IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 2, Ser. I (Mar. – Apr. 2021), PP 08-20
www.iosrjournals.org

IOV-Based Payment System for Fuel Pump

Sherif K. Hussein[1,] Abubaker Wahaballa[2], Nawal A. Baabdullah[3],.
[1]*Associate Professor, Department of Communications and Computer Engineering ,*
October University for Modern Sciences and Arts, Giza- Egypt,
Head of Computer Science Department, Arab East Colleges for Graduate Studies, Riyadh, KSA
[2]*Assistant Professor, Arab East Colleges for Graduate Studies, Riyadh, KSA*
[3]*Master of Computer Science, Arab East Colleges for Graduate Studies, - Riyadh, KSA*

Abstract
Internet of things (IoT) is one of the top emerging technologies in the world today, which refers to the billions of physical devices around the world that are now connected to the internet. Internet of Vehicles (IoV) is one of key members of IoT that allows vehicles to exchanges information and use wireless communication to provide more services and applications that serve humans, ensure efficiency, produce safety and security. The payment system is considered as variable element since it is closely linked to the e-commerce and the development of technology. Beside that, the technology has established significant scope to develop the payment system industry according to consumer requirements and service provider. This paper proposes a secure payment system based on Internet of vehicle that provides many services such as billing a fuel pump. The authors presents concept of payment system from different aspect to produce suitable design that reduce consumer's security concerns and increase consumer trust on this payment system method.

Keywords: *Electronic Payment System, Internet of Vehicle, Security Mechanism, Security Requirement.*

Date of Submission: 01-03-2021 Date of Acceptance: 14-03-2021

I. Introduction

E-payment system is a system used for selling and buying things, goods, services or financial transaction, through the internet. It is an electronic system without using any cash or checks [1]. The electronic payment system has grown increasingly due to growth that happen with e-commerce and technology development over the last decades. As the increment in using these electronic payment system and online payment transactions, that is offset by a decrease in the rate of use of cash money.

There are a wide varieties of e-payment systems that already used. These systems can be broadly classified into two types: account-based and electronic currency systems. In Account-based systems, user can make payment process through personal bank accounts, while in electronic system, payment process be happened only if user possesses an adequate amount of electronic currency. All these payment systems provide number of methods that include: Electronic payment cards (debit, credit, and charge cards), E-wallets, Virtual credit cards, Mobile payments, Loyalty and Smart cards, Electronic cash (E-cash), and Stored-value card payments [2].

Credit Cards is considered as the most commonly used online payment system. The security was a concern for this method but later on with the provision of more secure features to protect every transaction, user developed trust on the use of credit card payment system. To secure users' personal information, credit card companies developed Complementary system that includes MasterCard Secure Code and Verified by Visa [2].

Smart card: The outside shape looks like credit card, but actually it is different as the smart card has embedded chips that can hold a lot of information than credit cards. It can be supported with multiple applications and produce security. In smart card the personal information like account number, medical record and payment details can be protected/secured by encryption and PINs [3].

Mobile Wallets: it is a virtual wallet in smartphone device, which contains money that stored in virtual form. Actually this wallet is about merging software and hardware in a certain device to replace the using of traditional credit card payment by smart phones [4]. Mobile wallet has multiple functions such as user to user payment, secure registration and access in the wallet, storing of information about bank accounts, various numbers of credit and debit cards, virtual currencies, and coupons. Other functions are secure provisioning of credentials, secure downloading from applications and management of multiple mobile payment services [5].

Security in E-Payment System

Electronic payment system are threatened by the security issues, that are changing extremely quickly. These threats include worms, viruses and Trojan horses. Malicious programs can attack any electronic device

such as computers and smart phones, and can attack mobile payment system by tracing password on web browser or any cashed information stored in operating system. Worms can be classified as special viruses that are using direct internet to spread. Viruses disrupt electronic communications because of that it is classified as Denial of Service (DoS) tool. Viruses can infect files via emails or by downloading infected files. These days there are so many different types of malicious programs and computer viruses [6]. The Trojan horses is different type of Malicious software, its goal to spy on sensitive data (e.g. passwords, confidential data, etc.). Trojan horse programs pose the greatest threat to electronic payment systems because they can exceed or subvert the authorization mechanisms and authentication that are used in electronic transaction. The security of payment system is a set of techniques, systems and computer programs, which are used to verify source of data and guarantee the trustworthiness and protection of the data (information). Table 1 shows the list of the security mechanisms that are used to implement the e-payments system [7]. The most important factors for every e-payment system are privacy and security, which are essential demands for every party involved in e-payment system.

Table 1. *Basic building blocks of security mechanisms*

Name of security mechanisms	Description
Encryption	It provides confidentiality, authentication, and integrity
Digital signatures	It provides authentication, integrity protection, and non-repudiation
Checksums/hash algorithms	It provides integrity and authentication

Security Requirements for E-Payment System

Security payment system is involving sensitive data during transactions, these data need to transfer in secure way that guarantee protecting data from attacker and ensuring data safety. To consider system as a secure payment system it must satisfy the following fundamental security requirements:

1. Unforgeability: It means only authorized users allowed to make transactions.
2. Data confidentiality: To protect data from unauthorized disclosure. If there is a public network, the only solution to ensure confidentiality is through strong encryption. Confidentiality is an essential component as a deterrent to theft of information services, also in the protection of proprietary information.
3. Data Integrity: to ensure that data received is exactly the same data that sent by the authorized party, to prevent any modification on data.
4. Anonymity and traceability: Anonymity is to ensure confidentiality for user identity [8]. Traceability means ability to trace user transaction. User can be considered as untraceable if there is no linked message to this user identity or to any previous sent message [9].
5. Non-Repudiation: User cannot deny his/her confirmed payment. In addition, controller system cannot repudiate the origin and correctness of receipt information. Either user or controller cannot deny that transaction is done between them [10].
6. Unlinkability: It means no one can link two payments that made by the same user except user himself.

