IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 26 July 2023, accepted 12 August 2023, date of publication 18 August 2023, date of current version 24 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3306607

RESEARCH ARTICLE

Enabling IoT Service Classification: A Machine Learning-Based Approach for Handling Classification Issues in Heterogeneous IoT Services

MOHAMMAD ASAD ABBASI[1], YEN-LIN CHEN[2], (Senior Member, IEEE), ABDULLAH AYUB KHAN[1,3], ZULFIQAR A. MEMON[4], NOUMAN M. DURRANI[4], JING YANG[5], CHIN SOON KU[6], AND LIP YEE POR[5], (Senior Member, IEEE)

[1]Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi, Sindh 75660, Pakistan
[2]Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei 106344, Taiwan
[3]Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Pakistan
[4]Department of Computer Science, National University of Computer and Emerging Sciences (NUCES)-FAST, Islamabad 44000, Pakistan
[5]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[6]Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia

Corresponding authors: Yen-Lin Chen (ylchen@mail.ntut.edu.tw), Lip Yee Por (porlip@um.edu.my), and Chin Soon Ku (kucs@utar.edu.my)

This work was supported in part by the National Science and Technology Council, Taiwan, under Grant NSTC-112-2221-E-027-088-MY2 and Grant NSTC-111-2622-8-027-009; and in part by the Ministry of Education of Taiwan ''The study of artificial intelligence and advanced semi-conductor manufacturing for female Science, Technology, Engineering, and Mathematics (STEM) talent education and industry-university value-added cooperation promotion'' under Grant 1112303249.

ABSTRACT The Internet of Things (IoT) is a form of Internet-based distributed computing that allows devices and their services to interact and execute tasks for each other. Consequently, the footprint of the IoT is increasing and becoming more complex to the highest degree. This has also given birth to new IoT-enabled applications and services. Efficient service interaction and management also call for understanding and analyzing the nature of IoT services. Further, IoT services must be characterized into various classes, and different service-related attributes must be considered for the classification. This article assesses the requirements of heterogeneous IoT services by examining their interactions. Principally, heterogeneous IoT and their service interactions are targeted. The research work performs classification of IoT services into various classes. Services are classified on the basis of various attributes. The attributes reflect different characteristics of the services. This research enables improved utilization of IoT services through efficient classification of available resources using machine learning methods. To demonstrate service classification applicability, the SVM, voting classifier, and decision tree have been applied in a service-oriented environment along with different types of services. All the services in the data set were analyzed and divided into five classes. Moreover, the decision tree performed well and achieved higher accuracy values in all classes. However, the overall prediction and classification of the decision tree model were observed to be good and satisfactorily high.

INDEX TERMS Classification, heterogeneity, decision tree, SVM, service-oriented environment.

I. INTRODUCTION

The modern computing world is recurrently evolving and diversifying in order to keep up with the most advanced and cutting-edge technical advancements. This is a result of the increasing technological evolution of sensing devices and the widespread use of smart things in human life. All of which drive the development and use of a worldwide network of smart and linked objects. In this connection, the Internet of Things (IoT) is a concept that aims to create new

The associate editor coordinating the review of this manuscript and approving it for publication was Seifedine Kadry.

computing futures by connecting every smart thing to a worldwide network capable of detecting, communicating, sharing information, and doing smart analytics for a variety of everyday applications. It targets the adoption of new paradigms by altering traditional computing and putting its capabilities to use in everyday human life [1].

Internet of Things (IoT) networks are collections of internet-enabled physical devices and objects that are equipped with sensors, actuators, and smart machines with computation power, storage, and communication capabilities to get connected and exchange data. Wearables, smart air conditioners, refrigerators, computer devices, surveillance cameras, weather sensors, and other smart things are all part of the Internet of Things (IoT) vision.

One example of such an application is the IoT-enabled smart home. The basic concept of a smart home is to link household appliances in a network architecture and communicate using standard protocols. This is accomplished through the use of smart sensors and cameras. Moreover, many businesses are turning to the IoT to obtain a competitive advantage. They are concentrating on improving operational efficiency by utilizing real-time data management and job automation. This allows them to take a more creative approach to expanding and developing their company. Additionally, IoT is also used in smart agriculture to reshape traditional crop cultivation and decision-making. In this connection, IoT-based smart horticulture and irrigation systems are already evident in agriculture.

Further, advancements in the usage of IoT devices in various application areas have enabled an increasing number of IoT devices to connect to other networks. Smart lighting, surveillance, marketing, business, and smart appliances are some examples of such applications. Moreover, extensions of such applications are growing at a faster rate.

In order to exploit the future potential of digitalization and connectivity, IoT services from different application areas must be able to communicate, interact, share information, and perform tasks for each other. Therefore, the widespread use of smart devices and applications necessitates addressing some crucial concerns and obstacles that arise in such situations [2].

In the real world, millions of diverse IoT services are generated per year. Further, they vary in type of service, metadata, service areas, and other related attributes. The lack of understanding of the nature of services still needs to be addressed. Therefore, leveraging users to identify available IoT services in the vicinity is gaining popularity. However, one of the leading limitations is the identification of the required parameters to identify services accurately. Further, the dynamic adoption of such parameters and their appropriateness for heterogeneous types of services are also challenging.

As a solution to the problems mentioned, this research work addresses the problem by classifying heterogeneous IoT services through machine learning techniques.

- The research helped optimize the service interaction functionality of different IoT services working in the system.
- The main objective of the research is to highlight the usefulness of categorizing IoT services by considering their classification based on dynamic attributes such as criticality level, access permission, data type, and data rate.
- The service categorization has been implemented by using machine learning algorithms such as SVM, voting classifiers, and decision trees. All the services in the data set were analyzed and divided into five classes.

The remainder of the paper is organized as follows: the existing systems for device identification and classification have been explored in Section II. Further, Section III explains the adopted research methodology. Furthermore, Section IV presents an experimental setup. Additionally, Section V evaluates experiment results and discussions, whereas Section VI articulates conclusions and future directions. Finally, Section VII provides references.

II. LITERATURE REVIEW

The contemporary computing world is rapidly evolving, fueled by new computing services, nanotechnologies, and user-driven innovations of smart tools that are created out of need, design innovations, and human exploration of the potential of global networks of connected objects [3], [4], [5]. As the use of connected computing in daily life has expanded, existing internet infrastructures have iteratively become inadequate to handle the requirements of state-of-the-art equipment and applications [6], [7].

Considering the vision of IoT connectivity, various IoT domains must enable their respective domain services to interact with each other. Prior to that, there are some critical problems that need attention. With regard to this, the developments carried out by the IoT also call for the necessity of seamless interaction among the services. This illustrates that IoT services need to be classified according to their various attributes and categorized into multiple service classes. In addition, service coordination-related issues are important to consider as well. For such critical-natured service interactions, appropriate trust measurement mechanisms also need to be worked out.

Characteristics of Classification:

Aside from its potential, IoT characteristics present new hurdles in terms of service-to-service interactions. One of the most important research problems in IoT service interactions is the classification of heterogeneous services. The classification of services aids in the early identification and management of services in the area. Furthermore, service availability benefits the creation of solutions for selecting the most appropriate services based on the given request.

Generally, IoT service provisioning takes place between two or more services. These services may have interacted

previously with each other, or it may be the very first interaction between them. In such conditions, the service requester often has insufficient information about the service provider [8]. In this connection, trust measurement targets the selection of particular IoTs with a profound reputation. This ensures the reliability and credibility of the various services available in the IoT. Further, in a specified service environment, trust helps in making the decision to be involved in unexpected risks.

While considering a service-oriented architecture (SOA)-based IoT environment [9], every device offers single or multiple services. At a particular time, service may play the role of service requester or provider in a given service interaction. In the IoT background, trust measurement has been a vital component in context-aware service provision to the requesters, and it has become a driving force to fulfill future IoT service interaction requirements [10], [11], [12]. Most of the current research has divided trust into two broad categories: direct trust and indirect trust [13]. Direct trust is attained after single or multiple service interactions between the trustor and the trustee. Consequently, services categorically classify each other as trusted or untrusted. On the other hand, indirect trust is calculated as a result of third-party recommendations from other network entities' observations. Hence, it shows that for an indirect trust, it is not necessary that the trustor and trustee have interacted with each other prior to the trust [14].

