Int. J. Communications, Network and System Sciences, 2023, 16, 169-190
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

A 5G Perspective of an SDN-Based Privacy-Preserving Scheme for IoT Networks

Isaac Appiah[1*], Xiaoming Jiang[1#], Edward Kwadwo Boahen[2,3], Ebenezer Owusu[4]

[1]Department of Computer Science and Technology, Jiangsu University, Zhenjiang, China
[2]Department of Computer Science and Engineering, Jiangsu University, Zhenjiang, China
[3]Department of Computer Science, Ghana Communication Technology University, Accra, Ghana
[4]Department of Computer Science, University of Ghana, Accra, Ghana
Email: [#]jxm@ujs.edu.cn

How to cite this paper: Appiah, I., Jiang, X.M., Boahen, E.K. and Owusu, E. (2023) A 5G Perspective of an SDN-Based Privacy-Preserving Scheme for IoT Networks. *Int. J. Communications, Network and System Sciences*, **16**, 169-190.
https://doi.org/10.4236/ijcns.2023.168012

Received: September 28, 2022
Accepted: August 14, 2023
Published: August 17, 2023

Abstract

The ever-increasing needs of Internet of Things networks (IoTn) present considerable issues in computing complexity, security, trust, and authentication, among others. This gets increasingly more challenging as technology advances, and its use expands. As a consequence, boosting the capacity of these networks has garnered widespread attention. As a result, 5G, the next phase of cellular networks, is expected to be a game-changer, bringing with it faster data transmission rates, more capacity, improved service quality, and reduced latency. However, 5G networks continue to confront difficulties in establishing pervasive and dependable connections amongst high-speed IoT devices. Thus, to address the shortcomings in current recommendations, we present a unified architecture based on software-defined networks (SDNs) that provides 5G-enabled devices that must have complete secrecy. Through SDN, the architecture streamlines network administration while optimizing network communications. A mutual authentication protocol using elliptic curve cryptography is introduced for mutual authentication across certificate authorities and clustered heads in IoT network deployments based on IoT. Again, a dimensionality reduction intrusion detection mechanism is introduced to decrease computational cost and identify possible network breaches. However, to leverage the method's potential, the initial module's security is reviewed. The second module is evaluated and compared to modern models.

Keywords

Internet of Things, 5G, SDNs, Security and Privacy, Intrusion, Network Communications

[*]First author.
[#]Corresponding author.

1. Introduction

Internet of Things (IoTs) network concerning the next generation is nearing the end of its development cycle, paving the way for large-scale global implementation. Smart and sustainable communications may profit from technical advancements in the technology sector, such as usage-based insurance and greater income through IoT data monetization. This includes IEEE 802.11p, long-term evolution (LTE), the 5G Narrowband Internet of Things (NB IoT) [1], and Wi-Fi [2]. These technologies, however, have challenges in terms of data rates, latency, dependability, and, more importantly, connectivity due to a scarcity of spectrum and a complex surrounding environment. Furthermore, with the rising resilience of connected IoT devices, the IoTs network faces many issues, including high bandwidth requirements. The fifth generation (5G) networks were created to meet the stringent needs of IoT networks. Due to its spectrum coherence and energy economy, it is predicted to boost system capacity by 1000 times, data rate by 10 - 100 times, battery life by ten times, and latency by five times compared to 4G [3]. As a result, 5G-based IoT Networks may overcome the issues posed by the enormous demands and data flow generated by connected devices. Despite its various benefits, 5G networks confront challenges in offering ubiquitous and dependable IoT connections. As a result, a contemporary network technology, software-defined network (SDN), has evolved to provide intelligence, resilience, and flow programmability into 5G IoT networks [4]. It enhances the capability of 5G networks while supporting the dynamic nature of IoTn. To conceptually concentrate the network state and intelligence in SDNs, data and the control plane are decoupled from each other [5]. On the data plane, all forwarding devices (FDs) are gateways, switches, and routers that use the OpenFlow (OF) protocol. The control plane is responsible for data routing and allocating resources. Executing SDN controller directives, the control plane is also instrumental in providing information on security, identity, authentication, and mobility to the network [6] [7]. SDN has been connected with VNs in some preliminary studies to improve their flexibility, programmability, and efficiency. For example, [8] presented an IoT architecture based on 5G and SDN, in the Hidden Pattern (THP), which combines A visible password and a digital challenge value are used together to guard against various kinds of authentication threats. Researchers in [9] integrated NFV and SDN management of IoT bootstrapping for large networks. Finally, [10] discusses applications and domains of the Internet of Things It's simple to see rising patterns because of the standardized IoT-SDN systems implemented between 2012 and 2016. IoT has two major issues as a result of the intrinsic nature of wireless communications: security and privacy. A comprehensive and widespread communication architecture is thus essential to provide a reliable flow of information. Authentication plays a key role in this direction, offering a potential solution for future virtual networks. In the literature, authentication procedures include anything from hash-based techniques to pseudo-random number methods, as well as both private and public key cryptology [11] [12]. Furthermore, potential security flaws in IoT networks could lead to attacks like black holes, selective forwarding, packet duplication, wormholes, Sybil attacks and resource exhaustion. As a result, security must be built into such programs in order to preserve the data's integrity and ensure its correctness. Intrusion detection systems (IDSs) have demonstrated their effectiveness in detecting suspected events designed to disrupt network communication in this area [13] [14]. In order to solve security challenges in virtual networks, several IDSs have been developed in the literature [15] [16]. Despite the fact that numerous strategies for preserving IoTn's data integrity and accuracy are still issues that haven't been completely addressed in the literature, despite several proposals to this effect. Hence, we proposed a unified architecture based on software-defined networks (SDNs) that provides 5G-enabled IoT networks, with complete confidentiality.

The following are the major contributions of this research: 1) Authentication and intrusion detection is used in a composite architecture to enable end-to-end encryption in 5G-SDIoTN deployments. By demanding joint authentication amid the involved organizations before data transmission can commence, the former helps to identify any breaches in the underlying network.

2) It is the ECC concatenation, one-way hash, XOR and multiplication operations that underlie the authentication module's effectiveness. Furthermore, it is unique in that the certificate authority (CA), cluster head (CH), and IoT devices are all mutually authenticated.

3) Our suggested intrusion detection scheme takes advantage of pre-processing the raw dataset, tensor-based dimensionality reduction, with a Fuzzy C-means (FCM) clustered to detect intrusions. Our subsystem is unique in that it handles the clustering issue effectively using multi-objective dynamic programming with decomposition (MOEA/D). The proposed intrusion detection scheme's performance is also improved by reducing the dimensions using tensor-based.

The following is the structure of the rest of the manuscript: Section 2 discusses the relevant work. In Section 3, the suggested scheme's system model in the context of IoTNs backed by SDN and 5G is presented. Section 4 examines the developed authentication module, followed by Section 5 intrusion detection system (IDS). In Section 6, the corresponding simulation output is plotted against the current state of technology. Section 7 wraps up summarizes the results and makes suggestions for more investigation.

2. Related Work

In this segment, we will provide a quick overview of the relevant work presented by the scholars along certain areas. The existing techniques have been divided into two categories for clarity's sake: authentication of protocols in SDNs and models for detecting intrusion for IoT networks.