OBJECTIVES OF THE STUDY

To analyze Security Threats of IoV-Based payment system, defining the security requirements and implementing the system by developing secure application.

II. Literature Review

Adam Ali.Zare Hudaib (2014) reviewed several security methods and payment protocol that used in payment systems. Secure Sockets Layer (SSL) is a protocol used to preserve server and client authentication. Communication between server and client in SSL is encrypted. Transaction Layer Security protocol (TLS) is used based on SSL. Because of TLS flexibility and not having a client certificate, it is clearer and more precise specifications. Near field communication (NFC) is a method that used for payment system. NFC is covering a few inches, its set of standard used on smartphone or any device similar to smart phone. NFC used to establish radio communication between devices. The payment done by NFC needs to have physical device, deduction can done on pre-paid account or charged account [11].

Zlatko Bezhovski (2016) evaluated growth in electronic payment system and mobile payment. Security requirements that can ensure secure transaction include data integrity, authentication, non-repudiation and confidentiality. In other side, lack of security and consumer trust become the most important challenge with mobile payment transaction. The author inferred that, using security protocols with latest technology such as radio bar codes and mobile payment services could provide more convenient system to consumer [12].

Zhen Qina , Jianfei Suna , Abubaker Wahaballaa , Wentao Zhenga , Hu Xiongb, Zhiguang Qin (2016) identified some design requirement to protect privacy and security at mobile wallet. The authors proposed a novel approach to protect privacy and security of mobile by incorporating the pseudo-identity techniques and digital signature. Digital signature can guarantee authentication and non-repudiation of payment transaction.

Also, digital signature can be achieved by different approach such as traditional public key infrastructure (PKI), identity-based cryptography and digital signature based on the idea of certificateless signature. The author used certificateless signature approach and presented a lightweight privacy-preserving authentication protocol to secure mobile wallet. The proposed protocol, which based on certificateless signature and pseudo-identity techniques, can satisfy unforgeability, anonymity, non- repudiation and traceability for payment transaction. In additional, authors mentioned RFID as a technology that used with different mobile payment protocol. RFID is composed of RFID reader and tag, which responds with the identity (Unique ID) to the reader [13].

Burhan Ul Islam Khan, Rashidah F. Olanrewaju, Asifa Mehraj Baba, Adil Ahmad Langoo, Shahul Assad (2017) presented different definitions for online payment system. This study compared debit cards to credit cards, payment that done by debit card are withdrawn from the user's personal bank account and not from any intermediary account. The costs afford by the using of debit cards are less than cost of using credit cards, which make them suitable for small payment. But for Mobile payment method, it Consumes low cost overall transaction and provides better security [14]. Swapna Khandekar, Richard Kolk and Jingyuan Liang (2017) suggested secured payment protocol model that based on Self Certified key generation to increase level of security. A self-certified key generation protocol provides advantages of certificate-based and identity-based public key cryptosystems. [15]. S Fatimah, A Yulandari and F W Wibowo (2018) reviewed the previously researches to identify gap that have been missed on studies that made for e-payment system. After analysis, previous researchers recommended to increase studies on how to raise customer interest in using e- payment systems, to establish trust in e-payment system and more reaches on future of e-payment system [16].

M. Kavitha, D. Atchaya, S. Pavithra (2019) proposed Intelligent Vehicle Technology and Combustion fuel alert based on IoT. Cloud computing is a major technology that acts as central server used to keep information and important record. This system is implemented for wheeler; the cloud is used to store data. It is grouping of multiple sensors and actuators. Some of sensors are as: speed sensor and terrain sensor that can help to track the mileage of the vehicle. IoT as a technology that allows different objects to communicate through internet was the main concept along with cloud computing feature, which help author to design proposed system with support of GPS technology [17].

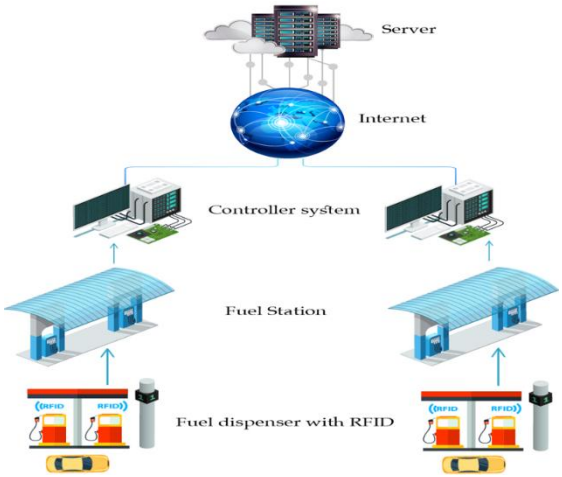
Chaithranjali R S, Lakshmi M, Vandana H S, Khateeja Ambareen (2019) introduced a secure transaction schema for mobile payment by using certificateless cryptographic primitives. The authors found that certificateless signature (CLS) is a suitable solution for their proposed system, which does not require a certificate and also avoid key escrow problems. CLS contains six phases, Setup, PartialPrivateKeyExtract, SetSecretValue, SetPublicKey, Sign,and Verify. In additional, this system were implemented on Android Pay as the Android is one of most popular platform. The proposed system involved intelligent mobile objects that provide needed computation power to perform cryptography mechanism through transaction. Transaction schema for key agreement relies on elliptic curve assumption as a secure component [18].

