper care and processing.

Figure 1 – IoT applications and Big Data [2]

The main challenges in the field of IoT are in the two areas of security and reliability. [1] The main problem with IoT is its heterogeneity, as each system has different network requirements for optimal use. For example, in:

- Smart Vehicle Applications: Data transfer with a delay of near to zero
- Industrial networks: Both latency and zero data loss
- Video surveillance system: data latency and lost do not matter, but they want more bandwidth

These special network needs with traditional network models that have limitations in:

- Scalability
- Mobility
- The amount of traffic

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

Therefore, traditional networks are inefficient to meet the new needs of the Internet of Things. [1] A new paradigm aimed at scalability and flexibility in network management is software defined networks.

[1] Software defined networks enable traditional centralized network management, efficient configuration and optimization by transforming traditional network components, the black box, into software-controlled components, the white box. This abstraction is possible by separating the control plane and the data plane. All control functions are performed in a programmable central controller. This controller, in turn, sends packet transmission and management policies to switches and routers controlled by software defined networks, dynamically coordinating their performance and consequently, network behavior. These features make software defined networks a promising place to develop IoT solutions.

1.1. IoT security threats

[2] There are four main categories of IoT attacks:

- Spoofing attack: In this type of attack, the attacker introduces himself as a component of the network. DNS and ARP spoofing are in this category.
- Resource exhaustion attack: An attacker gains resources by putting pressure on network equipment, the most common kind of this attack is DDoS attack.
- Eavesdropping attack: Theft of unencrypted and sensitive information occurs by eavesdropping when the information being transmitted.
- Malicious application attack: A malicious program such as worms and malware at the application layer disrupts network performance.

[8] In addition to the main categorization of attacks, we can also categorize common IoT threats based on their affected layer (Figure 2).

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

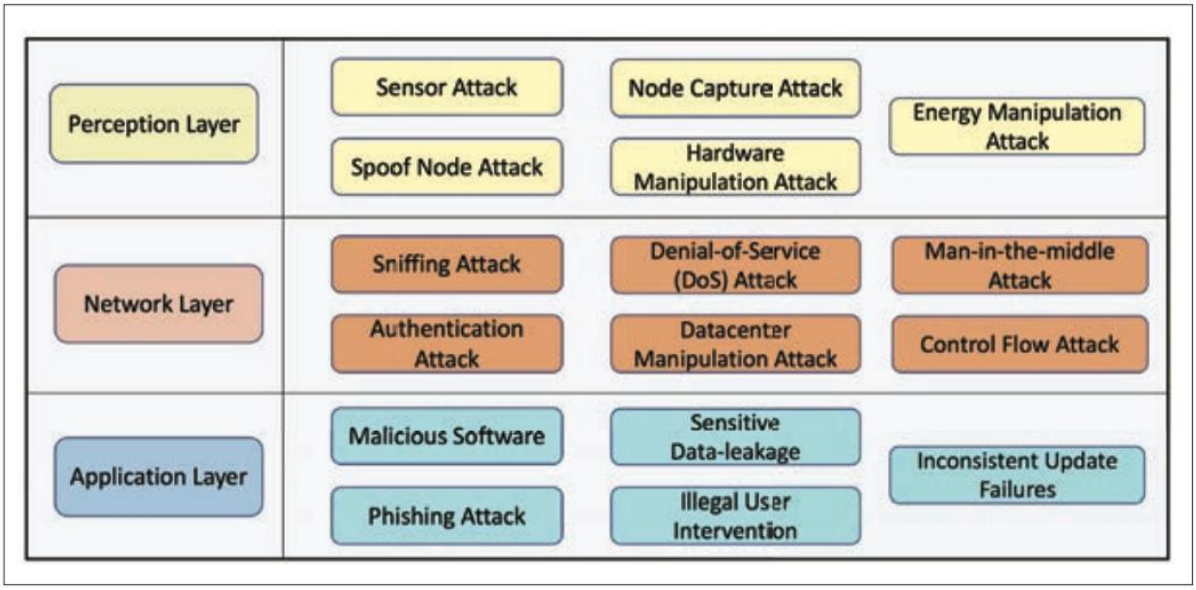

Figure 2 – Categorized common IoT threats based on their affected layer [8]

1.2. Blockchain and SDN

[5] If attackers gain access to the core data center on a software defined network, they are restricted to a specific part of the network that limits their impact. But software defined network technology alone cannot solve security issues because the integration of software defined network and cloud storage space creates DDoS attack vulnerabilities. Blockchain is another prominent technology used to solve this problem. The main feature of a blockchain is that it is very difficult to modify as soon as data is stored within the blockchain.

2. Proposed methods

In this paper, we discuss several solutions to the challenges of the Internet of Things based on software defined networks.

2.1. IBSDN solution

IPv6 expansion capability allows you to add different information. In paper [2], authentication is formed by using the IPv6 extension capability and adding an identifier for each terminal. In this method, the authentication of the ID from the origin occurs in the managed domain.

2.1.1. Main services

The proposed solution of the paper [2] has three main network services (Figure 3):

- Authentication service
- IP generation service

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

- Management policy service

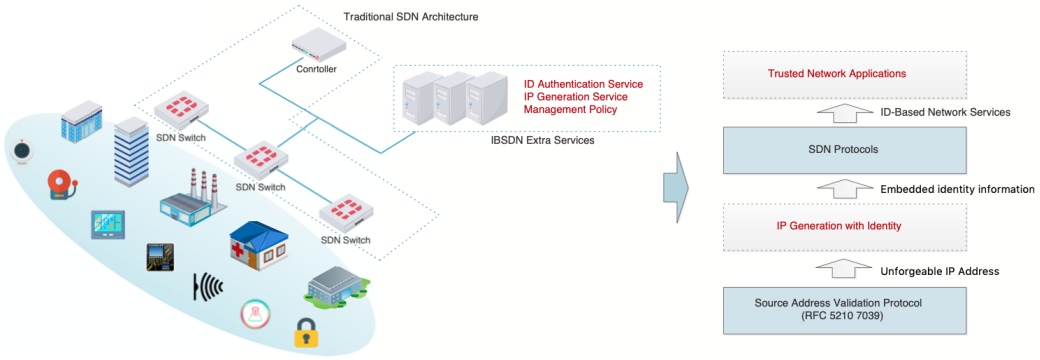

Figure 3 – Main services of paper [2]

In this method, using the source address validation protocol (RFC 5210, 7039), and creating a mapping between the ID and IP of the equipment, the necessary rules for the software defined network are created.