[17] presented a secure SDN deployed across a network of nodes architecture for IoT using the blockchain technique (DistBlockNet). The researchers stated that

their proposed model follows the requirements when it comes to creating a network architecture that is both safe and scalable. In the DistBlockNet IoT architectural concept, SDN and blockchains combine their benefits. Although the researchers claim their model outperformed the existing schemes, their model failed to include authentication protocols concerning the IoT networks. In [18], communication with or without the infrastructure known as an SDN domain is now possible, according to researchers. There was a single domain in their concept that had a wired, a wireless, and Ad-Hoc network. Border Controllers are used to facilitate communication across domains in their suggested approach. In the event of a failure, the Border Controllers must work together in a novel distributed way to ensure that each domain remains independent. The researchers claim their proposed model ensure the network's reliability as a whole. However, their model failed to tackle the computational cost and authenticate the protocols involved.

[19] proposes the use of edge computing to allow an external service provider to offer scalability for a Blockchain as a Service (BaaS) to address the additional attack vectors provided by an increasing number of linked susceptible devices connected to the network, along with a severance between the control and data planes of SDN By using an efficient, edge-distributed blockchain system, the suggested approach validates the added flows. Their results demonstrated the suggested algorithm's potential to optimize the combined earnings of BaaS plus SDN operators in relation to IoT networks. However, the researchers indicated that they would consider the numerous flow conformance rules that might be applied in a smart contract for future use. The authors [20] proposed IoT network intrusion detection and prevention system (IDPS) based on software-defined networking (SDN). An IoT network and collocated fog computing are at the heart of their design, which gives the proposed IDPS the ability to detect numerous attack types in near real-time and neutralize them with SDN-controlled efficiency. The researchers claim their model is more effective than the traditional techniques of IDPS in IoT networks. However, the model also failed to tackle the computational and scalability of the intrusion system.

In [21], an SDN-based autonomous security architecture based on blockchain technology is given for the IoT environment. This research intends to reduce current problems and identify assaults more effectively. It makes use of blockchain technology to dynamically update the threat detection framework and reward fog nodes based on "Proof-of-Work." However, their work did not take into concentration the authentication of the protocols involved. [22] propose a blockchain-based controller to protect against fraudulent flow rule injection, with an emphasis on SDN controller authentication. Although their proposed model effectively authenticated the SDN controller, the scalability of their model is in question, and their model could not resolve the problem with intrusions.

[23] introduce a new system to eliminate the need for recurrent re-authentication across heterogeneous cells in 5G, a new authentication handover using blockchain in an SDN-based 5G network is proposed. The researchers claim their model

outperformed the existing traditional models but failed to include the aspect of the intrusion detection system. Qiu *et al.* investigate the Industrial Internet of Things paradigm with several SDN controllers. To gather and synchronize network-wide views across multiple SDN controllers, a blockchain-based consensus system is described. The Q-learning approach is used in this study to simultaneously optimize view modification, access selection, and computing resources. Although their model was effective, it failed to address SDIIoT nodes and controllers' trustworthiness may be assessed in a number of ways. The researchers stated the limitations of measuring the trust features in their future work.

Although the above-related literature effectively performed its task they failed to resolve the above limitations as stated, hence, we propose a composite architecture that combines two sets of security modules to enable end-to-end security in 5G-SDIoTN deployments.

3. System Model

This section discusses the VN that is considered in SDN configurations that is 5G technology-enabled. The envisioned IoTN is supposed to be guarded with cutting-edge 5G and SDN technologies. A more comprehensive version of the scheme is seen in the concept [7]. The control plane's SDN takes responsibility to enforce global rules such as intrusion detection, routing, authentication, and mobility management; whereas the data plane is composed of base stations/access points (BSs/APs) that execute the controller's logic. Additionally, the participating IoT devices form clusters depending on their speed, direction of travel, and other parameters. Additionally, a cluster head (CH) is selected from inside before executing the control layer's logic.

The following facts concerning SDN and BS are related:

Base Stations (BS): In the arrangement discussed, each assumption is that BS hasan implementation function and a database (Local Database (LODB)) server. It holds data about the IoT devices in their local proximity (sometimes called their cell), as in their unique identification numbers, geographical coordinates, traffic demands, and transmission regulations. The LoDB is updated whenever IoT devices are active with regard to the BS. The SDN controllers make a determination on how authentication and intrusion detection should be implemented making use of the information acquired with regard to the LoDBs.

- Controller for SDN: The basic utility of an SDN is the control plane, which is in charge of managing the network configuration. The LoDB collects data from the underlying IoT devices and BS and makes authentication decisions for the cluster head and IoT devices. Additionally, the controller is expected should be configured with the two modules listed in the proposed configuration:
- AuthenticationModule: This module is run in part at the CA (the one associated with the controller) and in part at the CH (chosen from a range of IoT devices). The scheme contributes to the validation of the CA, IoT devices, and CHs. Our developed authentication procedure is divided into three parts

with offers security protection for mutual or shared authentication, anti-replay, confidentiality, and secrecy, among other things. The following Section 4 has a full explanation of this module.

- Detection of Intrusion System: This system is controlled at the control and data planes of SDNs and is in charge of defending the insider attacks on the network or intruders that surpass the first layer of protection, namely authentication. Section 5 describes it in-depth and consists of three phases: 1) data preparation 2) dimensionality reduction with tensor-based and 3) FCM Clustering by MOEA/D.

```
Algorithm 1: Algorithm 1: Certificate Authority
  Result: THE FIRST PHASE OF KEY GENERATION
  Input: public parameters are set p, a, b, G Let CA's
    pubic/private key pairs: K = k.G
    let A = all IoT device
    while k = all IoT device do
        unique Id is allocated: $Id_j$;
        random secret keys are generated $(k_j)$ ;
        Public keys are computed $K_j = k_j.G$ ;
  end
  return k ;
```

4. Proposed System

This section contains background knowledge on ECC as well as how it has been incorporated into the proposed mutual authentication arrangement between the devices or networks involved. The readers are urged to consult [24] for more information about ECC. The mutual authentication process amongst the participating entities, namely CA, CH, and IoT devices, has been divided into three sections:

4.1. Preliminary Generation of Key

It refers to the initial stage of the authentication procedure. It includes the creation of keys for all units, including the CA, CH, and IoT devices. The CA is in charge of this phase. The CA sets the general parameters linked G, p and the other ECC members, a, b, to produce the keys. Using these settings, random number extraction and ECC multiplication are used to produce the CA's public (K) as well as private (k) key pairs. The same procedure is used for the IoT devices, with K and k denoting their public and private keys, respectively. Each IoT device is also assigned an individual ID (ID_j). The information about all of the IoT device public and private keys is communicated to each device via a secure connection. In **Figure 1**, detailed procedure was shown. The value of TKCH is obtained by performing a multiplication operation concerning X and L_i. CH produces the corresponding value of its ID (ID_i) using this value and the value of A. The equivalence concerning ID_i and ID_i is then verified by CH. If they are deemed to be comparable, the authentication process continues; otherwise, the connection