The increasing number of IoT applications encompass smart objects in a network of connected devices. This wave of smart devices is serving almost all aspects of human life, such as supply chain, medical, business, transportation, and education. These IoT devices are equipped with capabilities like data collection, communication, and task mapping. The huge interconnectivity of the devices has also made IoT interactions increasingly complex, diverse, and distributed [15]. As IoT services are closely linked with each other and share information frequently, it is very important to measure and analyze trust between them. This creates the need for developing a trust system in an SOA-based IoT ecosystem. In such a hyper-connected environment, there are misbehaving services trying to provide services according to their self-centeredness, and due to the lack of trust between IoT service interactions, large-scale IoT adoption is likely to suffer [16]. By considering this necessity, a trust model plays the role of clarifying the service requester's or provider's trustworthiness with each other. Hence, it helps in increasing reliance among services within the IoT ecosystem and supports the provisioning of the most appropriate service responders among all available services. Further, this also prohibits untrustworthy services from getting the chance to interact with other legitimate services [17].

In this connection, the trust value is formulated by using various direct or indirect observations associated with the communicating parties. The simplest form of computing trust values is to sum the observed values of different annotations and maintain a total trust [18], [19]. Another way of computing trust values is through statistical methods and probability density functions. This helps in expressing uncertainty in forthcoming interactions as well [20], [21], [22]. Moreover, fuzzy models are also utilized for the trust value computation. In this case, fuzzy logic gives a set of rules for reasoning with fuzzy measures [23], [24].

In this connection, the level of trust required for a service exchange is dependent on the sensitivity of the service provided. For instance, sharing an individual's research interests requires a very low level of trust as compared to sharing bank account details with the same requester of information. Additionally, trust varies according to the context of the service interaction. Despite other influential factors, trust is also bound to a specific time interval within a particular context. However, IoT service providers can gain trust by providing services with the attributes required by the requester.

Given the current innovations in IoT services, there are myriad diversified services available for various kinds of computing environments [25], [26]. Moreover, the variety of service-to-service interaction leads to the creation of new value-added services out of several existing ones. In this connection, the heterogeneous nature of IoT services affects trust-based decision-making among the interacting services. Therefore, in such huge and complex service mapping environments, challenges associated with service interactions must be addressed appropriately. Considering heterogeneous IoT resource-constrained services and devices, establishing trust-based IoT interaction still requires the following considerations:

- Efficient device registration based on attributes such as computational power, memory, and available services.
- Service classification on the basis of service nature, type, and criticality level needs to be performed so that only appropriate interactions are stimulated.
- Consideration of trust measurement mechanisms for the different types of IoT service interactions to deal with challenges like self-configuration and dynamic adoption of services.
- In order to maintain the integrity of interactions, secure storage of computed trust values is necessary.
- Robust scheduling for modeling the communication and interaction of the huge number of sporadic IoT services so that the overall throughput of the system is maximized.

The requirements associated with service interactions are a major key driver for the enriched evolution of IoT, and this will help in fulfilling the objective of ensuring seamless connectivity between heterogeneous IoT services.

III. RESEARCH METHODOLOGY

The modern world has witnessed a major change from traditional embedded systems to smart and intelligent computing in the form of IoT-based systems for interacting devices and services. Figure 1 provides a detailed description of

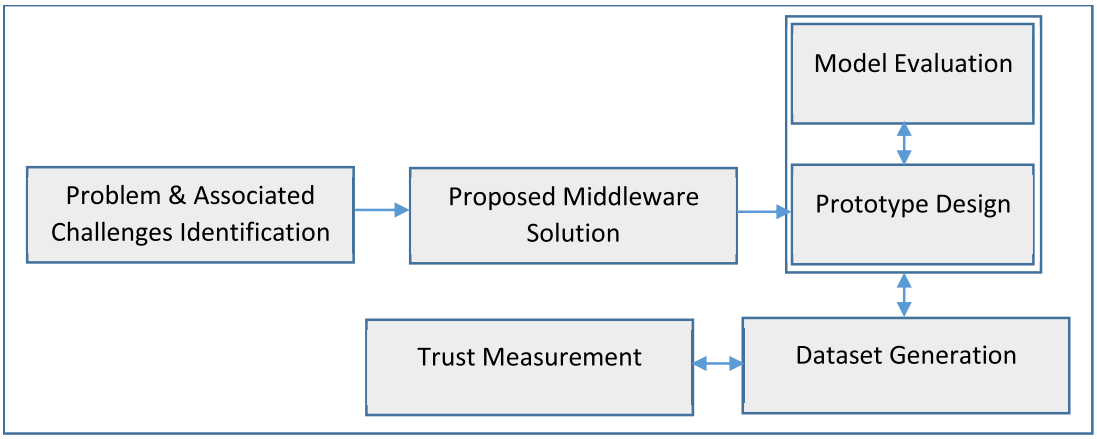


FIGURE 1. Research methodology flow.

the research methodology adopted to conduct the proposed research. Figure 1 refers to an extensive literature survey in the IoT domain that has been conducted, specifically targeting open challenges related to the interaction of IoT devices and their growing services.

After a comprehensive analysis of various service requirements and their challenges, heterogeneity and interoperability of IoT services were identified as an open issue in most of the research conducted by different researchers [27], [28]. In order to deal with the problem of IoT heterogeneity and interoperability, it has been found that the discovery and registration of different IoT services operating in the surroundings need to be performed in the first step [29]. In this connection, the research work has considered a service-oriented domain environment. Here, it is important to highlight that a service domain denotes a physical environment that may be a hospital, university campus, smart home, and many more. Further, every domain is managed through a domain controller. The basic operation of the model is such that whenever a service needs to interact with another service (within or outside the service domain), it sends a service request to the controller. If it is not a registered service, then the domain controller registers it by storing parameters like available computational power, memory, available services, and other related attributes. Once the IoT services are registered, their classification on the basis of nature, type, and criticality level needs to be performed so that only relevant service interaction requests are encouraged. In this connection, classification helps in categorizing heterogeneous IoT services into various classes. Further, it assists in understanding the nature of newer services as well. Associated with this, the research work has applied three classification algorithms: decision tree, support vector machine (SVM), and voting classification.

Challenges and Analysis: Since heterogeneous services will interact with each other, services will consider primarily their privacy; hence, privacy in the form of access controls, namely critical-urgent, critical-nonurgent, and non-critical, has been worked out to fulfill the requirements.

Further, the trust measurements of different types of IoT service interactions are considered to deal with challenges like self-configuration and dynamic adoption of services. In this regard, a novel trust-based algorithm has been developed for dynamically selecting the trust parameters, relative weight ranges, and decay factor for the interaction. For the integrity of interactions, computer trust values are securely stored on the blockchain. Moreover, the research work also targets trustful service scheduling among the interacting services. Here, the major objective is to optimally select and assign the most trusted full service to the requesters. In this connection, a trust-based service scheduler has also been worked out. Along with it, in order to demonstrate middleware applicability, its prototype has been implemented in a service-oriented environment with different types of services.

IV. EXPERIMENTAL SETUP

In order to validate the service classification process, the research team has conducted various tests. For this purpose, the simulations were run in a service-centric heterogeneous IoT system. The Cooja network simulator is used to validate the service classification lifecycle. Cooja is a well-known IoT and WSN network simulator. It is a small network simulator that is primarily used to simulate low-power wireless settings. Cooja with the Contiki 3.0 operating system was used as a network simulator for the experiments and generation of the required dataset. The simulations were conducted on a Core i5 (2.7 GHz) machine running Ubuntu 18.04.4 as the operating system. The simulation environment is split into four IoT service domains, each having a mix of heterogeneous and homogeneous services. Some of the services include light control, CCTV cameras, motion detectors, fire detectors, and many more.

These services are utilized to study the interaction patterns among the services. Further, the connection of service-to-service interaction was one-to-many, which means one service may request service(s) from the same domain or engage with services from different domains. Moreover, the

TABLE 1. Sample SCD dataset.

SNo	Service Requester	Service Provider	Urgency Level	Data Required	Access Permission	Data Rate	Data Type	Assigned Class
1	CCTV Camera	Emergency Services	CU	HealthCare	UrgentAllowed	High	Video	HealthCare
2	Banking	Change/Return	NC	OrderSupport	Allowed	Normal	XML	OrderSupport
3	File Sharing	Internet Access	NC	SmartHome	Allowed	Normal	CSV	Elementary
4	Entertainment	MobilePackages	NC	SmartHome	Allowed	Low	Images	OrderSupport
5	Heart Rate	Emergency Services	CU	HealthCare	Allowed	High	Text	HealthCare
6	Emergency Services	Air Aviation Services	CU	OrderSupport	Allowed	High	Text	OrderSupport
7	Smart Sprinkling	Temperature	CU	Agriculture	Allowed	High	Text	Elementary
8	Banking	Blood Availability	CU	HealthCare	CriticalAllowed	High	Text	HealthCare
9	Instant Messaging	Smoke Detector	CU	SmartHome	Allowed	High	Signal	HealthCare
10	Banking	Preventive Care	NC	HealthCare	CriticalAllowed	Normal	XML	HealthCare
11	GPS	Gaming	NC	SmartHome	NotAllowed	Normal	Text	Elementary
12	Smoke Detector	Emergency Services	CU	HealthCare	UrgentAllowed	High	Signal	HealthCare
13	Patient Monitoring	Camera	CU	HealthCare	Allowed	High	Video	HealthCare
14	Gaming	Drug Management	CNU	HealthCare	Allowed	Normal	Text	HealthCare
15	Uber	Fleet Management	CNU	Traffic	CriticalAllowed	High	Text	Traffic

large-scale simulation runs at different intervals resulted in a total of 3,000 service interactions stored in CSV format.