2.1.2. Security features

The proposed method of the paper [2] provides five main security features (Figure 4):

- Network permissions: The presence of IDs prevents malicious actions such as spoofing attacks.
- Isolation of traffic based on identifiers: Based on identifiers, heterogeneous equipment can be isolated. Therefore, access to sensitive information with traffic isolation requires higher level access.
- Network Security Monitoring: Identifiers enable monitoring of data flows at the network level. This monitoring also helps identify attacks and their patterns.
- Dynamic flow control: Identifying streams, despite assigned identifiers, improves countermeasures by creating appropriate and non-blind policies.
- Network security scheduling capability: Based on this feature, by designing programs, the understanding and maintenance of the Internet of Things network is improved.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

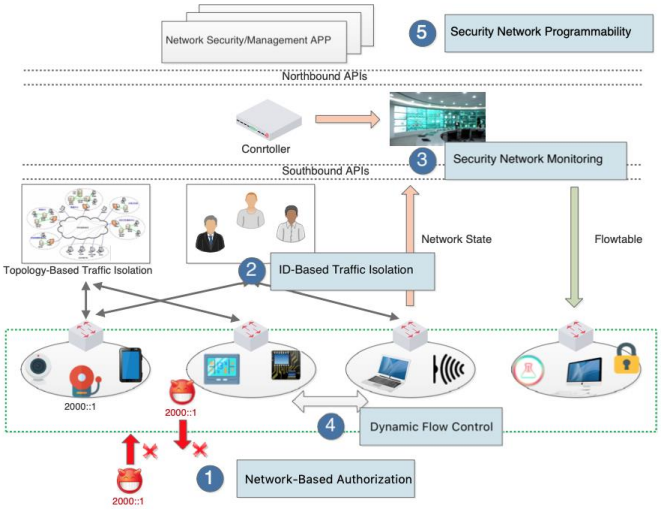

Figure 4 – Security features of paper [2]

2.2. Virtual Honeynets of IoT

[3] By diverting the attacker to Honeypot and imitated services, we will waste the attacker's time and thus gain the opportunity for necessary and mutual actions in the real system. with the help of virtualization, network applications deploy, manage and configure services and Honeypots. Traffic transfer and management between real and virtual networks is done by software defined network.

2.2.1 Main planes of proposed architecture

The proposed architecture of the paper [3] has three main planes (Figure 5):

- User plane: Policies are edited by the user on this plane.
- Security orchestration plane: Interpreters of policies, monitoring and reaction section are in this plane.
- Security enforcement plane: IoT controller and software defined network are the main components of this plane.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

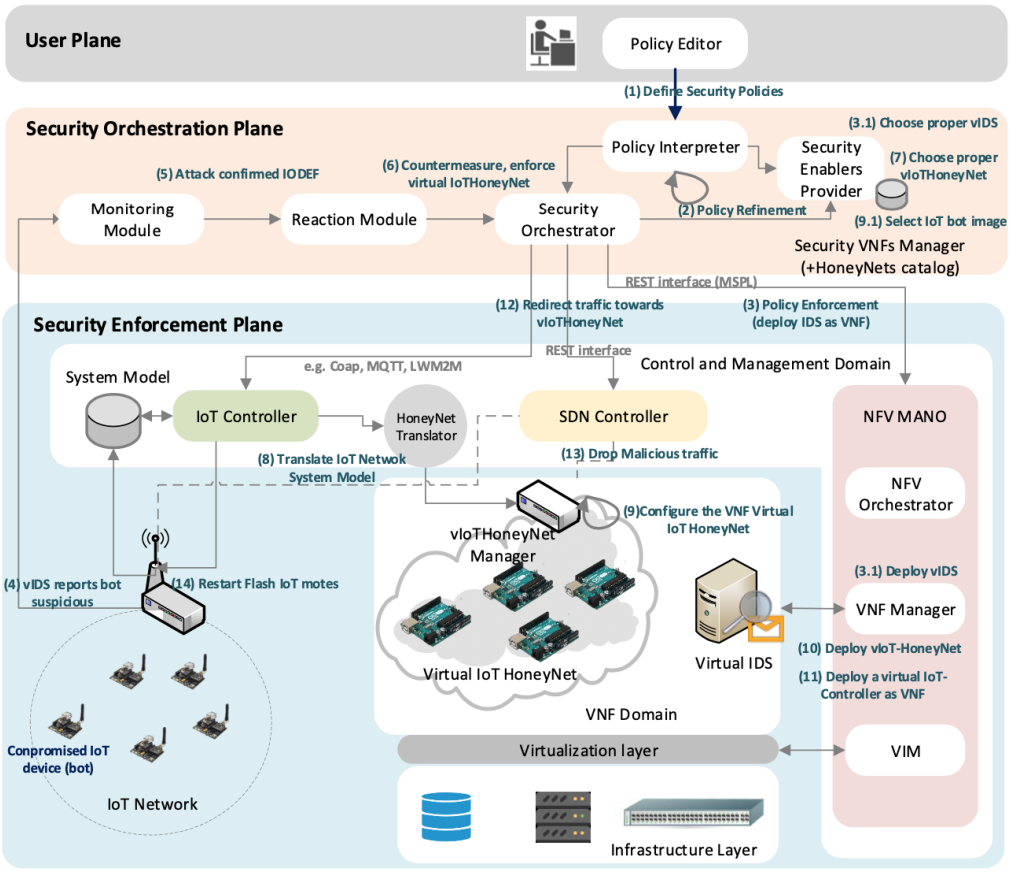

Figure 5 – Main planes of proposed architecture [3]

2.3. Secure framework for healthcare system

[4] The development of hardware technologies has made it possible to integrate artificial intelligence, the Internet of Things, edge computing and real-time decision making. The integration of AI and the IoT has created a new term called AIoT, in which IoT devices use the digital nervous system and AI as the brain of the system.

In AIoT, IoT devices limit the accuracy and speed of data transmission, while AI learns and improves on a pattern. AIoT is used in everyday tasks such as smart health, smart home and smart retail. In such applications, AIoT equipment transmits information to cloud services through edge computing for decision making.

AIoT-based health programs became popular after integrating with AI-enabled Edge computing and heterogeneous IoT networks for the optimal and timely transmission of medical information.

[4] Because in healthcare systems, IoT equipment constantly monitors patients and constantly transmits the required data, it is necessary to protect against malicious activity.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

Healthcare systems face two major problems, the permanent and secure transmission of information. One of the best ways to secure your IoT network is to use lightweight authentication. With low-power equipment, it is not possible to continuously transfer information while collecting multiple data from the patient's body. Overcoming these problems is made possible by the method of lightweight authentication and data processing near the place of their collection, using edge computing. AIoT incorporates artificial intelligence into equipment, and edge computing are used to deliver intelligence to equipment. One way to design such a system is to use a software defined network controller on the edge server or an intelligent software defined network controller to help the edge server, which balances the load and optimal use of resources.