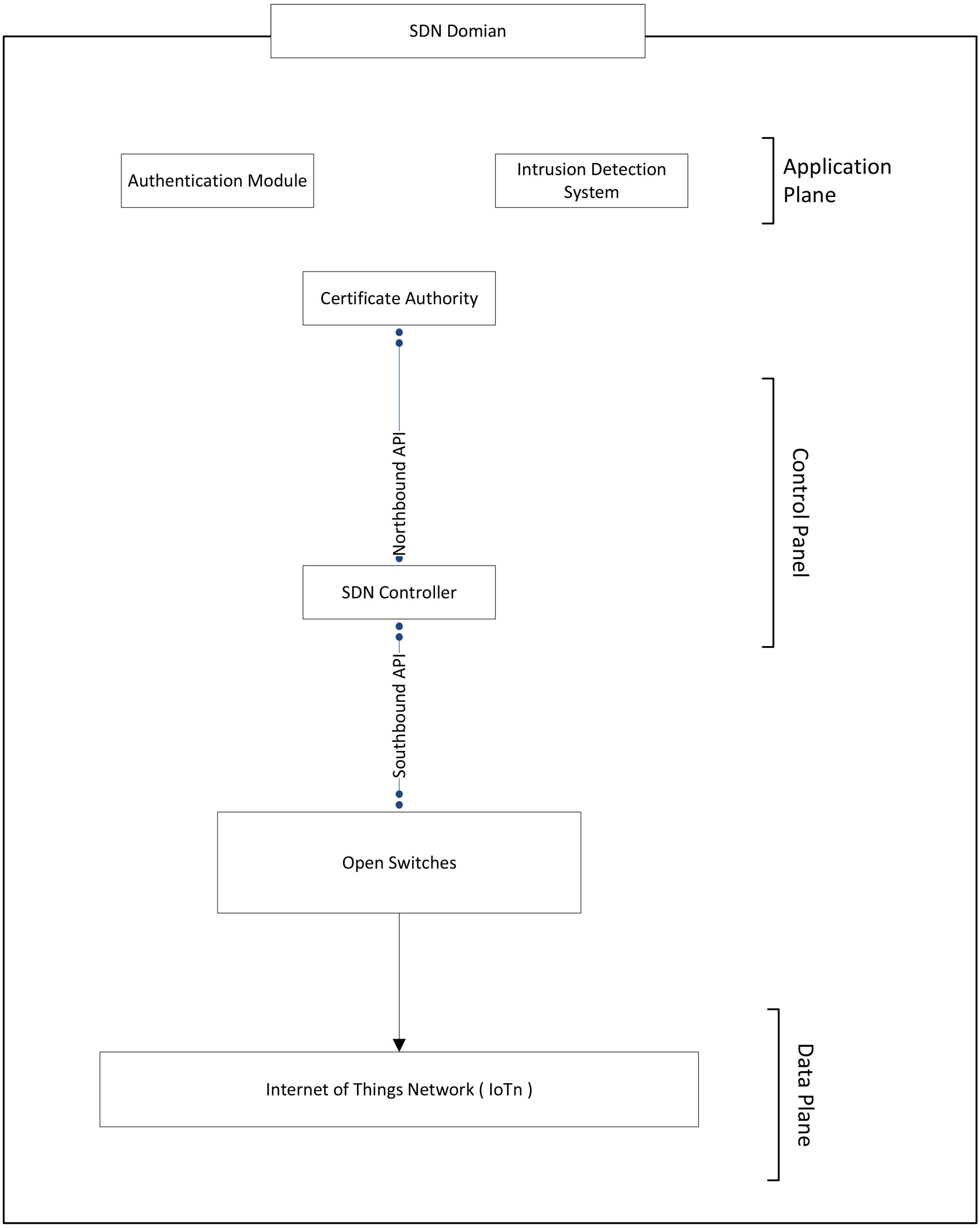

Figure 1. The architecture of the proposed model.

is severed. The intermediate tokens TK3 and TK4, as well as the corresponding authentication token AuthCA, are subsequently computed by CH. If the values of the received AuthCA and computed AuthCA match, the CH understands the information came from the legitimate CA and continues.

4.2. Process of Authentication between CA and CH

Table 1 depicts the authentication procedure with the CA and the CHs. The following steps will help you understand the procedure in detail:

Step 1: The CH creates a randomly generated number r1 in the domain of Zp to start the authentication procedure. The corresponding random number equivalent R1 is then computed using ECC multiplication, as well as the hash of where CH is right now (Loci) to the CA, *i.e.* L_i. The R_1, ID_i, Li values are subsequently relayed to the CA by the CH.

Step 2: The CA responds by taking the actions below. CA first creates a random integer xZp and then uses the multiplication method to generate its corresponding counterpart X. The value of Y is then computed using the approach of summing up L_i and G. The value of TKCA is calculated using the values of X and Y. The XOR operation is then performed on TKCA and ID_i, and the result is stored in A. Then, using the hash operation over ID_i, R1.k, and CAś current time-stamp TSCA, the intermediatevaluesoftokensTK_1, TK_2, and TK_3 are estimated.

Finally, utilizing CA performs concatenation and encryption operations on the interim tokens to provide an authentication token for CH to validate (AuthCA). Following that, the CA generates a random number r_2 Zp, which is multiplied by G to get R_2. This step's final responsibility is to provide the values to the following CH: A, X, AuthCA, T SCA, R_2.

Step 3: When CH receives the above-mentioned tokens (A, X, AuthCA, T SCA, R_2), it validates the time stamp TSCA and processes the following steps if it falls within the acceptable range; otherwise, it tears down the connection. The authentication token AuthCA is then created for CA to validate using TK_3, TK_5, and TS_i (the ith CH generates a time-stamp). Furthermore, The value of X is generated by multiplying a random integer x by G, which is generated by the CH. The CH then creates the value of TKCH using these parameters and the value of L_i. It also uses the XOR technique to construct A from T KCH and ID_i. Finally, the CA receives the following set of tokens: A, X, AuthCH, TS_i.

Step 4: The CA then uses the processes below to verify CH's legitimacy. It validates the received time-stamp TS_i in the first run. The value of ID_i is then used to execute the second step of validation. Finally, the authentication token Auth is used to verify CH's legitimacy. If the parties are confirmed to be similar, mutual authentication is established between them, followed by the CA generating a group ID for the ith cluster (GI $D4_i$). Finally, this GI D_i is forwarded to CH for further correspondence.

4.3. Authentication Process between CH and IoT Devices

Table 2 depicts the authentication procedure between the ith CH and the jth IoT device. The following steps will help you understand the procedure in detail: Step 1: The IoT device generates its Locj and communicates it to its CH to begin the authentication procedure.

Step 2: Using the geographical information data, the CH determines whether the devices belong to its cluster. If the connection is verified to be legitimate, it continues; otherwise, the connection has been disrupted. It then creates a random number r2 in the domain of Zp and uses ECC multiplication to compute the associated R_2. It also generates TS_i, a time-stamp token, and sends R_2 and TS_i to the device.

Step 3: After receiving the above-mentioned tokens, the device validates the time stamp TS_i and, if it falls within the permissible range, proceeds to the next step: if not, tears down the line of communication. The device then uses its respective time-stamp TS_j to compute the intermediate tokens TK_7 and TK_8, as well as the related authentication token Authveh. It also generates a random number r_3 Zp and uses the multiplication method to obtain its corresponding counterpart R_3. Finally, the CH receives the parameters Authveh, R_3, and TS_j for authentication.

Step 4: The CH responds by taking the following actions. It first verifies the received time-stamp. Then, using hash operations over ID_i, r_2, K_i, and CHś current time-stamp TS_i, the intermediate values of tokens TK_8 and TK_9 are estimated. Finally, concatenation and hashing of intermediary tokens is used by CH to create an authentication token (Authveh) to verify the device's legitimacy. Finally, the authentication tokens are compared for equivalency; if they are determined to be identical, the jth device's legitimacy is verified, and the procedure continues. The CH then creates an authentication token (AuthCH) for the device to authenticate using a time stamp TS_i and tokens (TK_8 and TK_{10}). It also produces a second token, GCH, for verification purposes. Finally, the device receives the following set of tokens: AuthCH, ID_i, GCH, TS_i.