Furthermore, each service domain had a controller, which is primarily responsible for operations such as service registration, service scheduling, and domain management. In this connection, the most important step is the registration of domain services.

For security and manageability reasons, registration has been proven to be an important part of any computing system. Likewise, before getting interacted with by any of the domain's services, a newer IoT service must first undergo the service registration process. Further, the service must be associated with a controller to perform an exchange of service(s) with others. In the proposed middleware, the domain controller accomplishes the task of registering services.

When a service wants to communicate with another service (inside or outside the service domain), the model's fundamental activity is to send a service request to the controller.

The IoT controller scans the list of already registered services for such services when trying to search for them. The connection is formed if the service is already registered and the trust value is within the allowed threshold. Otherwise, the service registration request is initiated. The controller maintains relevant information when registering a service in any of the service domains. Moreover, this helped in formulating the data set utilized for the classification of the services.

Once a service has been registered, it may offer service(s) for other devices, or it can also request to consume the services held by other surrounding devices. The registration helps an IoT service be represented in the domain and be discovered by service requesters. By using the registered information of the services, the controller becomes able to search, update, manage, and remove them. Moreover, the controller can monitor all available services in the vicinity and utilize these services more proficiently for improved resource consumption. Additionally, this helps in classifying available services into various classes.

The major objective of classification lies in accurately predicting the target class for each data item within the dataset. Further, classification tends to make analysis effective. Considering the diversity of IoT services, this research work presents a novel approach to classifying various IoT services into five distinct classes. Further, the classification has been performed according to their nature.

A. SERVICE CLASSIFICATION DATA SET (SCD)

In order to explore the characteristics of the services and their classification, it is important to formulate a data set associated with different types of services. The data set is then utilized to conduct experiments related to classification, scheduling, and decay analysis. The results obtained through processing this data set have helped in more meaningful coordination, classification, scheduling, and service mapping.

TABLE 2. Data transformation.

SNo	Service Requester	Service Provider	Urgency Level	Data Required	Access Permission	Data Rate	Data Type	Assigned Class
1	CCTV Camera	Emergency Services	1	2	3	0	5	1
2	Banking	Change/Return	2	3	0	2	6	2
3	File Sharing	Internet Access	2	4	0	2	1	0
4	Entertainment	MobilePackages	2	4	0	1	2	2
5	Heart Rate	Emergency Services	1	2	0	0	4	1
6	Emergency Services	Air Aviation Services	1	3	0	0	4	2
7	Smart Sprinkling	Temperature	1	0	0	0	4	0
8	Banking	Blood Availability	1	2	1	0	4	1
9	Instant Messaging	Smoke Detector	1	4	0	0	3	1
10	Banking	Preventive Care	2	2	1	2	6	1

TABLE 3. Classification report – support vector machine.

	Precision	Recall	F1-Score	Support	Kappa Coefficient
Elementary	0.790	0.844	0.816	103	0.776
HealthCare	0.913	0.903	0.908	186	0.865
OrderSupport	0.868	0.841	0.854	63	0.837
Traffic	0.942	0.883	0.912	129	0.888
Utility	0.834	0.875	0.854	104	0.822

The service classification dataset (SCD) utilized in service classification is depicted in Table 1. The service classification data set has been tabulated in comma-separated values (.csv) format after various service interactions during the experiments of the simulation run. The service classification data set contains three thousand instances. Further, the major features considered for classification are UrgencyLevel, DataRequired, AccessPermission, DataRate, and DataType. Additionally, the target class for service classification is AssignedClass. However, Table 1 refers to some of the interactions in the data set that have been presented as a sample. Moreover, a description of features and their possible data values is presented. In connection with the detailed representation of service classification in Table 2, there were a few data preprocessing steps that had been applied to transform the data into a more appropriate form, improve data quality, and remove inconsistencies. The details of the preprocessing steps are presented as follows:

B. PREPROCESSING OF THE SERVICE CLASSIFICATION DATA SET

Data preprocessing is a way of making data useful and efficient for usage in succeeding stages of the data analysis lifecycle. Primarily, it provides a scheme to organize raw data for further processing, and it has become one of the most essential components of modern data analytics.

Moreover, it helps in removing errors and inconsistencies from the data set, such as missing values, noise, outliers, redundancy, and many more.

As per the nature and requirements of the data set, the data has to pass through a series of steps such as data transformation, cleaning, reduction, aggregation, and normalization. These steps support standardizing the data so that it can be fed to the classification algorithm. The classification of IoT services has been implemented through Python (Jupyter Notebook). Jupyter Notebook is an open-source interface providing an environment for interactive computing to enable a more powerful relationship between the user, data, and results. Jupyter Notebook supports a variety of languages, such as Java, Python, R, Scala, and many more. Further, the Jupyter Notebook ships with an IPython kernel that facilitates writing code in Python.

In connection with service classification, the major steps incorporated in data preprocessing and classification are explained as follows:

- *Dropping inappropriate class values:* The service classification data set had some inappropriate class values, i.e., Health and Traffic-Critical. There are erroneous class names in the data set. All such entries in the data set were dropped.
- *Count of class occurrences:* In order to analyze the distribution of the data set classes, the observation of occurrences of all class values is very important.

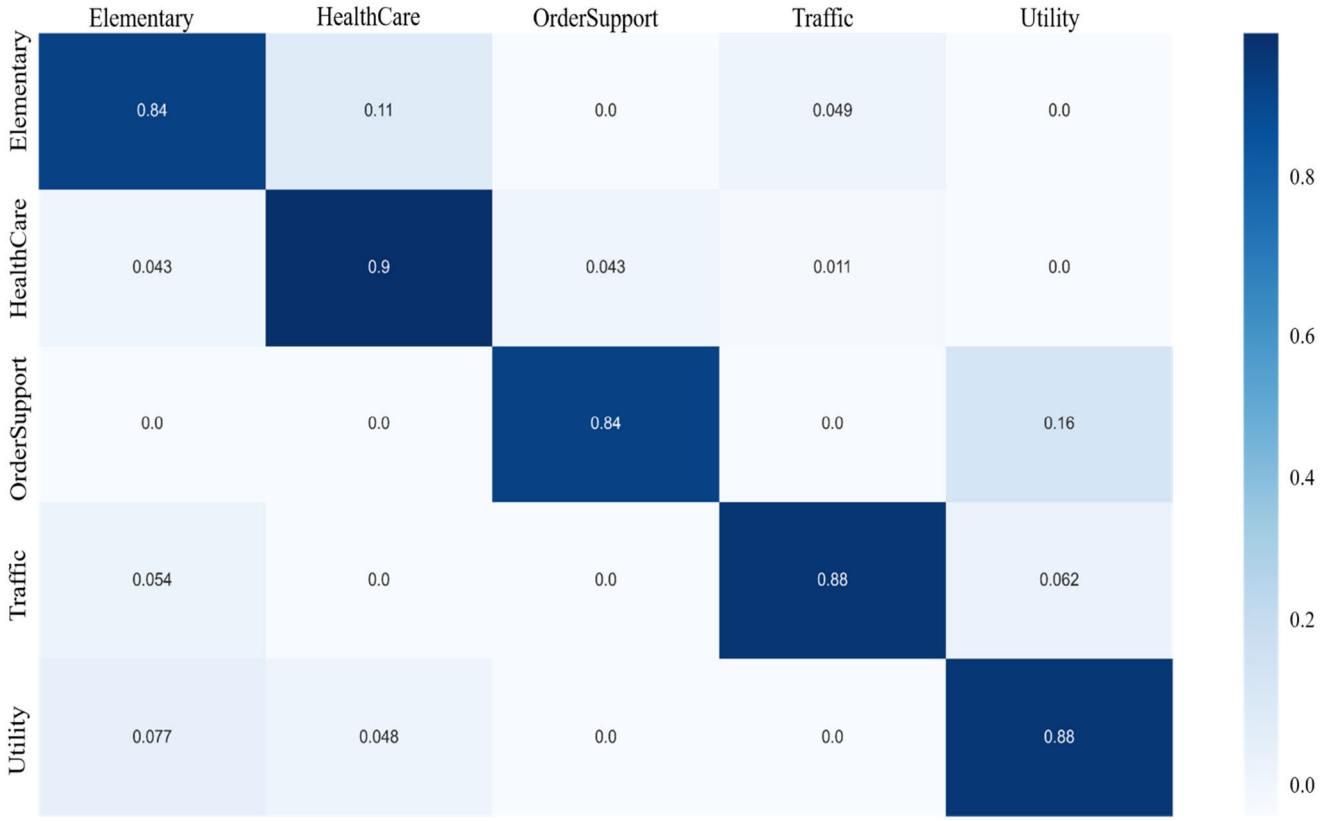


FIGURE 2. Confusion matrix – SVM.