In IoT-based healthcare systems, equipment must be authenticated before sending information. Once authenticated, the sensed data must be submitted to edge computing for fast processing. The information deposited on the edge is intelligently processed with the help of a software defined network controller that has the ability to fully program the network. Software defined network intelligence meets the needs of edge computing in terms of resource allocation and load balancing. The software defined network controller is responsible for data management, time sensitivity, edge scheduling, and fast and consistent data transfer. These characteristics are the main needs of a healthcare system that are not comprehensively presented in a solution.

In [4], to fill the existing research gap by combining these technologies, a secure framework for software defined network edge-based computing in the IoT-based healthcare system is presented. In this framework, a lightweight authentication method and edge-based computing based on a software defined network are used to balance the load between edge servers to overcome the limitations of an edge server.

2.3.1. Proposed model

Three layers are considered in the proposed model of the paper [4] (Figure 6).

- Infrastructure layer: This layer includes IoT equipment and low-power sensors, such as equipment that is attached to the patient's body or installed in a hospital. This equipment must be used efficiently with reliable information and in connection with other equipment.
- Edge computing layer: This layer is formed from different edge servers. This layer has various functions such as data transfer, storage, processing and transfer of operations between servers. This layer itself has attacks such as man-in-the-middle, reply, privacy and data integrity that impose a lot of latency and overhead on the network.
- Core computing layer: This layer has two parts: core networks and cloud services. Core networks are responsible for hosting various IoT applications and servicing and managing the IoT architecture. This layer has attack prevention mechanisms other than DoS attack. Threats to this layer are addressed through authentication, access, and encryption.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

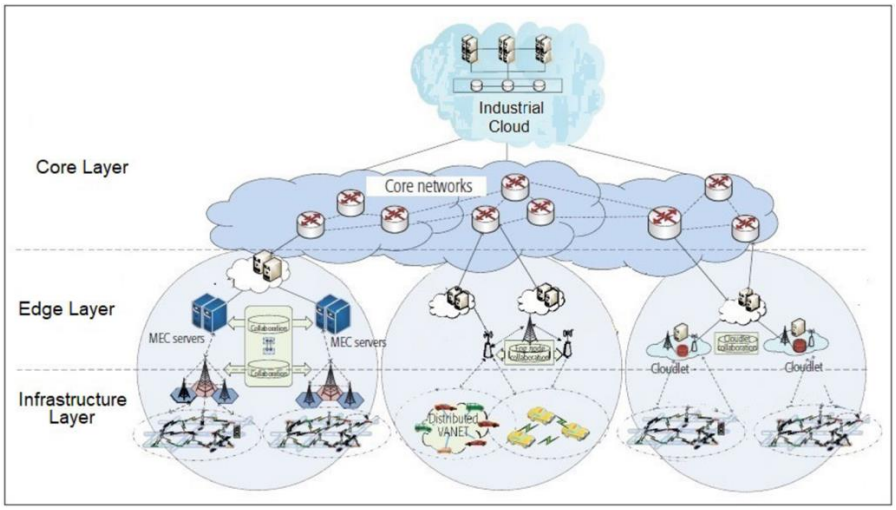

Figure 6 – Proposed method layers [4]

2.3.2. Lightweight authentication

The infrastructure layer, has no internal security mechanism. In the proposed framework, a lightweight authentication method is presented.

In this framework, communication channel specifications are extracted using p-KNN[3] and two hash functions (H1 and H2) are used to encrypt the selected specifications and modulated results. In this method, IoT equipment is identified based on operating frequency bands, access frequencies, and time slots (Figure 7).

[3] Probabilistic K-Nearest Neighbor

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

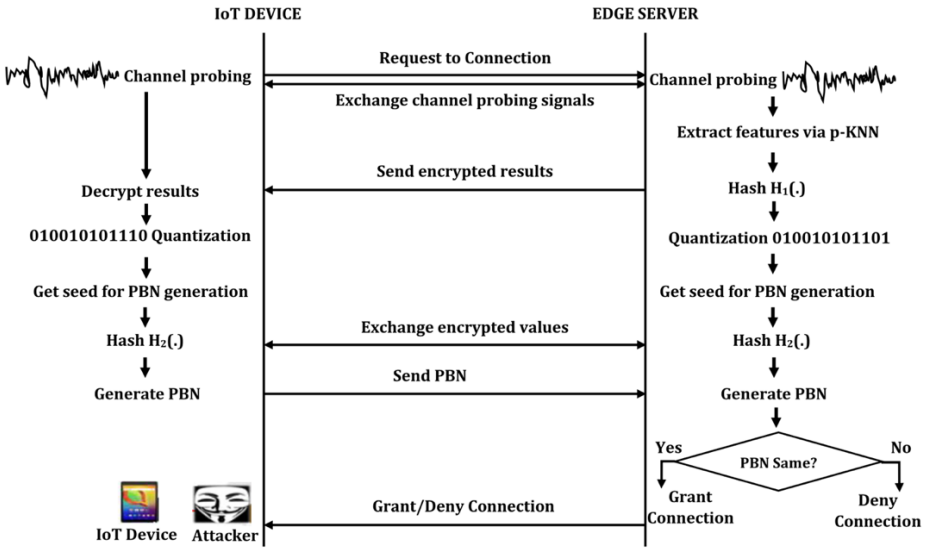

Figure 7 – Lightweight authentication [4]

2.3.3. SDN based collaborative edge computing

The edge computing layer is made up of various edge servers based on a software defined network that is responsible for intelligent data processing, storage, and interaction with other servers. The software defined network controller determines how the edge servers interact based on the load of these servers and predefined rules.