Step 5: The device then uses the processes below to verify CHś legitimacy. It validates the received time-stamp TS_i in the first run. The value of TK_7, TK_{11}, and TS_i are then used to accomplish the final level of validation. If the parties are confirmed to be similar, mutual authentication is established between them, followed by the CA generating a group ID for the ith cluster (GID_i). Finally, the device stores this GID_i for future communication.

5. Intrusion Detection System

This section describes the intended intrusion detection system (IDS) in the perspective of VNs in detail. The suggested method detects attack vectors such as preferential forwarding, black hole, packet duplication, resource depletion, wormhole, and Sybil attacks in VN traffic. It is divided into three stages:

5.1. Phase I: Pre-Processing of Data

The existence of missing values in the IoT traffic dataset has a significant impact on the model's learning, inference, and prediction capabilities. Transmitter connections are unreliable due to the failure of the OBU, cluster overlapping, or unannounced system maintenance can all cause inconsistencies in such data. In the literature, there are several approaches for estimating faulty and missing measurements. Methods such as ignoring, substituting, interpolating, and using the closest neighbor are the most prevalent. However, interpolating approaches outperform other methods in terms of accuracy [25]. As a result, the interpolation approach is used to evaluate missing values in this study. Required information is first validated to ensure that it correctly reflects the situation being studied. Following that, interpolation was employed to check that the data was correct and to restore the missing or incorrect values. The goal of this method is to interpolate unknown values using neighboring known values. It's calculated like this:

$$f\left(d_i\right)=\begin{cases}\dfrac{d_{i-1}+d_{i+1}}{2} & \text{if } d_i \in N_a N, d_{i-1}d_{i+1} \notin N_a N,\\ 0 & \text{if } d_i \in N_a N, d_{i-1} \text{ or } d_{i+1} \notin N_a N,\\ d_i & \text{if } d_i \notin N_a N,\end{cases} \tag{1}$$

where d_i is the number of data instances in IoT device traffic over time. NaN is used to represent d_i if it is not equal to any value or is non-numeric. If d_i is NAN and the neighboring values:

$$\frac{d_{i-1}+d_{i+1}}{2}$$

are not NAN, $f\left(d_i\right)$ takes the value of d_{i-1} and d_{i+1}. If d_i is NAN, $f\left(d_i\right)$ returns zero, but if d_{i-1} or d_{i+1} is NAN, $f\left(d_i\right)$ returns zero. Finally, if d_i is not NAN, $f\left(d_i\right)$ is identical to d_i. Next that, the preparation of data is subjected to reducing dimensionalities using tensors, as explained in the section as follows.

5.2. Phase II: Tensor-Based Dimensionality Reduction

The overall dimensionality of the dataset is decreased using the tensor-based technique at this phase before it can be analyzed for any potential invasions. During the data analytics phase, higher-dimensional data causes complex processing challenges such as over-fitting, under-fitting, and poor model interoperability [26]. By improving accuracy, searching speed, storage, and computational cost, lowering the dimensions of incoming data helps to ease and speed up the intrusion investigation process. Essentially, a tensor is a multi-way array that is used to represent higher-dimensional data with multiple attributes. These tensors denote different types of datasets namely unstructured (D_{us}), semi-structured (D_{ss}) and structured (D_s). A particular tensor of n-order is expressed as [27] [28]:

$$T \in R^{\alpha_1 \times \alpha_1 \cdots \alpha_n} \tag{2}$$

where $\alpha_1 \times \alpha_1 \times \cdots \times \alpha_n$ refer to the data dimensions. Moreover, the dataset can be expressed using the following equation:

$$E\left[x_1 \otimes x_2 \otimes \cdots \otimes x_n\right] = R^{\alpha_1 \times \alpha_1 \cdots \alpha_n} \tag{3}$$

In the above equation, the variables $x_1, x_2, \cdots, x_n$ denote the different attributes of the dataset. Thus, the acquired heterogeneous dataset can also be represented using sub-tensor (T_{us}, T_{ss}, T_s) formulations as depicted below [28]:

$$D_{us} \to T_{us}; D_{ss} \to T_{ss}; D_s \to T_s \tag{4}$$

The union operation is also used on the sub-tensors to make a single tensor. This is done to get rid of redundant and redundant transactions throughout the collected dataset. "Unified data tensorization" is the name given to this procedure. Following that, unified tensors' dimensionality is lowered by reducing them to lower-order tensors (also called reduced tensors). The steps below are used to do this. The nth ordering tensor is first turned into n matrix, a process known as "tensor unfolding or matricization" [27] [28]. A complex-valued matrix may then be factorized using the singular value decomposition (SVD) method. SVD is iteratively deployed to all mode-i matrices (M_i) that have been unfolded, which are expressed using the following equation:

$$M_i = U_i S_i V_i^* \tag{5}$$

U and V signify the set of unitary matrices that are orthogonal to each other in the above equation. The diagonal matrix S is used here, and V^* is the conjugate transpose of V. Then, for each Mis, the rank computation process is run, and the undesirable values are deleted to generate reduced tensors. These reduced tensors have fewer dimensions, yet they nonetheless provide the same useful information as the original tensor. To detect potential intrusions, the acquired dataset is fed into the FCM Clustering method.

5.3. Phase III: Fuzzy C-Means (FCM) Clustering

Data items are organized by constructing cluster centers and measuring the degree of membership between data samples and the generated cluster centers. When a distance function is used to specify the cluster membership function, the degree of membership reflects the proximity of data to clustered centers. FCM divides a dataset into clusters based on the number k where $D = \{d_i\}_{i=1}^{n}$ of n objects into $C = \{c_j\}_{j=1}^{k}$ fuzzy cluster centers of size k by minimizing the following objective function [29]:

$$J_m(U,V) = \sum_{i=1}^{n} \sum_{j=1}^{k} \left(U_{ij}^m\right) \left\| d_i - c_j \right\|^2 \text{ where } \underline{1} \le m \ge \infty \tag{6}$$

$$\sum_{j=1}^{k} U_{ij} = 1$$

Here, $J_m(U,V)$ is the sum of squared errors for the fuzzy clusters, m is the weighting exponent, greater than 1, that governs the influence of membership grades, $U = [u_{ij}]$ denotes a fuzzy membership matrix where $u_{ij} \in [0,1]$ is the membership grade of the jth cluster center to the ith data point, V corresponds to the associated set of cluster centers and metric $\left\| d_i - c_j \right\|^2$ measures the weighted sum of distances between cluster centers c_j and data elements di in a corresponding fuzzy cluster. Now, an iterative update of the membership grade u_{ij} and the cluster centers c_j is performed to reach the minimum of $J_m(U,V)$

as:

$$U_{ij} = \left(\sum_{l=1}^{k} \left(\frac{\| d_i - c_j \|}{\| d_i - c_k \|} \right)^{2/(m-1)} \right)^{-1} \quad \forall i, \forall j \tag{7}$$

where, l is the number of iterations and cluster centers c_j are computed in Equation (8) as:

$$c_j = \frac{\sum_{i=1}^{n} (u_{ij})^m d_i}{\sum_{i=1}^{n} (u_{ij})^m} \tag{8}$$

The fuzzy membership matrix U is generated using Equation (7) and the corresponding centroids are evaluated using Equation (8) in each iteration of the FCM algorithm, after which the sum of squared errors is computed using Equation (6). In FCM, the minimization of Equation (6) can be accomplished by maximizing the value of u_{ij} and minimizing the value of c_j separately. As a result, we've broken down our multi-objective function into two sub-objective functions. The following approach to infer the ideal number of clusters using FCM can now be used to solve these numerous objectives.