THE NEWLY PROPOSED SYSTEM

System Overview

Payment system based on IoV technology is provided on vehicles and smart fuel stations, which allows vehicle to communicate with other objects like fuel pump machine, objects inside the same vehicle, RFID reader, etc. Once the vehicle enters the fuel station and has detected by FRID reader, Identification of vehicle (RFID tag) should be sent to controller system. Controller system that works in background verify vehicle's ID, according to that vehicle type that sent the fuel filling order and attaches the payment process request after the vehicle taking the correct position for filling. When the driver arrives at the fuel station in order to fill the fuel, it requires the driver to stop the car near the fuel pump properly. Specific application should be installed in vehicle; it contains friendly interface display on dashboard with different services. If the user uses the application for the first time, he needs to register and create a new account in the system. Account should have many information related to user and his car like vehicle's ID, user personal details and payment account number. After the registration process is completed, all user information will be stored in the database server which accessed by controller system. The controller system is responsible for managing fuel filling, payment transaction, and update user information and handling refund process, it should associate each user with unique ID, which will be the vehicle identification that detected by scan RFID tag. After the RFID reader detecting a vehicle by RFID tag, will pass this information to controller, then the controller is sending the filling order attached with payment process request to user's application and waiting for the user to respond. Depending on the type of vehicle, there will be a list of the required fuel level and price for each fuel level. The user needs to choose an option to move later to payment process. User must provide confirmation on payment process to finish the purchase. Confirmation process needs 4-digit number code that will be sent each time to user phone number once he wants to make payment process to finalize the transaction securely. Figure 1 presents the system architecture.

***Figure 1** System architecture*

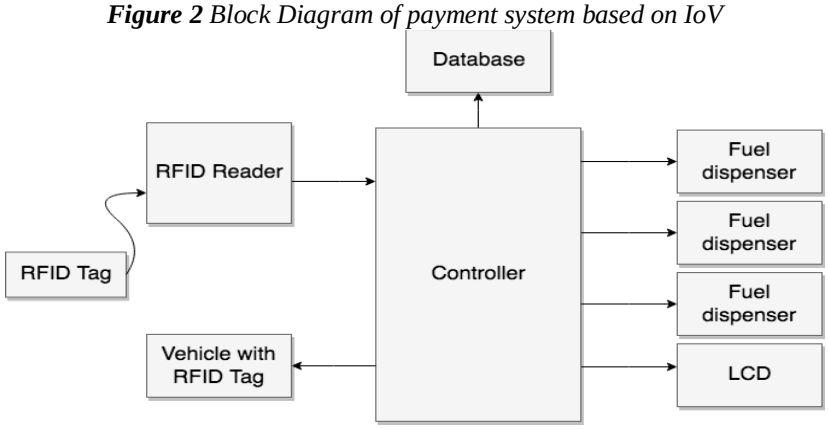


One of features that application provides is a warning issued to the user when fuel level at his vehicle reaches 25%, also the application is showing all the stations nearby the driver's location on dashboard screen by using GPS service.

System Block Diagram

In the proposed system, there are two stages for complete payment process and filling process. The application installed in vehicle with a user interface can be programmed in Java language .The controller system contains processor, memory card and database. The application has an interface that allows user to register in the system or login, to choose the required fuel level and to complete the money transaction process. Controller system is connected to the vehicle by ID, and to the user by an application that communicates with database server. Besides that, controller must receive vehicle's ID (tag) which comes from RFID reader to order fuel filling process for specific user according to his choices. Figure 2 represents block diagram for fuel pump process based on IoV that contains RFID technology.

***Figure 2** Block Diagram of payment system based on IoV*



Functional Requirements

Electronic payment system that located in vehicle should provide many different services such as:

- The system must provide the means for registration in order to make transactions.
- The system must enable user to login/logout.
- The system should allow user to edit personal information/payment account.
- The system must show alert to user that fuel level reaches 25% or less of fuel tank.
- The system enable user to choose specific task from Dashboard to operate.
- Dashboard displays the nearest fuel station once user ask for that or when fuel level is equal or less than 25% of fuel tank.
- The system should allow the fuel filling to vehicle.
- The system must allow user to choose fuel level need to be filled.
- The system should ask user to confirm the purchase process.
- The system must be able to refund amount of money in case of dispute.

Security Requirements

Security payment system is involving sensitive data during transactions, these data need to transfer in secure way that guarantee protecting data from attacker and ensuring data safety. To consider system as a secure payment system it must satisfy unforgeability, data integrity, data confidentiality, non-Repudiation, unlinkability, anonymity and traceability.

Non-Functional Requirements

Non-functional requirements describe the different sorts of requirements that are required for the smooth and proper functioning of the electronic payment system for fuel pump, which affect level of satisfaction with the system. Certain requirements are mentioned below.

- **Usability**

System should be easy to use for user, which can be measured by learning time that required from user to use application properly. This function can be provided in payment system by simplifying the interface to be easy, clear and friendly, which should be introduced on dashboard with an organized menu. Providing online channel between user and system to respond for any query that provided to help the user. Also the system can receive suggestion/feedback that improve the development of system later.

- **Reliability**

As the information required in payment system is sensitive and secure, the system must have capability to maintain its performance over the time. Besides that, system should be able to recover after any failure, although failure rate in such a secure payment system should be very low to consider system as reliable.

- **Performance**

Performance is an important criterion in any electronic payment system. Performance here is indicating the ability of system to process so many transactions per second without any failure to ensure performance. Performance can be measured by how well the system performs the process to reach to the required response time.

- **Automated**

Automate the fuel station allow customer to have the services any time and anywhere especially if the location of station is outside the city.

Hardware and Software Tools

Electronic Payment system is an application software that will be developed to work on dashboard, and based on Android system. Java programming language will be chosen to implement the system. In this part the authors introduce the hardware and software requirements that are needed to implement the electronic payment system based on IoV for fuel pump.

Hardware in the proposed system contains a controller system, which is a computer with special specifications such as High-speed processor and bigger storage capacity. Fuel station will have a RFID system that includes RFID reader and RFID tag. The RFID readers are to be installed at fuel dispenser, while the vehicle has a chip that hold RFID tag. System on Chip (SoC), it is a microchip integrated with all necessary computer components for a particular system onto single integrated chip (IC). These components include a central processing unit (CPU), graphical processing unit (GPU) and built-in memory (RAM). Software that will be used to implement the project are Android studio, Firebase Services, Paypal business account and Google Maps Platform APIs.