2.3.4. Task transfer process in edge servers

The task transfer process is shown in Figure 8. When a server receives a job from the patient equipment, it checks the number of tasks based on its capacity. If it has empty capacity, it does the job locally and sends a Beacon to neighboring servers. This Beacon signal contains information about the number of jobs that the sender can do. When the neighboring server has a job to run and receives this Beacon, it sends a job request and waits for the ACK. If the ACK is received at the expected time, the job is sent to the peer server, otherwise it is sent to the cloud server for processing.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

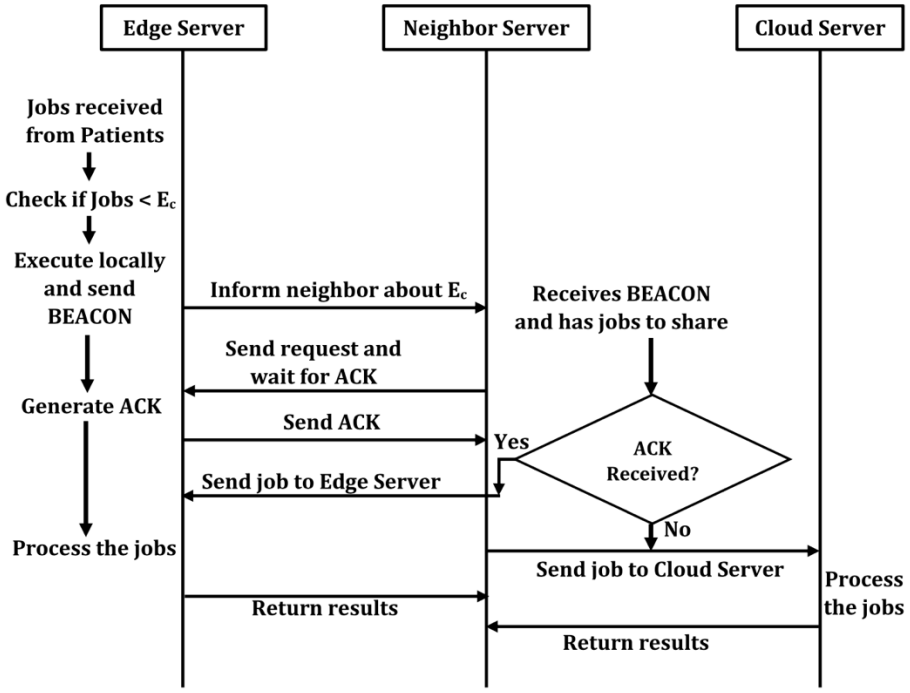

Figure 8 – Task transfer process between edge servers [4]

2.4. Near real-time security system using convolutional neural network

[1] Lack of IoT security has led to large-scale DDoS attacks via botnets. Traditional methods of counteracting these attacks have lost their use today due to the high volume of attacks. These attacks can disrupt the software defined network environment due to a central controller. Of course, Internet service providers protect the network from this type of attack by deploying DDoS prevention systems and attacking the software defined network controller.

In [1], an almost real-time security system in software defined network environments is presented to reduce DDoS attacks from internal devices such as botnets. The proposed central control system protects the software defined network against packet floods and prevents attacks from leaving the source network, which indirectly protects the victim server. This system is divided into two parts:

- Detection module: is responsible for detecting and identifying attacks that occur. This module uses a deep learning method using multidimensional IP flow analysis, called convolutional neural network. This method is widely applied to image recognition/classification problems and gives the system the ability to learn local patterns in the data set.
- Mitigation module: Responsible for selecting release policies to secure the software defined network controller.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

2.4.1. Proposed security system

The method proposed in this paper [1] mitigate software DDoS attacks by using a central software defined network controller. In this way, DDoS attacks on the Internet are mitigated by preventing attacks on external targets. The approach of this method is divide and conquer, which is formed by preventing attacks from the origin in the ISP (Figure 9).

The proposed system is based on the analysis of IP flow dimensions, using separate features to identify the pattern of normal network performance and detect the presence of DDoS attacks. To mitigate the impact of DDoS attacks on legitimate users, the proposed system works by extracting and analyzing IP stream data at one-second intervals almost instantly. This time-based analysis makes it possible to quickly detect and mitigate attacks, reduce damage to the software defined network controller (and its users), and the server being attacked externally.

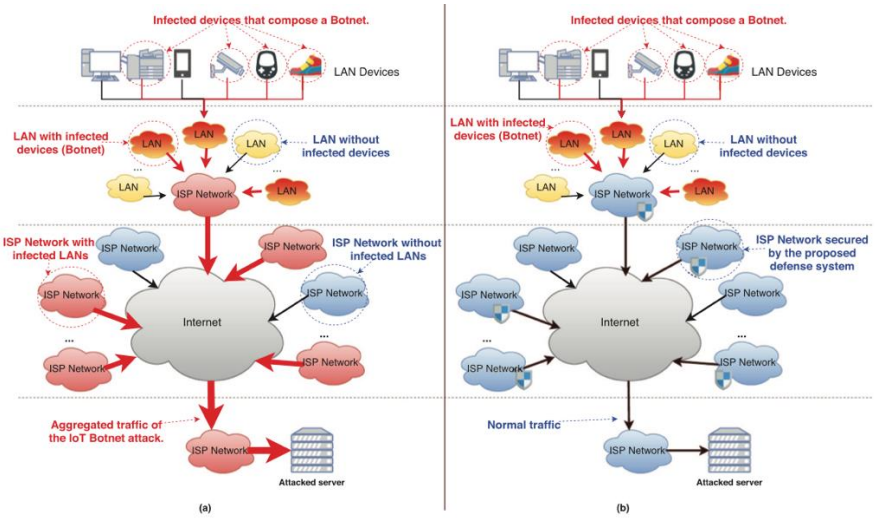

Figure 9 – Attack prevention from source in ISP [1]

The system operates automatically to detect and quickly mitigate attacks. Even if it has a notification system manager, it does not require human interaction to continue. The process diagram of the proposed system is shown in Figure 10.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

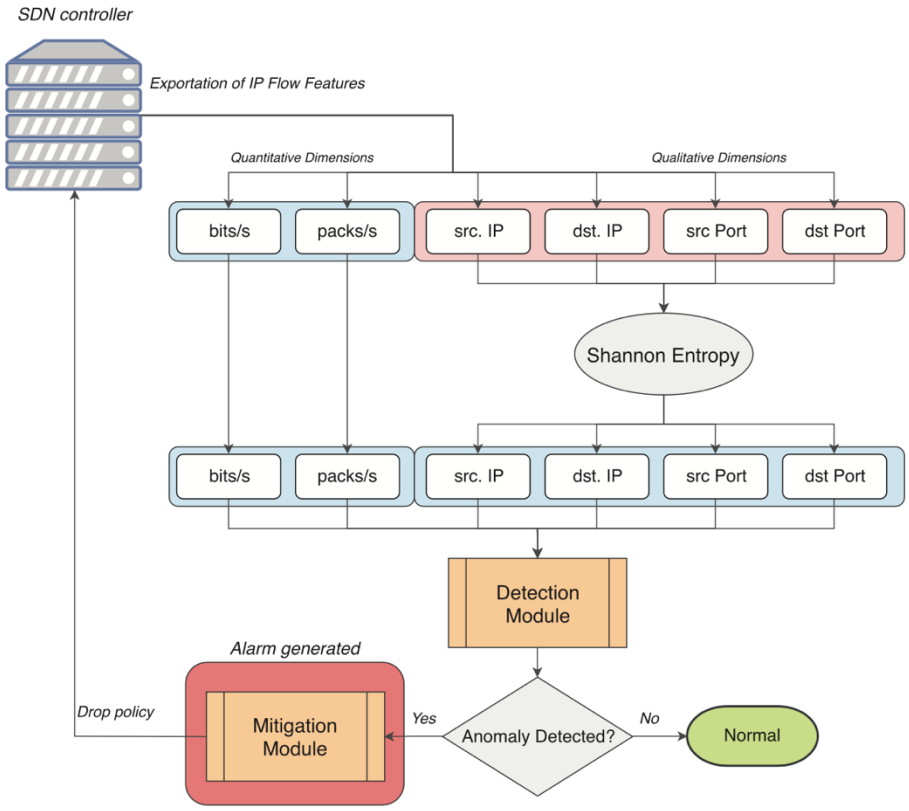

Figure 10 – Detection and mitigation module workflow [1]