1) Multi-Objective Evolutionary Algorithm Based on Decomposition: The evaluation of possible solutions in optimization problems can be computationally intensive. The computational cost of predictive distribution models will be extremely expensive, if not unaffordable. MOEA/D optimizes multi-objective problems in order to obtain robust performance. It's a brand-new multi-objective evolutionary algorithm framework based on traditional aggregation methods. It decomposes a multi-objective problem (MOP) into a series of single-objective optimization sub-problems, which are solved primarily utilizing knowledge from the sub-problems around them. The following is a description of it [30]:

$$\min F(x) = \left[f_1(x), f_2(x) \right]^{\mathrm{T}}, \tag{9}$$

subject to $x = (x_1, x_2, \cdots, x_n)^{\mathrm{T}} \in \Omega$, where $F(x)$ consists of k objective functions, $x \in \Omega$ denotes a decision variable vector where Ω corresponds to the decision space, and n is the dimension of variable x. Accordingly, the fuzzy clustering problem is converted into a MOP which is defined as follows:

$$\min F(x) = \left[f_1(x), f_2(x), \cdots, f_k(x) \right]^{\mathrm{T}}, \tag{10}$$

$$f_1(c_j) = \left(\sum_{l=1}^{k} \left(\frac{\| d_i - c_j \|}{\| d_i - c_k \|} \right)^{2/(m-1)} \right)^{-1} \tag{11}$$

$$\text{and} \quad f_2(u_{ij}) = \frac{\sum_{i=1}^{n} (u_{ij})^m d_i}{\sum_{i=1}^{n} (u_{ij})^m} \tag{12}$$

Considering the relationship between the two objectives, we adopt the decomposition strategy in MOEA/D to decompose the optimization of our two objective functions into amounts of scalar optimization sub-problems. Here, Tchebycheff approach is utilized as the decomposition strategy, and the sub-problem is defined by:

$$g^{te}\left(x/\lambda\right)=\max_{1\le i\le m}\left\{\lambda_i\left(f_i\left(x\right)-z_i^*\right)\right\} \tag{13}$$

$$\text{where } z_i^*=\min_{x\in\sum_{i=1}^{n}\left[a_i,b_i\right]} f_i\left(x\right) \tag{14}$$

Here, $z^*=z_1^*,\cdots,z_m^*$ refers to the ideal point in the objective space. For each Pareto optimal point x^*, there exists a weight vector λ such that x^* is the optimal solution of Equation (13) and each optimal solution of Equation (13) is a Pareto optimal to Equation (9).

6. Experimental Analysis

The experimental evaluation details of the suggested strategy in this section and compares the results to the current state of the art. A thorough explanation of the simulation setup, current strategies, and assessment settings is provided. The evaluation findings for both the authentication and intrusion detection modules are shown in this section.

6.1. Authentication Module

Security Analysis: This part emphasizes the proposed protocols' resistance to various cyberattacks, such as cloning and de-synchronization attacks. In this paper, we looked at scenarios in which the suggested module of authentication integrity can be compromised, putting the system at risk. The proposed protocol is capable of smoothly resisting the attack vectors listed below.

Mutual Authentication Supports: The developed authentication system allows for mutual authentication between the CA and the CH, as well as between the CH and the IoT devices. As a result, the validity of the involved entities can be verified before the data transmission can commence. The ECC-enabled verification module's second and third stages, as previously indicated, demonstrate this. Validation tokens are used in each of these stages (Auth$_{CA}$, Auth$_{CA}$ and Auth$_{veh}$) the ECC duplication of certain text data is used to create (R$_1$, R$_2$, R$_3$) with the corresponding private keys (k, k$_i$, k$_j$) of the entities involved. As a result, it assures that only authorized persons with real a private and personal key participating in the whole process. Furthermore, in the realm of ECC, extracting separating shared key from private ones is a difficult operation. Furthermore, the developed security protocol resists eavesdropping attempts even on unsecured channels, preventing the opponent from extracting/decrypting the exchanged communications. This is due to the whole authentication process's utilization of random integers (r$_1$, r$_2$, r$_3$), location attributes (Loc$_i$, Loc$_j$), time-stamps (TS$_{CA}$, TS$_i$, TS$_j$) information, and private keys.

Supports Anonymity: Our authentication mechanism is also intended to accommodate the idea of anonymity. The complexity of the underlying decryption procedure is increased by the usage of the following new characteristics (r$_1$, r$_2$, r$_3$)

per each run; as well as the usage of ECC-computed encryption key (k, k_i, k_j) and ECC-computed random numbers (R_1, R_2, R_3). Furthermore, the usage of locations, timestamps, and random numbers results in the development of new tokens with each run, promoting the notion of anonymity.

Replay Attacks Resistant: The suggested authentication protocol is also replay attack resistant. This is due to the fact that each phase computes and transmits a separate set of tokens related to ($Auth_{CA}$, $Auth_{CA}$ and $Auth_{veh}$). Furthermore, the designed protocol's temporal features (TS_{CA}, TS_i, TS_j) improve security by a factor of ten, with replayed messages being ignored and dropped by the designed solution.

Resists Tracking Attacks: A prospective adversary's tracking of specific IoT devices might have serious effects in the context of autonomous IoT devices, and the effects of VNs may be life-threatening. As a result, the designed solution must be resistant to tracking attacks. The suggested system generates intermediate tokens using This security advantage is provided by the underlying ECC, one-way hash algorithms, XOR and concatenation operations. Furthermore, the developed authentication protocol's location information (Loc_i, Loc_j) is also conveyed via ECC multiplication, prohibiting the extraction of location information [7].

Spoofing Attacks Resistant: The attacker cannot spoof the identity of the CA, CH, or IoT devices in the designed authentication approach. This is because the individual's private key generates the intermediate tokens (TK_1, ..., TK_{10}), and extracting them from the public keys is impossible with ECC.

Supports Forward Security: The suggested authentication system also provides forward security, which is achieved via the use of pseudo-random integers (r_1, r_2, r_3), the location (Loc_i, Loc_j) and time-stamp (TS_{CA}, TS_i, TS_j) attributes; This improves the security of the underlying communications. As a result, even if the adversary has current knowledge about the system, he cannot derive the prior communications.

Using SPAN for Formal Security Verification: This section shows how the suggested authentication protocol was formalized using the AVISPA's commonly used Security Protocol ANimator (SPAN) [31]. It has been implemented on SPAN to validate the security elements of the specified protocol, with high-level programming done using High Level Protocol Specification Language (HLPSL). In a combination of "session" and top-level role "environment," three basic roles (CA, CH, and IoT devices) have been defined. The basic roles are specified in detail by the following parameters: information they can use at first (represented as "parameters"), their initial state (kept by the parameter "State"), and state changes (denoted by one or more "transition"). In HLPSL, each transition is accompanied by RCV or SND parameters. The former denotes a message that is being sent out on the channel "dy," whereas the latter denotes a message that has been received by an agent. These transitions are followed by state changes, and they are the same as the execution steps listed in **Table 1** and **Table 2**. The

Table 1. Formal security verification using SPAN.

```
% OFMC
% Version of 2006/02/13
SAMMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF _SESSIONS PROTOCOL
C:
Program 1
SPAN
Output
ECCAutherCHCAvehiele.if
GOAL
As_ Specific
BACKEND
OFMC
COMMENTS STATITICS
parseTime: 0.00 s
SearchTime: 0.56 s
visitedNodes: 53 nodes
depth: 5 plies
```

Table 2. Evaluation of the proposed authentication module to the current state-of-the-art.