Therefore, the count of class occurrences has been performed first.

- *Transformation:* Another critical preprocessing phase is to encode the data set into a form that is more suitable and easier for the algorithms. In order to better organize the data set for the analysis, non-numeric labels such as high, normal, and low are encoded to numeric labels like 0, 1, and 2, respectively. Similar is done with all other non-numeric labels of the remaining classes. For this purpose, the research work has utilized the ''LabelEncoder'' class of the Python Sklearn library. In this connection, the data transformation and decoded sample data set are shown in Table 2.

Feature Assignment and Data Splitting: In connection with data preprocessing, feature assignment and data splitting have also been performed. Further, UrgencyLevel, DataRequired, AcessPermission, DataRate, and DataType are selected as features, and AssignedClass is set to be the target. Moreover, the 'train_test_split' library from Sklearn has been applied for splitting the data set into training and testing data.

Additionally, data is split in the ratio of 80:20, i.e., 80% of the data has been exploited for the training of the model and 20% of the remaining data has been utilized for the testing of the model. Afterward, the research team implemented various classification algorithms on the processed dataset.

V. EXPERIMENT RESULTS AND DISCUSSIONS

This section presents the results obtained against the proposed middleware framework in Section IV. In light of the data set explanation, the classification of heterogeneous services is very imperative for IoT. For the classification of the service's data set, this research work has applied three classification algorithms to the service classification data set. These classifiers are support vector machines (SVM), voting classifiers, and decision trees. The experiments first analyze the resultant classification using evaluation metrics such as accuracy, confusion matrix, precision, recall, support, f1-score, and Kappa coefficient. Afterward, results representing the comparative analysis of applied classifiers were demonstrated. Moreover, a head-to-head analysis of classifiers is also presented. Furthermore, the details of these classification algorithms and their performance evaluation are explained below:

A. SUPPORT VECTOR MACHINE (SVM)

The support vector classifier uses optimal hyperplanes, i.e., decision boundaries between the classes, to look for the separately classified data points. In a way, SVM divides data points in N-dimensional space into various classes with a clear separation. Further, newer data points are plotted onto the dimension space, and accordingly, it is tried to predict the target class with increased efficiency. In connection with

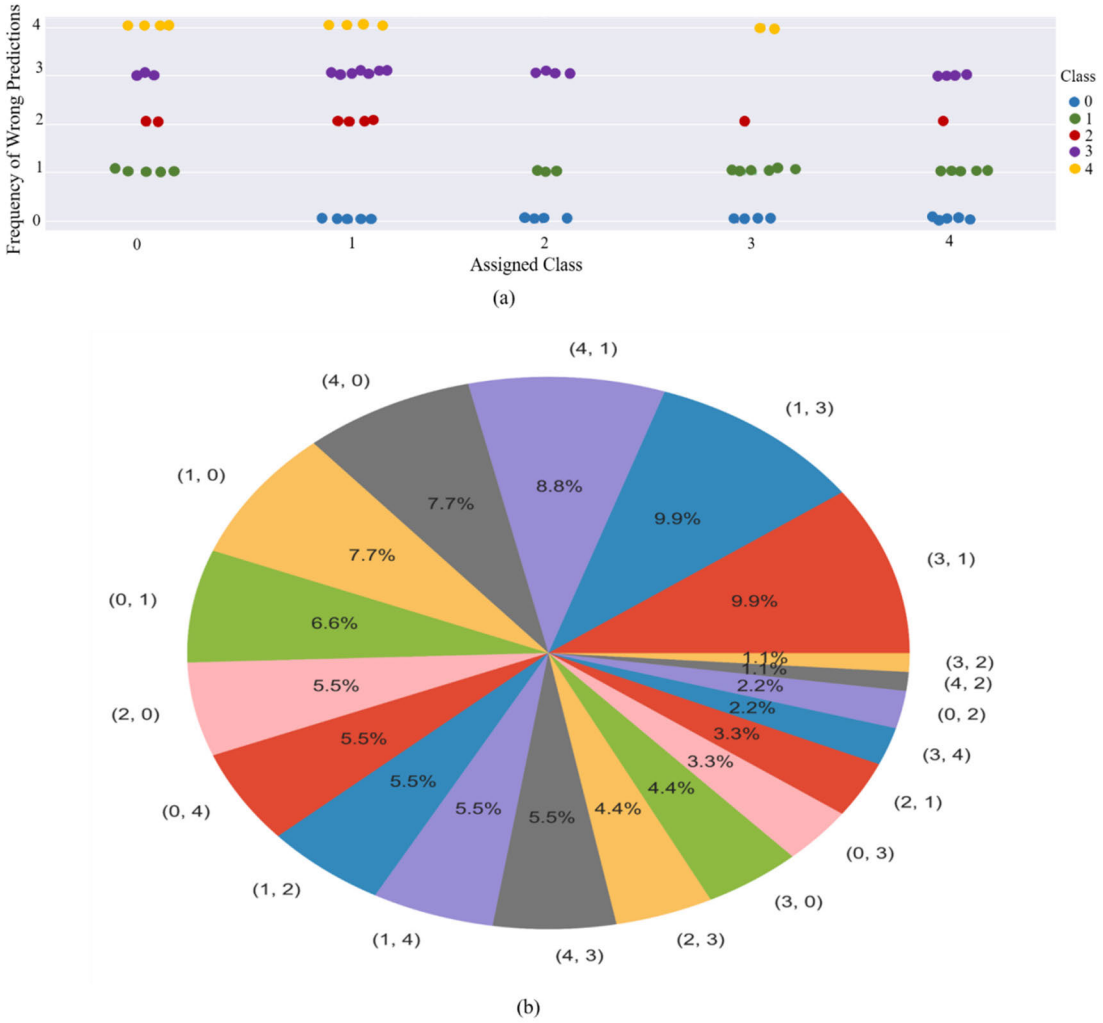


FIGURE 3. Support vector machine (a) Frequency of wrong predictions; (b) Class-wise percentage of wrong predictions.

this, the research work has applied the SVM classification algorithm for service classification. Consequently, the resultant classification report has been shown in Table 3. It is quite clear from Table 3 that the precision of the two classes, i.e., Traffic and HealthCare, was observed to be 0.942 and 0.913, respectively. Similarly, the precision of the Order-Support and Utility classes has been found to be 0.868 and 0.834, respectively. Further, the Elementary class had a precision of 0.79. Moreover, it is also observable through Table 3 that recall of the HealthCare class was measured at 0.903, whereas an average of 0.86 was found to be the recall of reminding classes. On the other hand, it is observed that precision and recall contributed to the f1-score, with an average value of 0.85 for all the classes present in the data set. Finally, the average Kappa coefficient value for all the classes was found to be 0.83.

Likewise, the performance of the SVM model has been illustrated through the confusion matrix in Figure 2. Additionally, the confusion matrix, as shown in Figure 2, displays the representation of a number of cases correctly predicted and incorrectly classified. As shown by the confusion matrix in Figure 2, the model accurately predicted the HealthCare class with an accuracy of 0.9, whereas the classes of Traffic and Utility achieved an accuracy of 0.8 and 0.8, respectively. On the other side, the model misclassified the Order-Support class as a Utility class with a value of 0.16. Another misclassified class, i.e., elementary, was classified as Healthcare and Traffic. Their respective values of miss-classification were observed to be 0.11 and 0.049, respectively. Furthermore, the analysis of wrong predictions from the classifier is also important. Therefore, the research work has examined wrong predictions during the classification as well. In this connection, Figure 3 (a) provides details of the wrong predictions that had very low instances of wrong predictions. However, classes 0, 1, and 3 had most of the wrong predictions. Figure 3 (a) refers to class 2 and class 4 instances as wrong predictions. On the other hand, Figure 3 (b) provides a detailed overview of wrong predictions in percentages.