As shown in Figure 10, every second the dimensions or characteristics of the IP stream are exported from the software defined network controller to the OpenFlow protocol. These are heterogeneous data dimensions that can be categorized quantitatively (such as packet rates and bits per second) and qualitatively (such as source/destination ports and IP addresses). To send dimensions to the detection section, qualitative dimensions are quantified using Shannon entropy.

Therefore, if there is a large concentration of the specific IP address of the destination, this dimension is indicated by a low entropy value. On the other hand, if there is a large scatter in the data related to the same dimension, a higher entropy value is retrieved.

The analyzed dimensions are sent to the detection section to analyze and detect the occurrence of a DDoS attack. If an attack is detected, the mitigation section is activated and creates a counter policy that must be entered by the software defined network controller. Figure 11 shows the relationship between system components.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

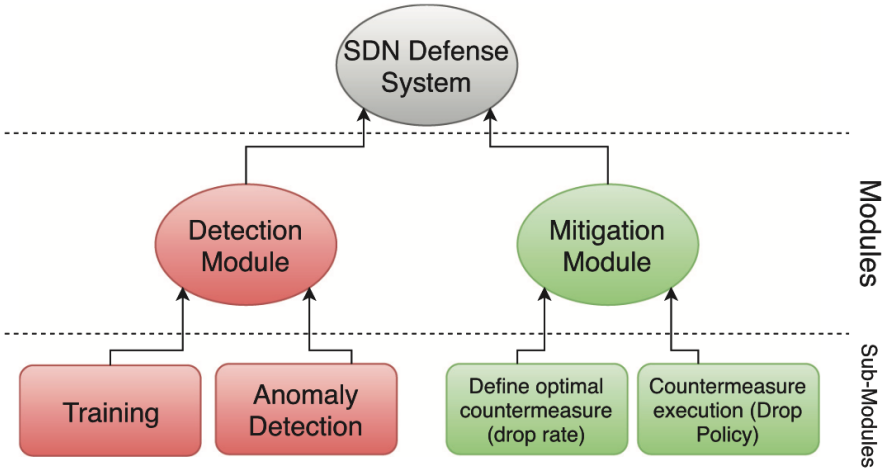

Figure 11 – Sections relation [1]

Training section in the Detection section, calibrate by neural network and previous data and attacks are detected by anomaly detection. The mitigations section after detecting an attack, by making a decision, mitigate the attacks. The mitigation section has two subsections. The first part, with a game theory approach, optimally calculates the necessary rules that apply to the software defined network router. Attacks may not directly target the performance of the software defined network, but traffic through the central controller can disrupt it. The output of this subsection is the optimal release rate of the package. Finally, the second subsection sends the policies created by the first subsection to the central controller of the software defined network to be implemented.

2.5. Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network

[5] Today, cloud storage space is recognized as one of the key resources provided by cloud computing in which data is stored on a remote server and can be retrieved from the server via the Internet. Cloud storage is divided into four categories: personal, public, private, and hybrid, and works under four layers: access, usage, management, and storage. Cloud computing allows users and businesses to store data in the cloud, which can raise security concerns such as data protection, privacy, and data integrity.

The main feature of a blockchain is that it is very difficult to modify as soon as data is stored within the blockchain. Each block contains some data, the hash block and the previous block hash, and the transactions section. The hash is basically used to identify the block with all its content and is unique. This way, transaction data is stored securely in the transaction section.

[5] The basis of the analysis of previous studies is the following:

- Software defined network can be used to reduce security issues within the network.
- Blockchain is used in conjunction with a software defined network to better protect the IoT network.
- Blockchains for data sharing with cloud storage can be integrated.
- Prior solutions can provide some security, confidentiality, stability, and scalability.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

Block-SDoTCloud is a robust architecture for storing data inside the cloud that requires less computing power than other methods. In this model, software defined network technology prevents cyber-attacks and blockchain technology maintains confidentiality and trust within the network. Also, the DDoS security threat is mitigated due to the use of blockchain technology. In general, this architecture provides data security and confidentiality better than other methods.

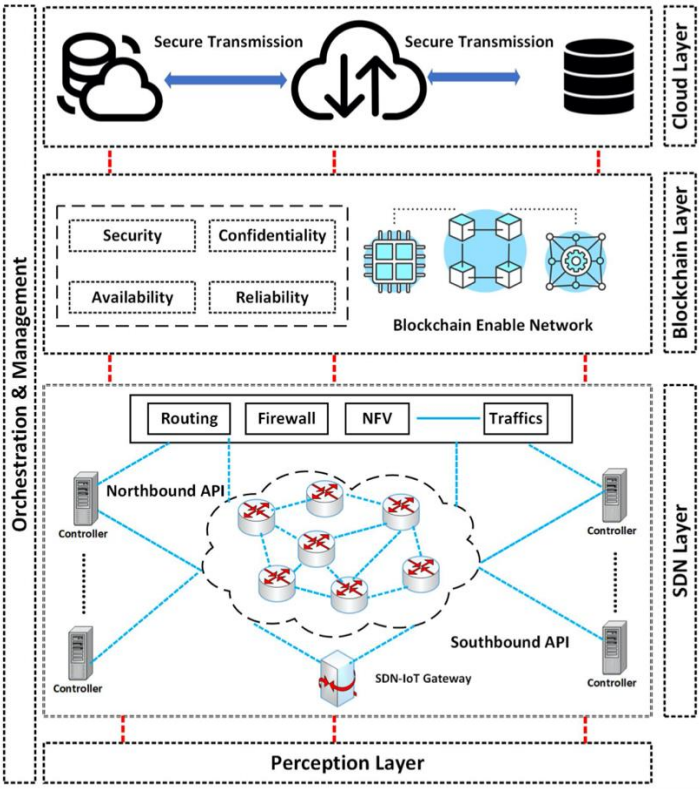

Figure 12 – Proposed architecture [5]

The architecture and layers of the proposed solution of the paper [5] are shown in Figure 12.