Schemes	SF1	SF2	SF3	SF4	SF5	SF6	SF7
Boahen *et al.* [32]	X	X					
Zhong *et al.* [33]	X					X	X
Boahen *et al.* [34]	X				X		
Li *et al.* [12]		X	X			X	
Proposed model							

SF1: Mutual Authentication; SF2: Resists Eavesdropping; SF3: Supports Anonymity; SF4: Resists Replay; SF5: Resists Tracking; SF6: Resists Spoofing; SF7: Supports Forward Secrecy.

"environment" role also defines various sessions between legitimate agents and invaders. This role also specifies how much information the intruder already possesses. In addition, HLPSL uses a separate "goal" block to express the proposed protocol's several security goals. For example, the suggested protocol has a number of different purposes, including the secrecy of private keys (k_j, k) and randomness.

Strong authentication on intermediate tokens (A, X, AuthCA, AuthCH, R_2, Authveh), numbers (r_1, x, r_2), etc. For threat analysis objectives, Dolev-(dy) Yao's model is considered [32] [35]. The adversary has access to the channel in this threat model for sniffing and message alteration, which is similar to real-life events. The back-end of the OFMC has also been considered in order to test the security characteristics of the designed authentication protocol. The acquired findings, as shown in **Table 1**, show that the protocol is safe from both active and passive attacks. Comparison with the Existing State-of-the-Art: This section compares the proposed authentication module for use in virtual reality with existing techniques. The comparison is based on the security characteristics that each protocol supports. **Table 2** summarizes their information.

6.2. Overhead Analysis

In terms of computation time and communication costs, Table IV summarizes the findings. We did not include the cost of the initial key generation step in our evaluation since it is a one-time activity. Authors are advised to see [14] for further details on the simulation setup.

For the computational cost, let us assume that T_{ecm}, T_{eca}, T_h, T_{mac}, T_{inv}, T_{bp}, $T_{sig\text{-}BOOS}$, $T_{sig\text{-}IBS}$, T_{enc}, and T_{dec} relate to the time necessary to execute ECC point multiplication, ECC point addition, one-way hash function, message decryption, IBOOS signature generation, modular inverse, IBS signature generation, bi-linear pairing, symmetric encryption and authentication code, etc. The suggested approach requires a total of $6T_{ecm} + 12T_h$; wherein $3T_{ecm} + 6T_h$ and $3T_{ecm} + 6T_h$ for authentication between CH and IoT devices. The overall computing cost for the suggested approach is 0.1061 seconds where T_h and T_{ecm} were equivalent to 0.00032 and 0.0171 seconds, respectively.

The following assumptions were used in the communicational overhead study. The output of location, Identity, timestamp, and hash was calculated to be 160 bits, 32 bits, 32 bits, and 160 bits, respectively. In addition, a 160 bit ECC was used, but an elliptic curve point requires a total of 320 bits. According to these facts, the suggested scheme's communicational overhead was quantified in terms of the number of messages exchanged between CH and the IoT device. In addition, the total cost of communication (in bits) was considered. The suggested method sent a total of four messages, *i.e.*, $M_1 = \{Loc_j, ID_j\}$, $M_2 = \{R_2, TS_i\}$, $M_3 = \{Auth_{veh}, R_3, TS_i\}$, and $M_4 = \{Auth_{CH}, ID_j, G_{CH}, TS_i\}$. The sizes of M_1, M_2, M_3, and M_4 were 352 bits, 192 bits, and 512 bits, respectively. This led to a significant communication overhead of 1568 bits. In compared to the other approaches, the suggested authentication module had lower overheads while providing the best level of security.

6.3. Intrusion Detection Module

Various attack vectors, including selective forwarding, DoS assaults, black holes, wormholes, resource exhaustion, Sybil, and packet duplication, were purposely added into the sample space to compare the proposed intrusion detection approache's performance to the current state-of-the-art. Existing-Schemes: AECFV [36], WEKNN [32], T-Claids [37] and PSOGSA [34] All of them have been thoroughly compared against the present state-of-the-art in intrusion detection algorithms.. **Evaluation Parameters:** According to the results of our evaluations, the following factors were taken into account while evaluating our new model:

Detection Rate (DR): DR, the total number of intrusions identified during the period of time is shown. To put it another way, it's a reference to the right way to classify occurrences as harmful or benign. Mathematically, it is expressed as follows:

$$\mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{15}$$

False Positive Rate (FPR): It's a measure of how often a trustworthy entity is mistakenly labeled malignant by the model under consideration. This is how you say it:

$$\mathrm{DR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \tag{16}$$

Accuracy: It is expressed using the following equation: TP + TN

$$\mathrm{Accuracy} = \mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN} \tag{17}$$

Detection Time (DT): The model's time to discover harmful entities in the configuration under consideration is represented by this value. The following equation is used to calculate it [36]:

$$\mathrm{DT} = \sum_{i=1} n \frac{D_i - T_i}{\text{Sampling Frequency} \times n} \tag{18}$$

The variables D_i, T_i, and n in the preceding equation denote the time it takes to detect a prospective adversary A_i, the time it takes for the A_i to launch an attack vector, and how many adversaries there are in total.

Communication Overhead: It refers to the total number of messages triggered by the IoT device to achieve a high level of security.

Performance Evaluation: Figure 2 compare the planned intrusion detection network efficiency to already installed systems. The tests were carried out on a variety of IoT devices (ranging from 50 to 300) using various assault vectors. The DR comparisons, for example, are shown in Figures 2(a)-(e) The collected data show that as the number of IoT devices increases, all of the systems reach a peak in their DR capabilities. The proposed approach, on the other hand, is best in the above case, and has the least variation in DR as the number of IoT devices fluctuates. Furthermore, given the studied setup, IDFV with T-CLAIDS have the poorest performance. Figure 2(a) depicts the corresponding results related to accuracy, which are also similar. Figure 2(b) demonstrates the recommended FPR comparison to AECFV, EKNN, T-CLAIDS and PSOGSA (b). The proposed strategies provide the fewest FPR fluctuations in the setting, followed by AECFV, EKNN, T-CLAIDS and PSOGSA. The collected data show that the FPR rises as the number of IoT devices increases. PSOGSA and T-CLAIDS, on the other hand, have demonstrated rapid fluctuations in the FPR value, whilst the other approaches have seen gradual variations. In Figure 2(c), an emphasis is placed on how one technique compares to the others in terms of detection time (c). In this scenario, all of the assault vectors have been introduced into the configuration in question in order to assess their impact on the various numbers of IoT devices. Overall, the proposed strategy with the shortest detection time demonstrated the best performance in this scenario. Figure 2(d) shows the proposed scheme's communication overhead analysis in comparison to existing schemes. The proposed scheme clearly illustrates the most desirable outcomes in terms of communication overhead, as evidenced by the shown findings. The reason for this can be linked to the suggested scheme's dimensionality reduction characte-