RFID Technology

Radio frequency identification (RFID) is a technology works on radio waves. It uses radio frequency to automatically trace or uniquely identify an object. RFID system consists of RFID tags (transponder), RFID readers (transceivers), antenna, communication infrastructure and application software [19]. RFID tag is used to transfer data to reader and carry object-identifying data while RFID reader is a device that is used to read out tags through radio signals and convert radio waves to more usable form of data [20]. The communication happened between tag and reader inside RFID system is based on radio frequency.

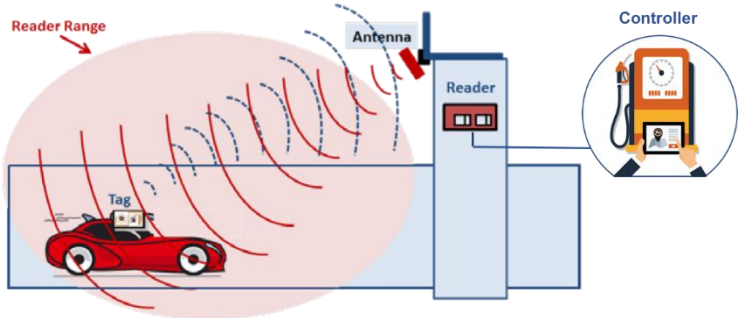
RFID Tag contains chip that store unique identification of each object, and the size of chip depends on antenna. Information provided by the tag can be ID or location or specific data of object like expire date. There are three types of tag according to its energy or power: [21]

- Active tag contains internal power supply that uses power circuits to transfer data to reader.
- Passive tag with no internal power supply which cause chip to be in sleep mode until receiving radio waves from reader.
- Semi-passive tag which takes place between passive and active tags, because its power circuits is provided by radio waves from reader.

RFID reader is a device that retrieves data stored on tag by using RFID antennas. RFID reader scan

specific era, which is called RFID reader range that depends on the type of tag. After scanning tags this information forwarded to backbone that consists of database and application interface [22]. Figure 3 shows the typical RFID system [23].

Figure 3 *The typical RFID system*

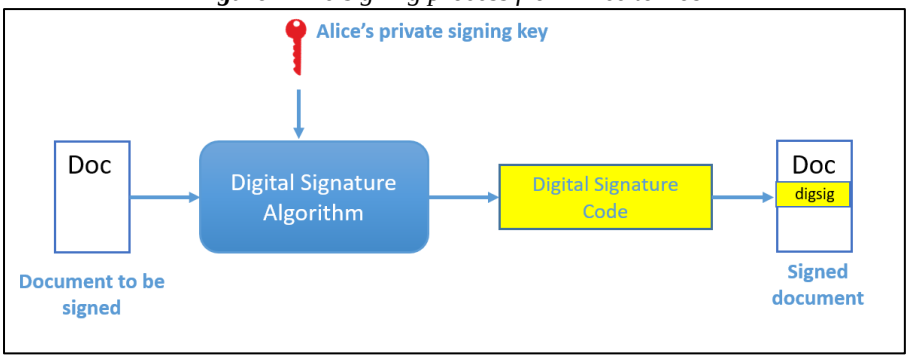


Digital Signature and Certificateless Signature (CLS)

Digital signature considered as one of most important security technology in cryptography. Digital signature is a concept that ensure authentication, data integrity and non-repudiation. It is a public key algorithm that guarantees authenticate message by using a piece of information called signature [24]. Digital signature algorithm uses two different keys, private key, which used to make signature and public key that used to verify signature. Public key is known to every one so any one can verify signature but for private key (secret key) is only known to sender who can sign the message [25].

Supposed that there are two parties Alice (sender) and Bob (receiver) with message M, Alice has a private key that used to sign message and Bob has a public key, which used to verify signature. Security of digital signature depends on ensuring that only Alice can access her private key. Only Alice can make digital signature on message, since she is the only person who has access to private key, from this point, the authentication and non-repudiation property are guaranteed. Each digital signature is related to the document, therefore the signature cannot be copied from one document to another [26]. Figure 4 shows the signing process from Alice to Bob [26].