2.5.1. Perception layer

The perception layer is at the lowest level of the target architecture, and this layer understands real-world data. This layer interacts directly with the environment in which the use of the Internet of Things is implemented. Almost all sensors and data collection equipment are connected at the perception layer. In this layer, the sensor elements collect data in real time and deliver the information to the software defined network protocol for further processing. The data collected by this layer is identified and transmitted by relative identification.

2.5.2. Infrastructure/Internet networks layer

Data transmission devices such as switches, routers, etc., can transmit data through software defined network gateways. IoT device data is managed through a dynamic software defined network controller and through the

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

OpenFlow protocol. The model proposed in paper [5] allows data to reach the target layer securely. IoT data is stored internally or externally in the cloud storage platform of blockchain networks for added security after being organized in the software defined network.

2.5.3. SDN based security in cloud

Software defined networking can control security threats, new threats, and various types of attacks, unlike the current network model. The software defined network consists of data, control, and application planes.

2.5.4. Blockchain approach

A blockchain is a special type of ledger or database that can distribute and resist risks while adding different operations. Blockchain can efficiently provide access control and security to the system and keeps transactions in a secure ledger. The blockchain does not use a database or central storage to store user activity.

Each block can consist of exactly several transactions. In addition, a hash chain is grouped in each block. Each block contains a timestamp, data, current hash, and previous data such as interference-prone transactions. Under these circumstances, it is clear that blockchain technology can be used in the architecture of paper [5] to ensure access control in the proposed cloud storage structure. The result of this approach is extensive security and unparalleled access efficiency policies.

2.5.5. Cloud storage and services management

In paper [5], the proposed model improves the various services in the cloud storage environment, based on the distributed blockchain approach. Blockchain-based software defined network architecture provides advantages such as flexibility, accessibility, security, privacy, and accurate storage of numerous resources in the cloud storage platform. Blockchain alone, without the cooperation of a software defined network, cannot provide reliability, highly stable and centralized controllers, and also increase the load balancing ability in the proposed architecture.

2.6. Blockchain based secure IoT data sharing framework for SDN-enabled smart communities

[6] The software defined network separates the data plane and the control plane through a software defined network controller and provides users with network programming capabilities. However, when IoT devices share data on a software defined network, the software defined network presents challenges in data security:

- The software defined network controller is centralized and suffers from a potential point of attack such as DoS. Attackers can control compromised and unauthorized IoT devices to infiltrate the software defined network controller and cause leaks.
- The application layer in the software defined network allows vendor applications to manage and configure network resources. When the software defined network does not set appropriate access policies for these applications, it may cause inadequate access to network data and threaten data security.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

Therefore, increasing the security of information in the software defined network is very important when sharing data on IoT devices. To meet this security challenge, the proposed design of the paper [6] uses blockchain technology and an initial cryptography called PRE[4].

Records in the blockchain are traceable and cannot be manipulated. Consortium blockchain is one of the three types of blockchain which has certificate authority to allow members in the blockchain network. Blockchain integration with software defined network is able to solve centralized software network problems. Therefore, in paper [6], blockchain technology is used to manage the identity of IoT devices in smart communities, which can increase the authenticity of the devices and reduce the risk of an attack point.

PRE is a basic public key encryption method in which a data owner can delegate the ability to decrypt their data to other data requesters. After a semi-secure proxy re-encrypts the password of the owner key in the public key, a data requestor can decrypt the new password via its secret key. The IBPRE[5] method is a type of PRE in which data holders and applicants take their identity as the public key and no longer need the public key infrastructure.

In paper [6], the IBPRE algorithm has been selected for three reasons:

- The IBPRE scheme effectively ensures the security and privacy of data sharing between both heterogeneous and unreliable network entities. Therefore, this scheme is suitable for sharing data between devices in smart communities equipped with software defined network.
- The equipment encrypts its data by IBPRE and stores it on cloud servers. They do not need to load encrypted data when sharing with other devices, which simplifies the data sharing process compared to other schemes.
- IBPRE is a PRE enhancement that gets rid of PKI and facilitates certification management in PRE.

The IBPRE method requires a private key generator to authenticate users. If curious or malicious members gain access to the control of the private key generator, they will be able to access user data. To solve this problem, blockchain is used to manage device data encryption keys and record access keys to understand responsibility and increase security.

[4] Proxy Re-Encryption
[5] Identity-based Proxy Re-Encryption

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

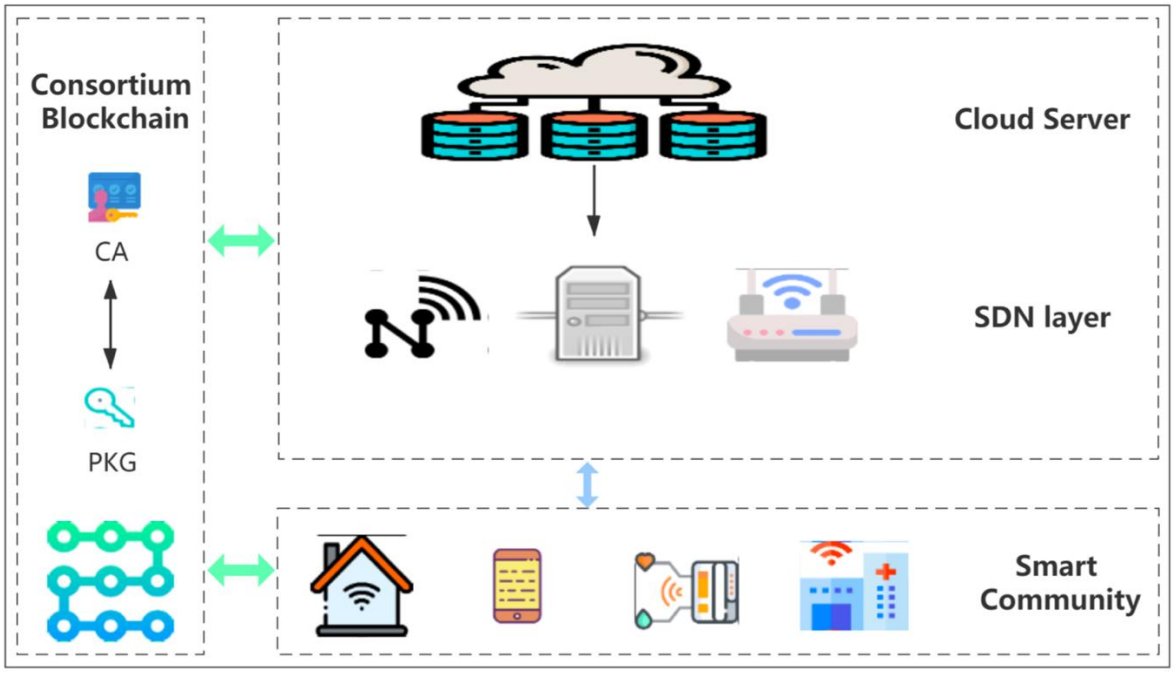

Figure 13 – Proposed framework [6]

Figure 13 shows the proposed framework of the paper [6]. This framework consists of three parts:

- Smart community
- Cloud with software defined network capability
- Blockchain network

At the bottom of the framework are smart communities such as smart homes, smartphones, wearables, sensors and smart healthcare.