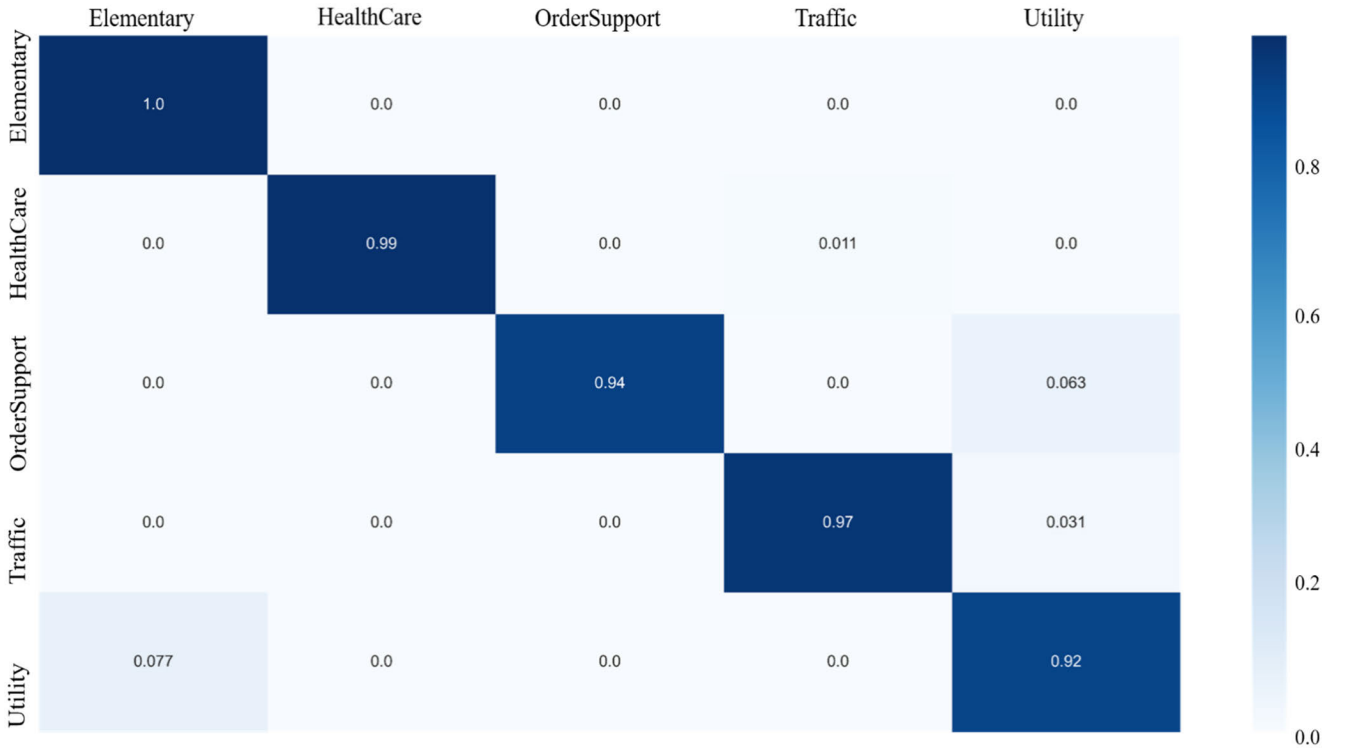


FIGURE 4. Confusion matrix – voting classifier.

TABLE 4. Classification report – voting classifier.

	Precision	Recall	F1-Score	Support	Kappa Coefficient
Elementary	0.927	1.0	0.962	103	0.954
Healthcare	1.0	0.989	0.994	186	0.992
Order-Support	1.0	0.936	0.967	63	0.963
Traffic	0.984	0.968	0.976	129	0.969
Utility	0.923	0.923	0.923	104	0.906

Additionally, Figure 3 (b) also demonstrates the actual classes and the classifier's wrongly predicted class, which were predicted against the actual classes. Figure 3 (b) also highlights that major wrong predictions were observed where class 3 was predicted as class 1. Likewise, class 1 was predicted to be class 3. These two classes of wrong predictions contributed cumulatively 20% to the wrong predictions. While some of the other major contributors in wrongly predicted classes were found to be (4, 1), (4, 0), (1, 0), (1, 2), (1, 4), and (4, 3).

B. VOTING CLASSIFIER

The voting classifier ensures the involvement of the collection of various machine learning classifiers in the classification process. These models work together by combining their individual predictions to come up with a final prediction. Further, the final decision on output is taken based on a majority of votes, i.e., the maximum likelihood of a class being predicted by the adopted classifiers. Consequently, this yields higher performance as compared to employing a single classifier. Moreover, this mixing of classifiers is more appropriate for situations where a single classifier does not reach the required accuracy in predictions.

In connection with voting classification, the research work applied three different classifiers to voting. These classifiers include logistic regression, decision trees, and support vector machines. Moreover, the resultant classification report from employing these three classification algorithms is presented in Table 4.

As it has been depicted in Table 4, the precision of the two classes, i.e., HealthCare and Order-Support, was found to be 1. On the other hand, two classes, i.e., Elementary and Utility, had a value of 0.92. However, the Traffic class had a precision value of 0.984. Moreover, the recall value of the Elementary class was observed to be 1. Although, for the remaining classes, this value was found to be within an average of 0.95. On the other side, the average f1-score value for all the classes was measured to be 0.96. As far as

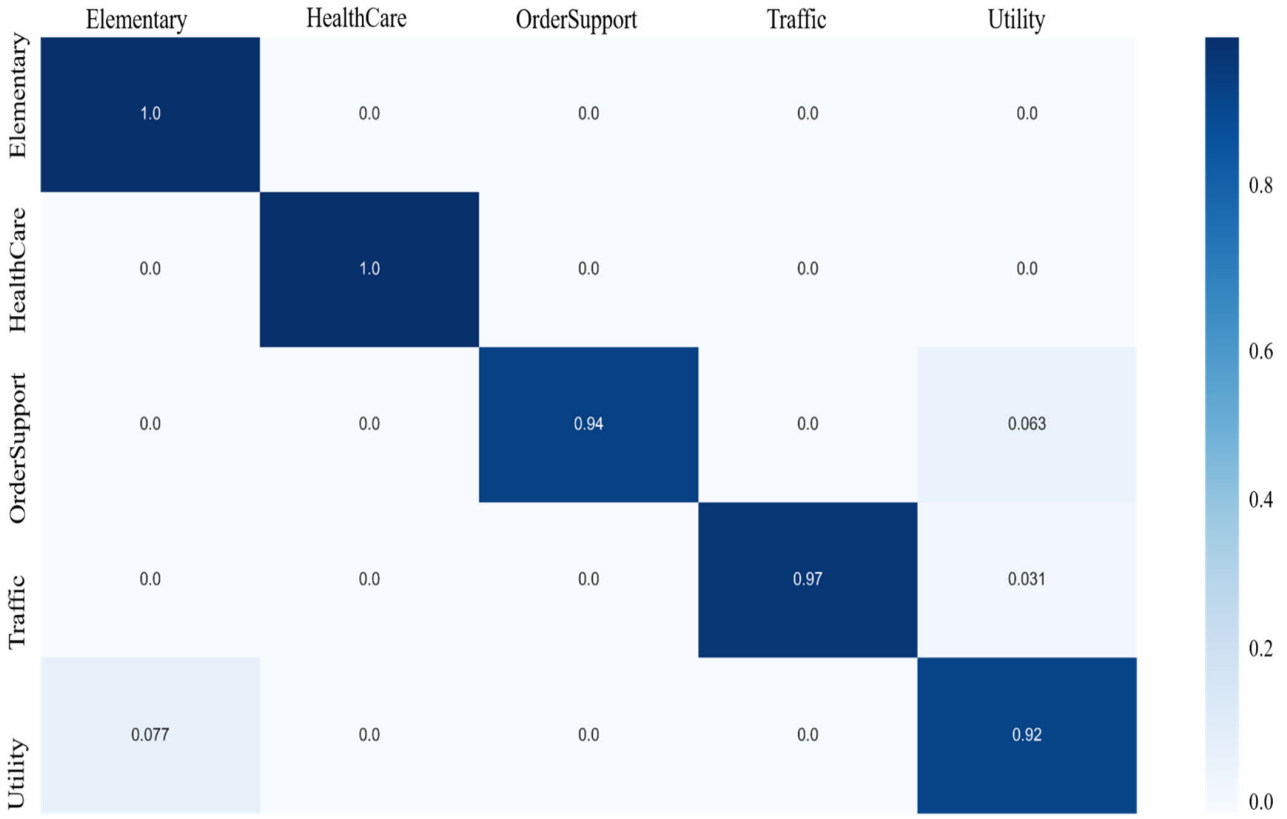


FIGURE 5. Confusion matrix – decision tree.