Figure 4 *The signing process from Alice to Bob*



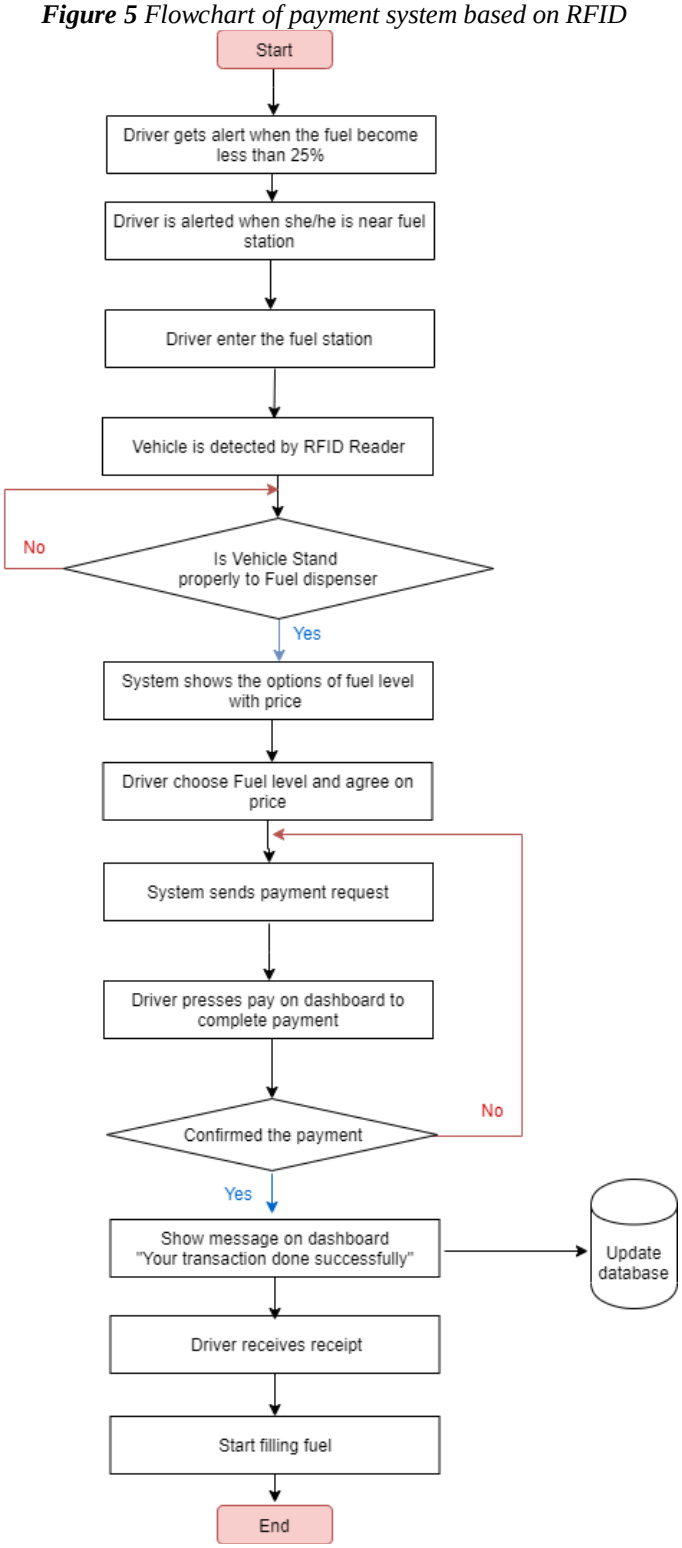
In the traditional public key infrastructure (PKI), the digital certificate could be issued by certificate authority (CA) to verify user's public key. This process is costly, needs high communication and large storage for computing. To reduce these resources, another approach named identity-based cryptography (IBC) can be used,. Identity-based cryptography (IBC) depends on third party called Private Key Generator (PKG) that generates a public/private keypair, In IBC the user's public key is derived from name, email Id or phone number (or any identity information). The most benefit of this approach is that there is no need to have PKI, so less of public information can be shared with others who actually do not need to know. However, IBC is suffering from key escrow problem since that PKG is a third party that generate the entire key [27].

Certificateless public cryptography (CL-PKC) is an approach that avoids key escrow problem in IBC. CL-PKL, key generator center (KGC) is computing partial private key; where other part of private key is chosen as a secret value by user, while user's public key computed from KGC's public parameters and secret value given by user. In additional, CL-PKC does not require a digital certificate for authentication [28]. Key generation center could replace public key infrastructure for Identity-based encryption by computing user's private key. KGC is computing partial private key and not the entire key, second part of key will be given by the user as secret value [29].

Flowchart of system

When the user crosses the fuel station entrance, RFID reader will be ready to scan vehicle ID when it is in the frequency range. The RFID readers are to be installed at fuel dispenser to enable the system to manage each client easily and to prevent the collision that could be happened when RFID is trying to read more than one vehicle at the same time. The Controller checks its own database for the user based on his/her vehicle ID to prepare the suitable order. Transaction process starts and execute using the verification code that will be sent to user mobile number to ensure the authentication process. Figure 5 shows the flowchart of payment system based RFID.

Figure 5 *Flowchart of payment system based on RFID*



IMPLEMENTATION AND TESTING

Project Techniques

1. Build a new project in Android studio

Any project in Android Studio involves at least one or more modules along with resource files and codes, which all connected to main project file.

First: AndroidManifest.xml is important file in each Android Studio project that describes essential information about the application to the Android build tools, the Android operating system, and Google Play. Manifest.xml contain the following code

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission
android:name="com.google.android.providers.gsf.permission.READ_GSERVICES" />
<uses-permission android:name="com.vivianaranha.mapsapp.permission.MAPS_RECEIVE" />
<uses-permission
android:name="com.google.android.providers.gsf.permission.READ_GSERVICES" />
<uses-feature
   android:glEsVersion="0x00020000"
   android:required="true" />

<activity android:name=".PermissionsActivity" />
<activity android:name=".Map2Activity" />
<meta-data
   android:name="com.google.android.geo.API_KEY"
   android:value="AIzaSyBeBBIW8A38dazl0kW6NtPy4TgOz6M1gjQ" />
<meta-data
   android:name="com.google.android.gms.version"
   android:value="@integer/google_play_services_version" />
<activity android:name=".ThankYouActivity" />
```

Second: Dependencies allow authors to access and add many libraries to the project with less efforts and size. Build.gradle file contain the following code

```
dependencies {
   implementation fileTree(dir: 'libs', include: ['*.jar'])
   implementation 'com.google.firebase:firebase-database:19.2.1'
   implementation 'com.google.firebase:firebase-core:17.2.3'
   implementation 'com.google.firebase:firebase-storage:19.1.1'
   implementation 'com.firebaseui:firebase-ui-database:3.2.2'
   implementation 'com.squareup.picasso:picasso:2.71828'
   implementation 'com.github.rey5137:material:1.2.5'
   implementation 'androidx.cardview:cardview:1.0.0'
   implementation 'androidx.recyclerview:recyclerview:1.1.0'
   implementation 'androidx.appcompat:appcompat:1.1.0'
   implementation 'io.paperdb:paperdb:2.6'
   implementation 'de.hdodenhof:circleimageview:3.1.0'
   implementation 'androidx.constraintlayout:constraintlayout:1.1.3'
   implementation 'androidx.legacy:legacy-support-v4:1.0.0'
   implementation 'com.google.android.material:material:1.1.0'
   implementation 'androidx.lifecycle:lifecycle-extensions:2.2.0'
   implementation 'com.theartofdev.edmodo:android-image-cropper:2.8.0'
   implementation 'com.google.firebase:firebase-auth:19.3.0'
   implementation 'com.craftman.cardform:cardform:0.0.2'
   implementation 'com.paypal.sdk:paypal-android-sdk:2.15.3'
   implementation 'com.github.mancj:MaterialSearchBar:0.8.1'
   implementation 'com.google.android.libraries.places:places:1.1.0'
```