Cloud with software defined network capability consists of cloud server and software defined network layer. The cloud server includes some of the central servers of cloud service providers and network operators that provide computing and storage resources for IoT devices. The software defined network layer is enabled with the software defined network controller and provides a programmable network with some protocols, such as OpenFlow.

The blockchain network integrates an IBPRE algorithm to ensure the security and privacy of user device data. Except for two devices, no other third party can obtain useful information from the encrypted data. The blockchain network securely manages the encryption key in the IBPRE algorithm. In addition, the blockchain records the entire process of data sharing between two devices. The data in the blockchain is transparent, controllable and traceable.

There are usually three types of blockchain:

- Public blockchain: Allows people around the world to access and interact with it.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

- Consortium blockchain: Used in associations that consist of several companies or organizations and has a certification body to verify the identity of the participants and grant them access control.
- Private blockchain: Accepted by an internal company or team.

In the proposed framework of the paper [6], Hyperledger Fabric, a kind of consortium blockchain, is considered as a blockchain network.

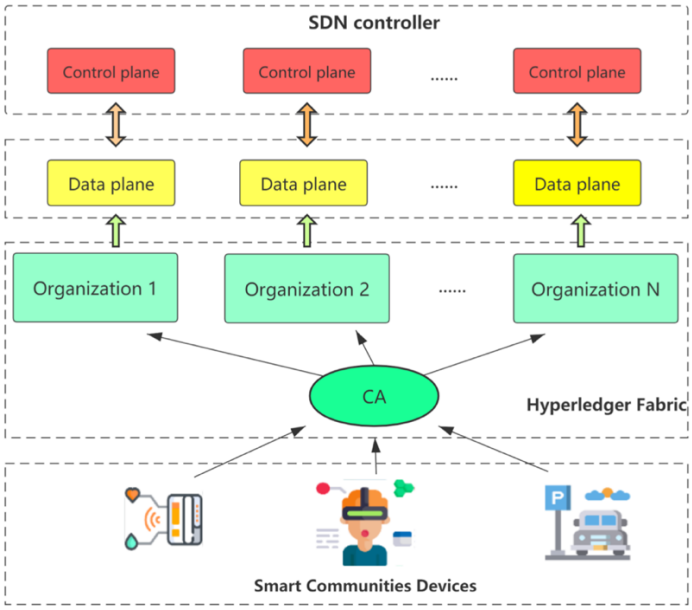

Figure 14 – Process of IoT devices registration and validation [6]

Figure 14 shows the IoT device registration and validation process in Fabric CA to improve software defined network security. In smart communities, software defined network techniques control numerous IoT devices and provide streaming services. However, the software defined network controller is vulnerable to a single attack such as DoS or DDoS from devices in smart communities. In paper [6], the blockchain authorized all devices through the certificate authority. All smart community devices must register with Fabric CA to receive their certificates and keys in order to improve authentication and reliability when logging in. This will overcome the problem of DoS attacks on the Internet of Things. In addition, the blockchain controls and records the process of data sharing between two IoT devices. whenever a device wants to make a smart contract in a blockchain, the certificate authority checks that device's membership. Some of the contracts designed in this scheme check the caller's certificates to see if the caller's identity matches the parameters of the contract.

2.7. A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks

[7] Existing IoT models, such as cloud-based security infrastructures, are unable to maintain IoT security and privacy due to resource constraints and flexibility. This weakness exposes IoT equipment to attacks of counterfeiting and upgrading privileges. An attractive alternative is the blockchain, which provides a decentralized infrastructure to counter DDoS attacks and single point of failure risk.

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

Blockchain is seen as the infrastructure for many IoT applications:

- Energy sales
- Ensure fair payment in smart grids
- Electric vehicles
- Monitoring the quality of the environment in the smart city
- Trusted healthcare systems

In addition to the benefits mentioned, the blockchain is not financially viable due to the high power consumption by the miner. Also, due to the unchanging design of smart contracts, updating their software code or security patches becomes difficult or impossible.

Software defined networks help meet IoT needs by delegating computing to the cloud and the edge of the network. Also, software defined networks deliver flows to the destination and meet QoS requirements when nodes fail due to load conduction and distribution.

The paper [7] presents a blockchain-based architecture for securing IoT transactions by implementing decentralized software-aware applications on software defined networks that listen to miner nodes, reporting suspicious IPs, and authenticating unknown packets. This architecture introduces the PoA[6] consensus algorithm that detects suspicious IoT devices and reports them under smart contract. Contrary to the approaches of previous studies, the solution of this paper assigns IP blacklists to virtualized functions within the Docker.

2.7.1. System design

The proposed solution architecture of the paper [7] consists of four different layers. First, the peer-to-peer network layer is a blockchain that uses IPFS to store and share data in a distributed file system. Blockchain nodes, miner and customers, use IPFS to work with smart contracts and blockchain transactions.

The second part includes the virtualization layer and the abstract layer of the network control service. The virtualization layer provides the blockchain on Kubernetes as infrastructure as code, so that applications are stored inside Docker containers on multiple physical hosts. This layer also provides many management features to facilitate the setting of VNFs. On the one hand, these virtual appliances host decentralized customer blockchain nodes in the form of lightweight containers (such as Pods) that connect to the main blockchain network to make contract-based decisions with each other. On the other hand, they communicate with blockchain applications (such as DApps) via ABI over RPC to interact with smart contracts. Smart contracts are self-executing contract objects that facilitate interaction with blockchain nodes to exchange data securely and without conflict.