TABLE 5. Classification report – decision tree.

	Precision	Recall	F1-Score	Support	Kappa Coefficient
Elementary	0.927	1.0	0.962	103	0.954
HealthCare	1.0	1.0	1.0	186	1.0
Order-Support	1.0	0.936	0.967	63	0.963
Traffic	1.0	0.968	0.984	129	0.979
Utility	0.923	0.923	0.923	104	0.90

the Kappa coefficient value is concerned, the highest Kappa coefficient value in voting was observed with a value of 0.992 in the HealthCare class. Whereas, for the rest of the classes, the average Kappa coefficient value was found to be 0.942. Additionally, the confusion matrix of the voting classifier has been depicted in Figure 4.

As it is observable from the representation in Figure 4, the accuracy of the elementary, Order-Support, Traffic, and Utility classes was improved by using the voting classifier.

Additionally, in order to consider the wrong predictions during the classification, depict the count of classes found to be wrongly predicted.

In this connection, it is observable that classes 0 and 1 had higher frequencies of wrong predictions with the voting classifier. Conversely, classes 2, 3, and 4 had a smaller number of instances of wrong predictions. In order to have clear insights into wrongly predicted classes, this paper presents a thorough class-wise analysis of expected classes and their counter-wrongly predicted classes. As depicted, the lowest percentage of the wrong prediction, i.e., 1.1%, belongs to class 3, where it was predicted as class 2 by the classifier. Alternatively, the highest percentage of wrongly predicted class 1 was predicted to be class 3 by the classifier, and the percentage of such wrong predictions is observed to be

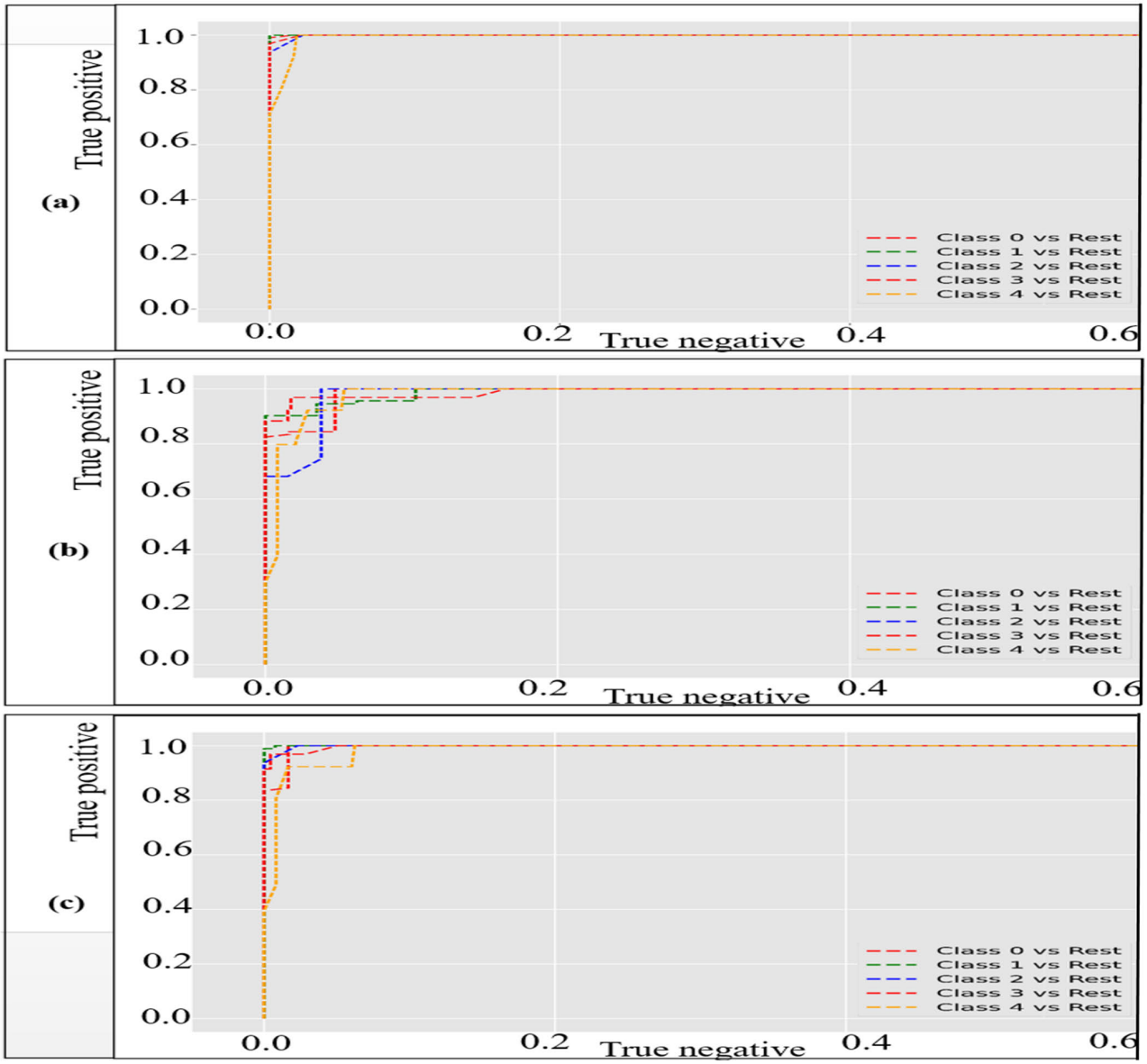


FIGURE 6. ROC curve: (a) Decision tree, (b) SVM, (c) Voting classifier.

between 1.1% and 9.9% of the total wrong predictions by the voting classifier, as shown in Figures 3(a) and 3(b). Similarly, other major contributors were (4, 1), (4, 0), (3, 1), (0, 1), and (2, 0). Further, the percentage of wrong predictions in these classes was 8.9%, 8.9%, 8.9%, 7.8%, and 6.7%, respectively.

C. DECISION TREE

Decision trees are one of the most widely used supervised learning algorithms for classification. It is based on dividing the original data set into smaller chunks and generating a tree structure out of them. More specifically, nodes in the decision tree represent data set features; branches provide decision rules; and a leaf node denotes the final decision. In this way, every tree node serves the purpose of a test case with some attributes of the data set. Further, this helps in producing decision rules associated with smaller test cases of the dataset (Morfino & Rampone, 2020; F. Wang et al., 2020). The research work has also applied a decision tree classification algorithm for service classification. Further, the detailed classification report has been depicted in Table 5. However, Table 5 refers to the service classification report, and it is important to note that out of five target classes, the precision of three classes has been found to be 1. This reflects that all these classes, i.e., Healthcare, Order-Support, and Traffic, were accurately predicted, and there was no false-negative prediction in these classes. Moreover, in two of the classes, i.e., Elementary and Utility, this ratio was observed to be 0.927 and 0.923, respectively. Whereas the recall of the two classes, i.e., Elementary and HealthCare, was found to be 1. However, the recall of the classes Order-Support, Traffic, and Utility was found to be 0.936, 0.968, and 0.923, respectively. Additionally, the balance between precision and

TABLE 6. Class-wise prediction performance (in%) of SVM, voting classifier, and decision tree.

	Class				
Model	Elementary	Utility	Order-Support	Traffic	HealthCare
SVM	18.8	18.6	10.4	20.7	31.5
Voting Classifier	19.0	17.8	10.1	21.7	31.5
Decision Tree	19.0	17.8	10.1	21.4	31.8

TABLE 7. Class-wise f-1 score of SVM, voting classifier, and decision tree.

	Class				
Model	Elementary	Utility	Order-Support	Traffic	HealthCare
SVM	0.816	0.912	0.854	0.912	0.908
Voting Classifier	0.962	0.976	0.967	0.976	0.994
Decision Tree	0.962	0.984	0.967	0.984	1.0

recall, i.e., the f1 score, was found to be an average of 98% in all classes. This shows that precision and recall contributed relatively equally to the f1 score. Moreover, the research work has also calculated the Kappa coefficient for every class, and it has been observed that the average Kappa value for all the classes was approximately 95%. In addition to this, the decision tree confusion matrix is shown in Figure 5. The decision tree classifier shows better performance as compared to the SVM and voting classifiers. More specifically, as represented through Figure 5, classes in elementary, healthcare, and traffic have been significantly improved. Furthermore, in order to examine wrong predictions during the classification, the frequency of wrong predictions has been plotted. In this regard, a seaborn Cat plot represents the class-wise distribution of wrong predictions using a decision tree classifier. Additionally, it is quite clear that wrong predictions mostly belong to classes 0, 1, and 3. Moreover, very few instances were predicted wrong in classes 2 and 4. Likewise, a more detailed analysis of wrong predictions in percentages has been depicted. Figure 3 refers to an x-axis as the actual class and a y-axis as the wrongly predicted class. It is observable that 1.1% of the wrong predictions belong to class 1, where the classifier predicted class 1 as class 3. Similarly, 9.9% of wrong predictions are from class 4, where it was predicted as class 1 by the classifier. In this way, all the wrongly predicted classes and their percentages have been reflected in the pie chart.