```
    implementation 'com.skyfishjy.ripplebackground:library:1.0.1'
    implementation 'com.github.iammert:ReadableBottomBar:0.2'
    implementation 'com.google.android.gms:play-services-location:16.0.0'
    implementation 'androidx.navigation:navigation-fragment:2.2.1'
    implementation 'androidx.navigation:navigation-ui:2.2.1'
    implementation 'androidx.multidex:multidex:2.0.1'
    implementation 'com.github.mancj:MaterialSearchBar:0.8.2'
    implementation 'com.google.android.gms:play-services-maps:16.1.0'
}
```

Third: Android Studio Activity, In order to create the main page in Android Studio, first the author need to create new activity which establish two files (PaymentActivity.java – activity_payment.xml). Payment activity file contains all java lines to run the first page, while payment.xml contain the file layout. PaymentActivity java code is contain the following code:

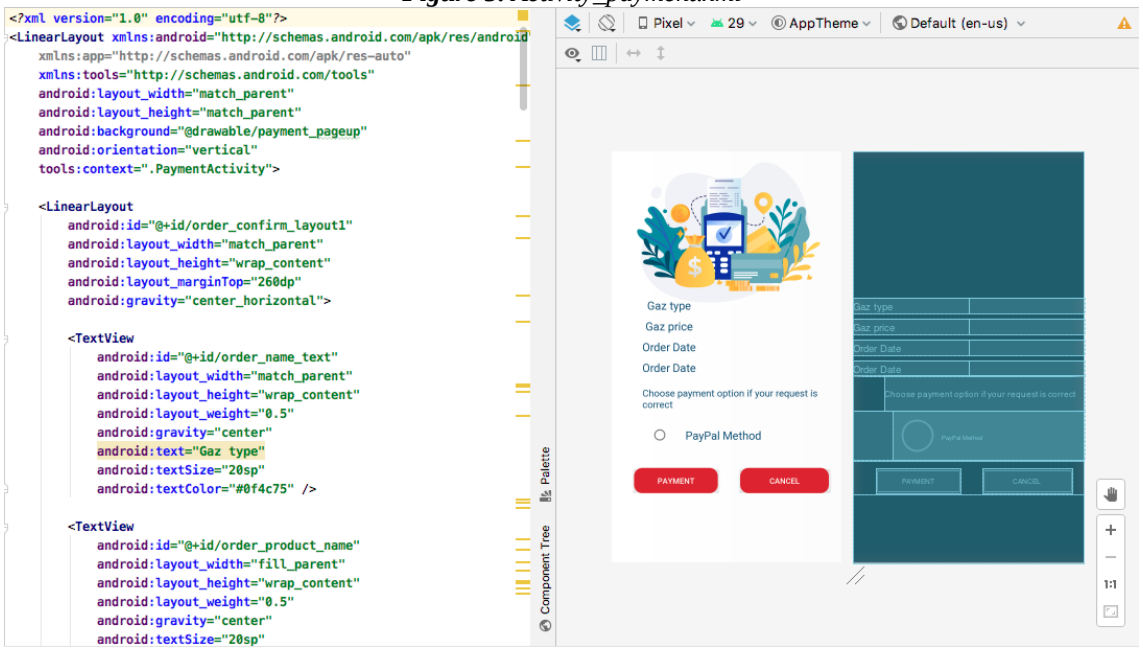
```
public class PayPalPaymentActivity extends AppCompatActivity {

    public static final int PAYPAL_REQUEST_CODE = 7171;
    String amount = "";
    Order order;
    private DatabaseReference databaseRef, ref, rootRef, rootRef2;
    private FirebaseAuth mAuth;
    String currentUserID;

    @Override
    protected void onDestroy() {
        stopService(new Intent(this,PayPalService.class));
        super.onDestroy();
    }

    private static PayPalConfiguration config = new PayPalConfiguration ().environment
(PayPalConfiguration.ENVIRONMENT_SANDBOX)
            .clientId (Config.PAYPAL_CLIENT_ID);

    private static final String CONFIG_ENVIRONMENT =
PayPalConfiguration.ENVIRONMENT_SANDBOX;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate (savedInstanceState);
        setContentView (R.layout.activity_pay_pal_payment);


        mAuth = FirebaseAuth.getInstance();
        currentUserID = mAuth.getCurrentUser().getUid();
        rootRef =
FirebaseDatabase.getInstance().getReference().child("Users").child(currentUserID).child("phone");
        rootRef2 =
FirebaseDatabase.getInstance().getReference().child("Users").child(currentUserID);

        //start paypal service
        Intent pintent = new Intent (this, PayPalService.class);
        pintent.putExtra (PayPalService.EXTRA_PAYPAL_CONFIGURATION, config);
        startService (pintent);

        mAuth = FirebaseAuth.getInstance ();
        currentUserID = mAuth.getCurrentUser ().getUid ();
        ref = FirebaseDatabase.getInstance ().getReference ().child ("Users").child
(currentUserID).child ("Order");

        ref.addListenerForSingleValueEvent (new ValueEventListener () {
```

```
        @Override
        public void onDataChange(@NonNull DataSnapshot dataSnapshot) {
            if (dataSnapshot.exists ()){
            Order order = dataSnapshot.getValue (Order.class);
            amount = order.price;
            processPayment(amount);}
            else {

            }
        }

        @Override
        public void onCancelled(@NonNull DatabaseError databaseError) {