2.7.2. Flow management

Figure 15 shows the details of flow management between different layers. The blockchain layer in this architecture consists of several units:

[6] Proof-of-Authority

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

- Identification unit: manages user/node access using public and private keys. IoT nodes receive addresses using the last 20 bytes of the 32-bit public key, which is also used in the node account to receive and send transactions.
- AAA Unit: A unit for authentication, granting access and maintaining accounts based on blockchain. Nodes can access the infrastructure services according to a specific scenario, using the special account given to them, and through the blockchain API, reserve the required resources and execute the transaction. Authentication is based on identities to prevent authentication and protect the data and control page from intrusion to ensure that malicious attacks do not interfere with the controller configuration.
- Traceability unit: This unit is responsible for fully following the transaction process from the originator node to all processes on the blockchain infrastructure.
- Smart contract unit: is responsible for the interaction between contract functions and IoT nodes from creation to implementation.

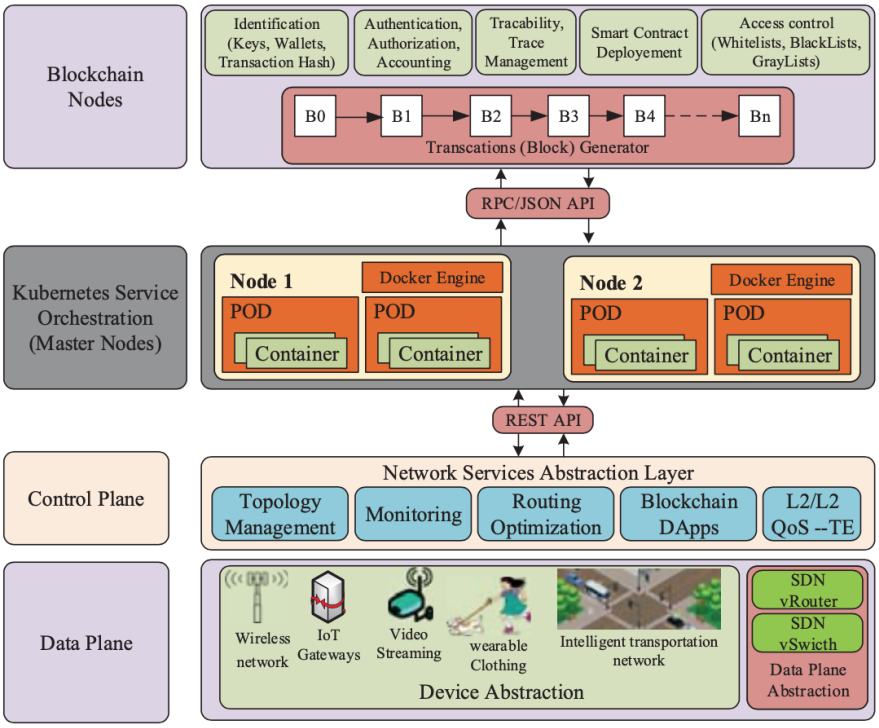

Figure 15 – Flow management between layers [7]

2.7.3. Smart contract design

[7] The smart contract is made up of 400 lines of code. Reporting all misbehavior, in addition to MAC and IP, includes IP nodes affected. The SuspectBehavior data structure is used to detect and the Report data structure is used

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

to report misbehavior to the software defined network controller. A blockchain-based validator checks the validity of connected IoT equipment. Detects the source and destination of incoming traffic based on OpenFlow messages. The software defined network controller provides an overview of the network, including the state of the structure and details of transactions, based on information contained in the OpenFlow package header. Accordingly, using packets exchanged between IoT and network equipment, it detects any malicious operations and creates a black and white list of equipment.

2.7.4. Consensus Algorithm

In the paper [7], the number of N trusted nodes is selected using the PoA algorithm. To enforce network security, PoA pre-selects a number of IoT-eligible nodes to validate transactions under strict rules. Nodes are first selected based on QoS parameters such as more bandwidth, less latency, and more hardware resources. These nodes can themselves select a limited number of headers that have a set of authority to maintain and operate the network.

The proposed framework of the paper [7], using the identity of pre-selected nodes, pays more attention to the validity of a node than the Bitcoin PoW[7] algorithm and Atrium PoS[8] algorithm. This approach gains more decentralization efficiency while requiring less computing power.

3. Conclusion

In this paper, we reviewed several papers and their proposed solutions for security challenges of the Internet of Things. All methods try to:

- Detect,
- Prevent and
- Mitigate attacks

This study shows that Integration of software defined network, blockchain and IoT can mitigate network attacks and can be customized for constrained IoT devices. Performance analyzes of each paper show that proposed lightweight solutions can be used with low overheard and performance impacts.

This effort increases the security and reliability of IoT networks based on software defined networks.

As suggestions for completing the proposed solutions, in the form of future work, the following can be considered:

- Redundancy for software defined network controller to solve single point of failure problem
- Use a variety of deep learning methods to detect attacks
- Adding different methods of monitoring and reporting in detecting attacks
- Extend methods to all IoT protocols such as IPv4 and ZigBee
- Combining the idea of using blockchain with fog and edge computing technologies
- Use the power of edge computing in system processes instead of using the cloud

[7] Proof-of-Work
[8] Proof-of-Stack

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021

- Comparison of PoA consensus algorithm in blockchain based solutions with other algorithms

4. References

[1] Marcos V.O. de Assis et al., "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network," Computers & Electrical Engineering, vol. 86, pp. 106738, 2020

[2] X. Wang et al., "ID-Based SDN for the Internet of Things," IEEE Network, vol. 34, no. 4, pp. 76-83, July/Aug 2020

[3] A. M. Zarca et al., "Virtual IoT HoneyNets to Mitigate Cyberattacks in SDN/NFV-Enabled IoT Networks," IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1262-1277, June 2020

[4] J. Li et al., "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System," in IEEE Access, vol. 8, pp. 135479-135490, 2020

[5] A. Rahman, M. J. Islam, M. Saikat Islam Khan, S. Kabir, A. I. Pritom and M. Razaul Karim, "Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network," 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1-6

[6] Y. Gao, Y. Chen, H. Lin and J. J. P. C. Rodrigues, "Blockchain based secure IoT data sharing framework for SDN-enabled smart communities," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 514-519

[7] A. Hakiri, B. Sellami, S. Ben Yahia and P. Berthou, "A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks," 2020 Global Information Infrastructure and Networking Symposium (GIIS), 2020, pp. 1-4

[8] Mishra, Pritish, Ananya Biswal, Sahil Garg, Rongxing Lu, Mayank Tiwary, and Deepak Puthal, "Software Defined Internet of Things Security: Properties, State of the Art, and Future Research", IEEE Wireless Communications 27, no. 3, pp. 10-16, 2020

DOI: 10.5281/zenodo.5188651
Received: January 12, 2021 Accepted: July 10, 2021