D. COMPARATIVE PERFORMANCE ANALYSIS OF APPLIED CLASSIFICATION ALGORITHMS

Considering the above service classification discussion, Figure 6 assesses accuracy among the applied classifiers. In this regard, Figure 6 (a) shows the ROC curve of the decision tree classifier, Figure 6 (b) represents the ROC curve of the SVM classifier, and Figure 6 (c) illustrates the ROC curve of the voting classifier. Further, it is noticeable from Figure 6 that the decision tree classifier and voting classifier perform better as compared to the SVM classifier. Moreover, Table 7 provides a depiction of the class-wise individual valuation of f1-cores. In this regard, it is important to notice that SVM showed the lowest f1-scores in the elementary and Order-Support classes.

TABLE 8. Performance summary of SVM, voting classifier and decision tree.

Model	Accuracy
SVM	0.876
Voting Classifier	0.969
Decision Tree	0.972

Moreover, the class-wise prediction accuracy comparison has been depicted in Table 6. It is evident from Table 6 that the SVM prediction ratio was lower in the Elementary and Traffic classes. Overall, the class-wise prediction accuracy of decision trees was found to be higher than that of SVMs and voting classifiers. Further, this relationship between model accuracies has also been represented in Table 8. However, Table 8 refers to the fact that the decision tree performed well and achieved higher accuracy values in all classes. However, the overall prediction and classification of the decision tree model were observed to be good and satisfactorily high.

VI. CONCLUSION AND FUTURE DIRECTION

IoT service interaction has been limited due to the heterogeneous nature of devices, communication protocols, types of data, data rates, quality of service requirements, and trust measures between applications. For instance, in many situations, IoT services want to interact with other services; however, due to challenges such as cross-platform interaction and service dependencies, applications are unable to communicate with each other. The problem becomes more complex in large-scale IoT deployments, where self-configuration and dynamic adoption of various service requirements are considered on the fly. Due to the large number and diversity of IoT services, their relationships must be investigated. This calls for persistent observation of the services' interaction behavior and scheduling resource availability accordingly. The results of the proposed simulations are illustrated, which highlights how well the system performs in terms of high accuracy and efficiency. The classifiers used to investigate are as follows:

(1) SVM, (2) voting classifier, and (3) decision tree, with evaluation results noted as 0.876, 0.969, and 0.972. It clearly shows that the decision tree performs well enough as compared to other classifiers. Therefore, enhanced mechanisms for exploring service-oriented relationships among IoTs are also to be worked out. Industry-wide global standards, unified communication protocols, highly enhanced security aspects, and middleware problems are left for future work.

REFERENCES

[1] Q. Fang, R. Ye, L. Li, Y. Feng, and M. Wang, "STEMM: Self-learning with speech-text manifold mixup for speech translation," in *Proc. 60th Annu. Meeting Assoc. Comput. Linguistics*, Dublin, Ireland, 2022, pp. 7050–7062, doi: 10.18653/v1/2022.acl-long.486.

[2] W. Haider, E. M. Nadeem, H. A. S. Khan, A. Abbasi, and Z. Anwar, "Computing in humanity: To predict the human behaviors over social media," *Webology*, vol. 19, no. 3, pp. 3081–3570, 2022.

[3] Y. Kim, S. Lee, and I. Chong, "Orchestration in distributed web-of-objects for creation of user-centered IoT service capability," *Wireless Pers. Commun.*, vol. 78, no. 4, pp. 1965–1980, Sep. 2014, doi: 10.1007/s11277-014-2056-9.

[4] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial Internet of Things (IIoT)—Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016, doi: 10.1016/j.comnet.2016.01.009.

[5] W. Ahmed, S. Muhamad, I. Sentosa, H. Akter, E. Yafi, and J. Ali, "Predicting IoT service adoption towards smart mobility in Malaysia: SEM-neural hybrid pilot study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 1, pp. 524–535, 2020, doi: 10.14569/ijacsa.2020.0110165.

[6] H. Derhamy, J. Eliasson, and J. Delsing, "IoT interoperability—On-demand and low latency transparent multiprotocol translator," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1754–1763, Oct. 2017, doi: 10.1109/JIOT.2017.2697718.

[7] M. Jeyaselvi, M. Sathya, S. Suchitra, S. J. A. Ibrahi, and N. S. K. Chakravarthy, "SVM-based cloning and jamming attack detection in IoT sensor networks," in *Advances in Information Communication Technology and Computing* (Lecture Notes in Networks and Systems), vol. 392, V. Goar, M. Kuri, R. Kumar, and T. Senjyu, Eds. Singapore: Springer, 2022, pp. 461–471, doi: 10.1007/978-981-19-0619-0_41.

[8] E. Dushku, M. M. Rabbani, M. Conti, L. V. Mancini, and S. Ranise, "SARA: Secure asynchronous remote attestation for IoT systems," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3123–3136, 2020, doi: 10.1109/TIFS.2020.2983282.

[9] U. K. Lilhore, S. Simaiya, H. Pandey, V. Gautam, A. Garg, and P. Ghosh, "Breast cancer detection in the IoT cloud-based healthcare environment using fuzzy cluster segmentation and SVM classifier," in *Ambient Communications and Computer Systems* (Lecture Notes in Networks and Systems), vol. 356, Y. C. Hu, S. Tiwari, M. C. Trivedi, and K. K. Mishra, Eds. Singapore: Springer, 2022, pp. 165–179, doi: 10.1007/978-981-16-7952-0_16.

[10] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014, doi: 10.1007/s11276-014-0761-7.

[11] I. Banerjee and P. Madhumathy, "IoT based agricultural business model for estimating crop health management to reduce farmer distress using SVM and machine learning," in *Internet of Things and Analytics for Agriculture, Volume 3* (Studies in Big Data), vol. 99, P. K. Pattnaik, R. Kumar, and S. Pal, Eds. Singapore: Springer, 2022, pp. 165–183, doi: 10.1007/978-981-16-6210-2_8.

[12] Y. NarasimhaRao, P. S. Chandra, V. Revathi, and N. S. Kumar, "Providing enhanced security in IoT based smart weather system," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 18, no. 1, pp. 9–15, Apr. 2020, doi: 10.11591/ijeecs.v18.i1.pp9-15.

[13] A. M. Alfarshouti and S. M. Almutairi, "An intrusion detection system in IoT environment using KNN and SVM classifiers," *Webology*, vol. 19, no. 1, pp. 3500–3517, Jan. 2022.

[14] N. B. Truong, "Evaluation of trust in the Internet of Things: Models, mechanisms and applications," Ph.D. dissertation, Liverpool John Moores Univ., Merseyside, U.K., Aug. 2018, doi: 10.24377/researchonline.ljmu.ac.uk.00009241.

[15] Y. Masoudi-Sobhanzadeh and S. Emami-Moghaddam, "A real-time IoT-based botnet detection method using a novel two-step feature selection technique and the support vector machine classifier," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109365, doi: 10.1016/j.comnet.2022.109365.

[16] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: A systematic literature review," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, Jun. 2019, Art. no. 21, doi: 10.1186/s13673-019-0183-8.

[17] Z. Solatidehkordi, J. Ramesh, A. R. Al-Ali, A. Osman, and M. Shaaban, "An IoT deep learning-based home appliances management and classification system," *Energy Rep.*, vol. 9, pp. 503–509, May 2023, doi: 10.1016/j.egyr.2023.01.071.

[18] N. Ahmed, R. Amin, H. Aldabbas, D. Koundal, B. Alouffi, and T. Shah, "Machine learning techniques for spam detection in email and IoT platforms: Analysis and research challenges," *Secur. Commun. Netw.*, vol. 2022, pp. 1–19, Feb. 2022, doi: 10.1155/2022/1862888.