        }
    });
}

private void processPayment(String amount) {

    PayPalPayment payPalPayment = new PayPalPayment (new BigDecimal (String.valueOf
(amount)), "USD",
            "Paid Fuel App", PayPalPayment.PAYMENT_INTENT_SALE);
    Intent intent = new Intent (this, PaymentActivity.class);
    intent.putExtra (PayPalService.EXTRA_PAYPAL_CONFIGURATION,config);
    intent.putExtra (PaymentActivity.EXTRA_PAYMENT, payPalPayment);
    startActivityForResult (intent, PAYPAL_REQUEST_CODE);
}
protected void onActivityResult(int requestCode, int resultCode, Intent data)
{
    super.onActivityResult (requestCode, resultCode, data);
    if (requestCode == PAYPAL_REQUEST_CODE) {
        if (resultCode == RESULT_OK) {
            PaymentConfirmation confirmation = data.getParcelableExtra
(PaymentActivity.EXTRA_RESULT_CONFIRMATION);
            if (confirmation != null) {
                try {
                    String paymentDetails = confirmation.toJSONObject ().toString (4);
                    startActivity (new Intent (this, PaymentDetailsActivity.class)
                            .putExtra ("Payment Details", paymentDetails)
                            .putExtra ("Amount", amount));

                    rootRef2.child ("payment_status").setValue ("1");

                    sendToThankyouActivity();

                } catch (JSONException e) {
                    e.printStackTrace ();
                }
            }
        } else if (resultCode == Activity.RESULT_CANCELED)
            Toast.makeText (this, "Cancel", Toast.LENGTH_SHORT).show ();
    } else if (resultCode == PaymentActivity.RESULT_EXTRAS_INVALID)
        Toast.makeText (this, "Invalid", Toast.LENGTH_SHORT).show ();
}

private void sendToThankyouActivity() {

    Intent thankIntent = new Intent(PayPalPaymentActivity.this, ThankYouActivity.class);
```

```
        thankIntent.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK |
Intent.FLAG_ACTIVITY_CLEAR_TASK);
        startActivity(thankIntent);
        finish();
    }