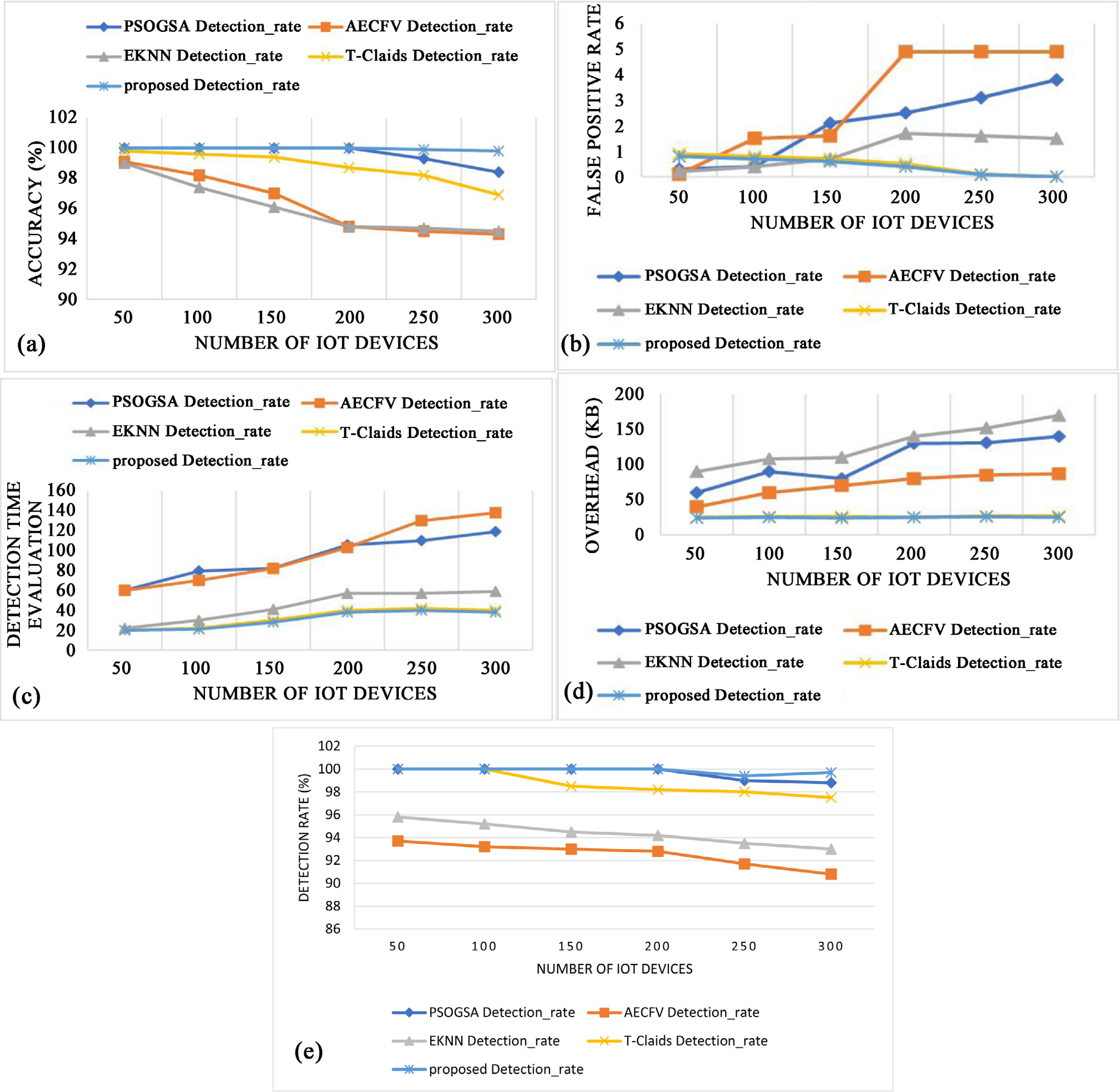

Figure 2. Show the performance assessment of the proposed intrusion detection scheme as compared to existing systems. (a) Accuracy; (b) FalsePositive; (c) DetectionTime; (d) OverHead; (e) DetectionRate.

ristic, In compared to previous techniques, this minimizes the bulk of the data to be analyzed and processed. In a word, the suggested approach outperforms existing strategies in terms of the evaluation parameters under consideration.

7. Conclusion

Future IoTNs are expected to face additional challenges as a result of the combination of SDN plus 5G cellular connection. In such situations, it is critical to give an all-encompassing security solution for IoT networks in order to protect them from unanticipated effects. In this regard, many models are created in the literature that enable either detection mechanism or authentication protocols. Furthermore, these existing methods fail to meet a variety of evaluation criteria. For example, authentication techniques fall short of providing acceptable security, while intrusion detection solutions have significant FPR when traffic increases on the IoT devices. As a result, this paper presents a modular security framework for current IoTNs. Its integrated features, such as authentication. In future, we will research into applying blockchain in the area of security to enhance the scheme.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Fattah, H. (2018) Internet of Things. In: Fattah, H., Ed., *5G LTE Narrowband Internet of Things* (*NB-IoT*), CRC Press, Boca Raton, 1-6. https://doi.org/10.1201/9780429455056-1

[2] Lee, J., Kim, Y., Kwak, Y., Zhang, J., Papasakellariou, A., Novlan, T., Sun, C. and Li, Y. (2016) LTE-Advanced in 3GPP Rel-13/14: An Evolution toward 5G. *IEEE Communications Magazine*, **54**, 36-42. https://doi.org/10.1109/MCOM.2016.7432169

[3] Dong, P., Zheng, T., Yu, S., Zhang, H. and Yan, X. (2017) Enhancing Vehicular Communication Using 5G-Enabled Smart Collaborative Networking. *IEEE Wireless Communications*, **24**, 72-79. https://doi.org/10.1109/MWC.2017.1600375

[4] Rastogi, E., Saxena, N., Roy, A. and Shin, D.R. (2020) Narrowband Internet of Things: A Comprehensive Study. *Computer Networks*, **173**, Article ID: 107209. https://doi.org/10.1016/j.comnet.2020.107209

[5] Chaudhary, R., Aujla, G.S., Garg, S., Kumar, N. and Rodrigues, J.J.P.C. (2018) SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment. *IEEE Transactions on Industrial Informatics*, **14**, 2629-2640. https://doi.org/10.1109/TII.2018.2789442

[6] Kaur, K., Garg, S., Aujla, G.S., Kumar, N., Rodrigues, J.J. and Guizani, M. (2018) Edge Computing in the Industrial Internet of Things Environment: Software-Defined-Networks-Based Edge-Cloud Interplay. *IEEE Communications Magazine*, **56**, 44-51. https://doi.org/10.1109/MCOM.2018.1700622

[7] Garg, S., Kaur, K., Kumar, N. and Rodrigues, J.J. (2019) Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multi-

media Perspective. *IEEE Transactions on Multimedia*, **21**, 566-578. https://doi.org/10.1109/TMM.2019.2893549

[8] Fang, L., Li, Y., Yun, X., Wen, Z., Ji, S., Meng, W., Cao, Z. and Tanveer, M. (2019) THP: A Novel Authentication Scheme to Prevent Multiple Attacks in SDN-Based IoT Network. *IEEE Internet of Things Journal*, **7**, 5745-5759. https://doi.org/10.1109/JIOT.2019.2944301

[9] Molina Zarca, A., Garcia-Carrillo, D., Bernal Bernabe, J., Ortiz, J., Marin-Perez, R. and Skarmeta, A. (2019) Enabling Virtual AAA Management in SDN-Based IoT Networks. *Sensors*, **19**, Article 295. https://doi.org/10.3390/s19020295

[10] Tayyaba, S.K., Shah, M.A., Khan, O.A. and Ahmed, A.W. (2017) Software Defined Network (SDN) Based Internet of Things (IoT) a Road Ahead. *Proceedings of the International Conference on Future Networks and Distributed Systems*, Cambridge, 19-20 July 2017, 1-8. https://doi.org/10.1145/3102304.3102319

[11] Tangade, S., Manvi, S.S. and Lorenz, P. (2018) Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs. *IEEE Transactions on Vehicular Technology*, **67**, 8647-8655. https://doi.org/10.1109/TVT.2018.2839979