[19] Y. Liu, X. Gong, and C. Xing, "A novel trust-based secure data aggregation for Internet of Things," in *Proc. 9th ICCSE*, Vancouver, BC, Canada, Aug. 2014, pp. 435–439, doi: 10.1109/ICCSE.2014.6926499.

[20] A. A. Khan, S. Bourouis, M. M. Kamruzzaman, M. Hadjouni, Z. A. Shaikh, A. A. Laghari, H. Elmannai, and S. Dhahbi, "Data security in healthcare industrial Internet of Things with blockchain," *IEEE Sensors J.*, early access, May 11, 2023, doi: 10.1109/JSEN.2023.3273851.

[21] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, and C.-T. Lu, "LogitTrust: A logit regression-based trust model for mobile ad hoc networks," in *Proc. 6th ASE Int. Conf. PASSAT*, Cambridge, MA, USA, Dec. 2014, pp. 1–10.

[22] N. Parde and R. Nielsen, "Finding patterns in noisy crowds: Regression-based annotation aggregation for crowdsourced data," in *Proc. EMNLP*, Copenhagen, Denmark, Sep. 2017, pp. 1907–1912, doi: 10.18653/v1/D17-1204.

[23] E. Damiani, S. De Capitani di Vimercati, P. Samarati, and M. Viviani, "A WOWA-based aggregation technique on trust values connected to metadata," *Electron. Notes Theor. Comput. Sci.*, vol. 157, no. 3, pp. 131–142, May 2006, doi: 10.1016/j.entcs.2005.09.036.

[24] M. Lesani and N. Montazeri, "Fuzzy trust aggregation and personalized trust inference in virtual social networks," *Comput. Intell.*, vol. 25, no. 2, pp. 51–83, May 2009, doi: 10.1111/j.1467-8640.2009.00334.x.

[25] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and challenges in technology and standardization," *Wireless Pers. Commun.*, vol. 58, no. 1, pp. 49–69, Apr. 2011, doi: 10.1007/s11277-011-0288-5.

[26] A. A. Khan, A. A. Laghari, M. Rashid, H. Li, A. R. Javed, and T. R. Gadekallu, "Artificial intelligence and blockchain technology for secure smart grid and power distribution automation: A state-of-the-art review," *Sustain. Energy Technol. Assessments*, vol. 57, Jun. 2023, Art. no. 103282, doi: 10.1016/j.seta.2023.103282.

[27] A. A. Khan, A. A. Shaikh, and A. A. Laghari, "IoT with multimedia investigation: A secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth," *Arab. J. Sci. Eng.*, vol. 48, pp. 10173–10188, Dec. 2022, doi: 10.1007/s13369-022-07555-1.

[28] F. Nasri and A. Mtibaa, "IoT platform for healthcare system: Protocols interoperability," *Int. J. Appl. Eng. Res.*, vol. 12, no. 22, pp. 12510–12518, Dec. 2s017.

[29] A. A. Khan, A. A. Laghari, M. Shafiq, O. Cheikhrouhou, W. Alhakami, H. Hamam, and Z. A. Shaikh, "Healthcare ledger management: A blockchain and machine learning-enabled novel and secure architecture for medical industry," *Hum.-Centric Comput. Inf. Sci.*, vol. 12, Nov. 2022, Art. no. 55, doi: 10.22967/HCIS.2022.12.055.

MOHAMMAD ASAD ABBASI received the Ph.D. degree from the National University of Computer and Emerging Science (NUCES)-FAST, Karachi, Pakistan, in 2021. He is currently an Assistant Professor with the Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University, Lyari, Karachi. He has published more than 15 articles in reputed journals and international conferences. His research interests include the Internet of Things, heterogeneous devices, device-to-device communication, computing, AI, and data science.

YEN-LIN CHEN (Senior Member, IEEE) received the B.S. and Ph.D. degrees in electrical and control engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2000 and 2006, respectively. From February 2007 to July 2009, he was an Assistant Professor with the Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan. From August 2009 to January 2012, he was an Assistant Professor with the Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei, Taiwan, where he was an Associate Professor, from February 2012 to July 2015, and has been a Full Professor, since August 2015. His research results have been published in more than 100 journal articles and conference papers. His research interests include artificial intelligence, intelligent image analytics, the Internet of Things, smart manufacturing, intelligent vehicles, and intelligent transportation systems. He is a fellow of the IET and a member of the ACM, IAPR, and IEICE.

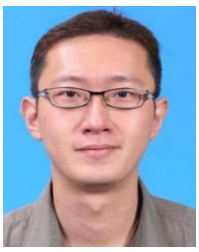
ABDULLAH AYUB KHAN is currently pursuing the Ph.D. degree with the Department of Computer Science, Sindh Madressatul Islam University, Karachi. He is a Lecturer with the Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi, Pakistan. He has published more than 40 research articles in well-reputed journals, such as IEEE Access, IEEE Transactions, MDPI, Elsevier, Spring, Wiley, and Hindawi, in the domains of digital forensics, cyber security, blockchain, hyperledger technology, multimedia systems, and artificial intelligence.

ZULFIQAR A. MEMON received the bachelor's and master's degrees in distributed systems from the University of Sindh, Jamshoro, Pakistan, and the Ph.D. degree in artificial intelligence from Vrije University, Amsterdam, The Netherlands. He was an Associate Professor with Sukkur IBA University, Sukkur, Pakistan, where he was involved in building up a cyber-physical system for stroke detection. He is currently a Full Professor and the Head of the School of Computing, National University of Computer and Emerging Sciences (NUCES)-FAST, Karachi, Pakistan. He co-taught behavioral and organizational dynamics to bachelor's students as a Visiting Scholar with the Behavioural Informatics Group, Vrije University. He is interested in providing intelligence support to humans in handling non-communicable diseases, smart transportation, assistive devices, and software. He is also interested, particularly in the interoperability of heterogeneous IoT platforms and enhancing the current software for e-learning by equipping it with the features of a smart multi-agent, voice-enabled AI-based virtual assistant. He is currently developing a blockchain-based, auditable framework for inter-country trading. His work has been carried out with several bodies, including community groups of all types, local authorities, government departments, health providers, and businesses. He has been invited by the East-West Center, Honolulu, HI, USA, as a Panel Member in the 2019 International Symposium on Humane Artificial Intelligence. He has supported researchers and social innovators to develop research, training, and development projects for a wider cross-section of audiences and contexts. He regularly chairs and presents at conferences and seminars worldwide.

NOUMAN M. DURRANI received the Ph.D. degree from the National University of Computer and Emerging Science (NUCES)-FAST, Karachi, Pakistan, in 2017. He is currently an Assistant Professor with the Department of Computer Science, NUCES-FAST. He is a member of the Systems Research Laboratory, and a Co-PI with the Smart Video Surveillance Laboratory, an affiliated Laboratory of the HEC-National Centre for Big Data Cloud Computing, NUCES-FAST. He has published more than 30 research articles in quality journals and international conferences. His research interests include heterogeneous devices, volunteer computing systems, computer vision, human computation, cloud computing, distributed systems, WSNs, and big data analytics.

JING YANG received the B.E. degree in navigation technology from Shandong Jiaotong University, in 2022. He is currently pursuing the master's degree in data science with the Universiti Malaya. His primary research interests include medical image processing and deep learning.

CHIN SOON KU received the Ph.D. degree from the University of Malaya, Malaysia, in 2019. He is currently an Assistant Professor with the Department of Computer Science, Universiti Tunku Abdul Rahman, Malaysia. His research interests include visual password authentication for computer security, decision support applications, and speech recognition.



LIP YEE POR (Senior Member, IEEE) received the Ph.D. degree from the University of Malaya, Malaysia, in 2012. He is currently an Associate Professor with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology (FCSIT), Universiti Malaya, Malaysia. He has been among the first to obtain funds from the IRPA, E-Science, FRGS, ERGS, PRGS, HIR, and IIRG from FCSIT. Besides collaborators from Malaysia, he has international collaborators from France, the U.K., New Zealand, Pakistan, Turkey, Saudi Arabia, Taiwan, Hong Kong, and China. He also established connections with national and international collaborators, including some industrial partners in Malaysia and other countries. He has published more than 70 academic papers in respectable journals. He was one of the first few pioneers who managed to publish within the top 1% of ISI journals from FCIST. He received a very good number of citations in the Web of Science database. He was also one of the first pioneers to successfully file a patent in FCSIT. Until now, he has filed up to eight patents, and all the patents were granted. His research interests include bioinformatics (e.g., biosensors and pain research), computer security (e.g., blockchain, information security, steganography, authentication (graphical password), neural networks (e.g., supervised and unsupervised learning methods, such as support vector machines and extreme learning machines), the IoT, grid computing, and e-learning frameworks).