[12] Kaur, K., Garg, S., Kaddoum, G., Gagnon, F. and Ahmed, S.H. (2019) Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure. 2019 *IEEE International Conference on Communications Workshops* (*ICC Workshops*), Shanghai, 20-24 May 2019, 1-6. https://doi.org/10.1109/ICCW.2019.8757184

[13] van der Heijden, R.W., Dietzel, S., Leinmüller, T. and Kargl, F. (2018) Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. *IEEE Communications Surveys & Tutorials*, **21**, 779-811. https://doi.org/10.1109/COMST.2018.2873088

[14] Gupta, D., Garg, S., Singh, A., Batra, S., Kumar, N. and Obaidat, M.S. (2017) ProIDS: Probabilistic Data Structures Based Intrusion Detection System for Network Traffic Monitoring. *GLOBECOM* 2017—2017 *IEEE Global Communications Conference*, Singapore, 4-8 December 2017, 1-6. https://doi.org/10.1109/GLOCOM.2017.8254439

[15] Sedjelmaci, H., Senouci, S.M. and Abu-Rgheff, M.A. (2014) An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks. *IEEE Internet of Things Journal*, **1**, 570-577. https://doi.org/10.1109/JIOT.2014.2366120

[16] Wu, W., Huang, Y., Kurachi, R., Zeng, G., Xie, G., Li, R. and Li, K. (2018) Sliding Window Optimized Information Entropy Analysis Method for Intrusion Detection on in-Vehicle Networks. *IEEE Access*, **6**, 45233-45245. https://doi.org/10.1109/ACCESS.2018.2865169

[17] Sharma, P.K., Singh, S., Jeong, Y.S. and Park, J.H. (2017) DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. *IEEE Communications Magazine*, **55**, 78-85. https://doi.org/10.1109/MCOM.2017.1700041

[18] Flauzac, O., González, C., Hachani, A. and Nolot, F. (2015) SDN Based Architecture for IoT and Improvement of the Security. 2015 *IEEE* 29*th International Conference on Advanced Information Networking and Applications Workshops*, Gwangju, 24-27 March 2015, 688-693. https://doi.org/10.1109/WAINA.2015.110

[19] Hu, J., Reed, M., Thomos, N., AI-Naday, M.F. and Yang, K. (2020) Securing SDN-Controlled IoT Networks through Edge Blockchain. *IEEE Internet of Things Journal*, **8**, 2102-2115. https://doi.org/10.1109/JIOT.2020.3017354

[20] Shafi, Q., Basit, A., Qaisar, S., Koay, A. and Welch, I. (2018) Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network. *IEEE Access*, **6**, 73713-73723. https://doi.org/10.1109/ACCESS.2018.2884293

[21] Rathore, S., Kwon, B.W. and Park, J.H. (2019) BlockSecioTNet: Blockchain-Based Decentralized Security Architecture for IoT Network. *Journal of Network and Computer Applications*, **143**, 167-177. https://doi.org/10.1016/j.jnca.2019.06.019

[22] Boukria, S., Guerroumi, M. and Romdhani, I. (2019) BCFR: Blockchain-Based Controller against False Flow Rule Injection in SDN. 2019 *IEEE Symposium on Computers and Communications* (*ISCC*), Barcelona, 29 June-3 July 2019, 1034-1039. https://doi.org/10.1109/ISCC47284.2019.8969780

[23] Yazdinejad, A., Parizi, R.M., Dehghantanha, A. and Choo, K.K.R. (2019) Blockchain-Enabled Authentication Handover with Efficient Privacy Protection in SDN-Based 5G Networks. *IEEE Transactions on Network Science and Engineering*, **8**, 1120-1132.

[24] Vasundhara, S. (2017) The Advantages of Elliptic Curve Cryptography for Security. *Global Journal of Pure and Applied Mathematics*, **13**, 4995-5011.

[25] Zheng, Z., Yang, Y., Niu, X., Dai, H.N. and Zhou, Y. (2017) Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids. *IEEE Transactions on Industrial Informatics*, **14**, 1606-1615. https://doi.org/10.1109/TII.2017.2785963

[26] Garg, S., Kaur, K., Kumar, N., Batra, S. and Obaidat, M.S. (2018) Hyclass: Hybrid Classification Model for Anomaly Detection in Cloud Environment. 2018 *IEEE International Conference on Communications* (*ICC*), Kansas City, 20-24 May 2018, 1-7. https://doi.org/10.1109/ICC.2018.8422481

[27] Kuang, L., Hao, F., Yang, L.T., Lin, M., Luo, C. and Min, G. (2014) A Tensor-Based Approach for Big Data Representation and Dimensionality Reduction. *IEEE Transactions on Emerging Topics in Computing*, **2**, 280-291. https://doi.org/10.1109/TETC.2014.2330516

[28] Kaur, D., Aujla, G.S., Kumar, N., Zomaya, A.Y., Perera, C. and Ranjan, R. (2018) Tensor-Based Big Data Management Scheme for Dimensionality Reduction Problem in Smart Grid Systems: SDN perspective. *IEEE Transactions on Knowledge and Data Engineering*, **30**, 1985-1998. https://doi.org/10.1109/TKDE.2018.2809747

[29] Garg, S. and Batra, S. (2017) A Novel Ensembled Technique for Anomaly Detection. *International Journal of Communication Systems*, **30**, e3248. https://doi.org/10.1002/dac.3248

[30] Zhang, M., Jiao, L., Ma, W., Ma, J. and Gong, M. (2016) Multi-Objective Evolutionary Fuzzy Clustering for Image Segmentation with MOEA/D. *Applied Soft Computing*, **48**, 621-637. https://doi.org/10.1016/j.asoc.2016.07.051

[31] Avispa, S. (2019) The Security Protocol Animator for Avispa.

[32] Boahen, E.K., Changda, W. and Brunel Elvire, B.M. (2020) Detection of Compromised Online Social Network Account with an Enhanced Knn. *Applied Artificial Intelligence*, **34**, 777-791. https://doi.org/10.1080/08839514.2020.1782002

[33] Zhong, H., Wen, J., Cui, J. and Zhang, S. (2016) Efficient Conditional Privacy-Preserving and Authentication Scheme for Secure Service Provision in VANET. *Tsinghua Science and Technology*, **21**, 620-629. https://doi.org/10.1109/TST.2016.7787005

[34] Boahen, E.K., Bouya-Moko, B.E. and Wang, C. (2021) Network Anomaly Detection in a Controlled Environment Based on an Enhanced PSOGSARFC. *Computers &*

Security, **104**, Article ID: 102225. https://doi.org/10.1016/j.cose.2021.102225

[35] Kaur, K., Kumar, N., Singh, M. and Obaidat, M.S. (2016) Lightweight Authentication Protocol for RFID-Enabled Systems Based on ECC. 2016 *IEEE Global Communications Conference* (*GLOBECOM*), Washington DC, 4-8 December 2016, 1-6. https://doi.org/10.1109/GLOCOM.2016.7841955

[36] Sedjelmaci, H. and Senouci, S.M. (2015) An Accurate and Efficient Collaborative Intrusion Detection Framework to Secure Vehicular Networks. *Computers & Electrical Engineering*, **43**, 33-47. https://doi.org/10.1016/j.compeleceng.2015.02.018

[37] Kumar, N. and Chilamkurti, N. (2014) Collaborative Trust Aware Intelligent Intrusion Detection in VANETs. *Computers & Electrical Engineering*, **40**, 1981-1996. https://doi.org/10.1016/j.compeleceng.2014.01.009