}
```

As each activity contains files, java code and non-java code, activity_payment.xml code is shown in Figure 5.

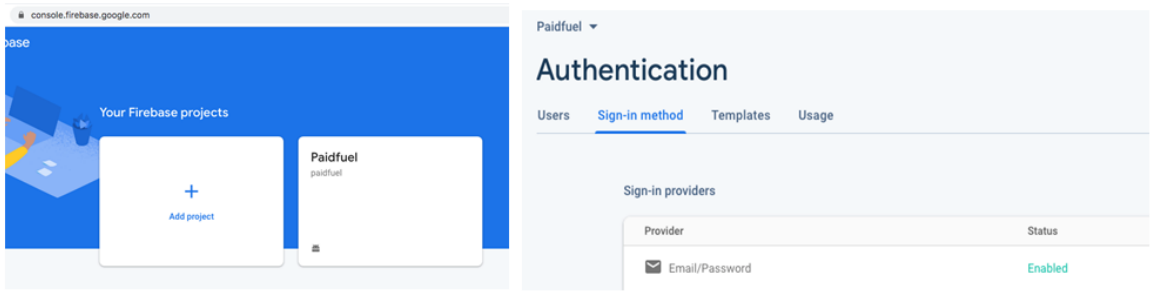
Figure 5. *Activity_payment.xml*



2. Connect project with Firebase database

Firebase is a web application platform that help developers to store, update and retrieve data with no-SQL single code as it is store data in JavaScript Object Notation (JSON) format. Real-time Database is a services provided by firebase which enables application data to be synchronized across customers and stored on Firebase's cloud [30]. Firebase Authentication is a service that allows author to check credential for each registered user in android application. Figure 6 Illustrates Firebase Console and enabling the authentication .

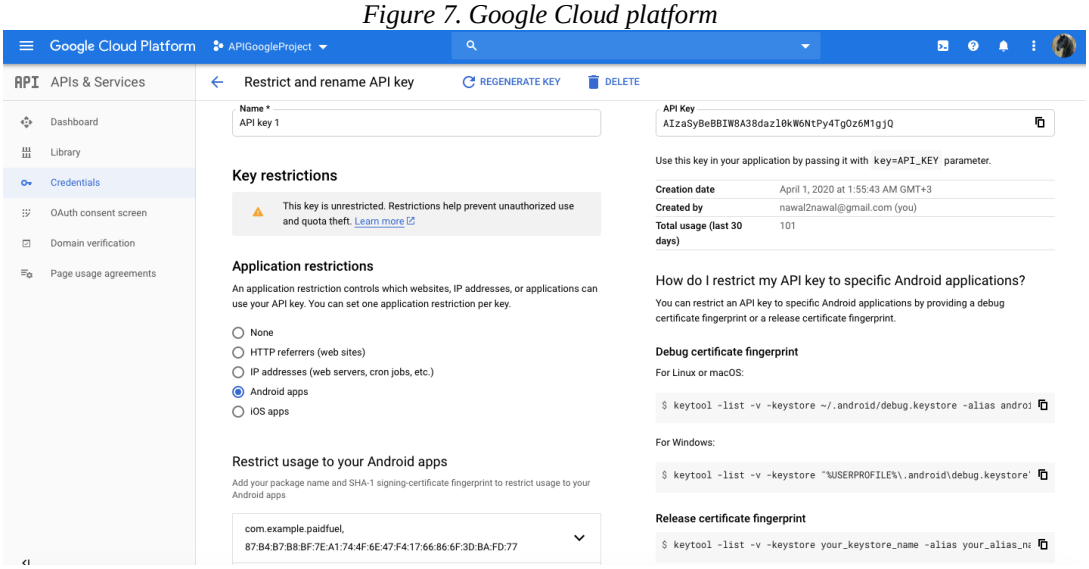
Figure 6. Firebase Console and Authentication



3. Create Google Maps Platform APIs

To use places SDK in Android project, first must get API key. The API key is a unique identifier that is used to authenticate requests associated with the project for using Google Map services. The author creates new account at Google Cloud platform to establish unique API key. The same key is used in android studio project in the map activity java code to request google map services. Figure 7 shown Google Cloud platform after connecting Android project with APIs key.

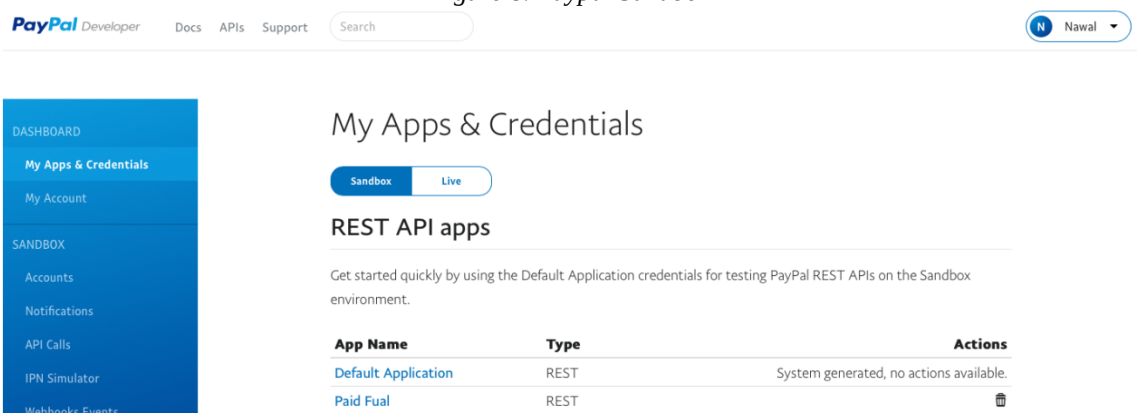
Figure 7. Google Cloud platform



4. Create Paypal Sandbox

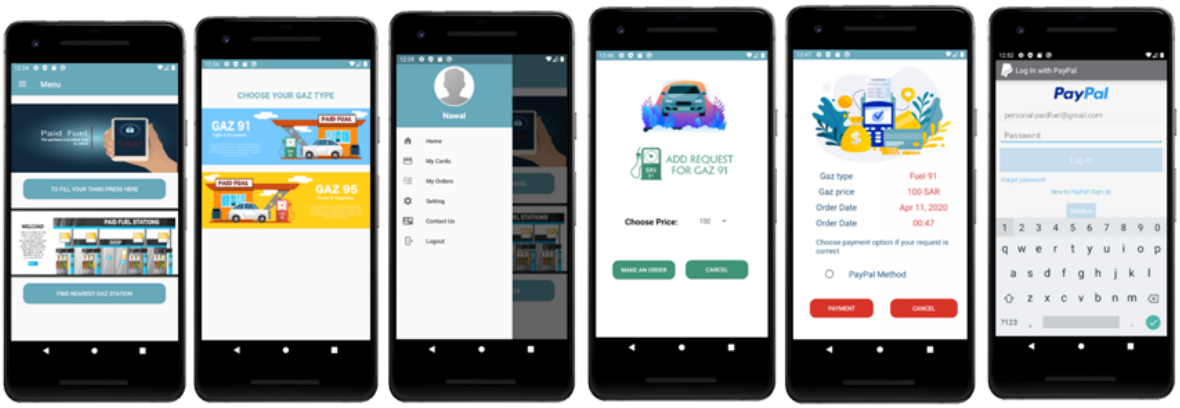
The PayPal sandbox mirrors the features on the PayPal production servers. It is free version that allow the author to test business Android application before publishing this application to market. Figure 8 presents Paypal Sandbox.

Figure 8. Paypal Sandbox



After all these component executing together, the Android application can get the final result shown in Figure 9.

Figure 9. Android Studio application result



III. Conclusion And Future Work

This paper introduced the concept of the IOV technology. A list of previous techniques had been discussed in details. In line with the fast revolution in economic and technology in the world vision, the author tried to match the demand of this vision and keep it in mind by proposing a new model serving the payment for the fuel pumps. The newly proposed system is based on designing a system that allows user to make an electronic payment transaction for fuel pump using RFID technology. It is composed of controller and an application that execute simultaneously to make secure payment transaction for fuel pump filling. Objects will communicate based on IoV technology. The proposed system will guarantee privacy and security of the payment by using digital signature technology. Also, efficiency will be enhanced by using database server and clouds that will allow user to use the payment system in different fuel stations reliably and securely. This project is implemented by Android Studio software to ensure secure transaction for each registered user requesting for paid fuel. Future work will be dedicated for improving proposed IOV payment system for fuel pump by adding new technologies to the payment process.

References

[1]. Jerrin Yomas, Chitra Kiran N. (2018). A Critical Analysis on the Evolution in the E-Payment System, Secuiry Risk, Threats and Vulnerability, Communications on Applied Electronics (CAE), Volume 7– No. 23.

[2]. Zlatko Bezhovski. (2016). The Future of the Mobile Payment as Electronic Payment System, European Journal of Business and Management, Vol.8, No.8, Page 128.

[3]. Craig M. Parker and Paula M. C. Swatman. (2002). Electronic Payment Systems, School of Information Systems.

[4]. Mansi Prakashbhai Bosamia. (2017). Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures, ResearchGate.

[5]. Kremena Marinova-Kostova (2017). Mobile wallet – functions, components and architecture, ResearchGate, Page 1-2.

[6]. Bogdan-AlexandruURS. (2015). Security issues and solutions in e-payment systems, pages 175-176.

[7]. Awais Ahmed, Abdul Aziz, Muhammad Muneeb. (2019). Electronic payment system: A complete guide", Journal of Multidisciplinary Sciences.

[8]. Raylin Tso. (2018). Untraceable and Anonymous Mobile Payment Scheme Based on Near Field Communication, Symmetry.

[9]. Jan L. Camenish, Jean-Marc Piveteau, Markus A. Stadler. An Efficient Electronic Payment System Protecting Privacy.

[10]. Ajeet Singh, Karan Singh, Shahazad, M.H Khan, Manik Chandra. (2012). A Review: Secure Payment System for Electronic Transaction, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, pages 238-239.

[11]. Adam Ali.Zare Hudaib, "E-payment Security Analysis In Depth", International Journal of Computer Science and Security (IJCSS), Volume (8), Issue (1), 2014.

[12]. Zlatko Bezhovski, "The Future of the Mobile Payment as Electronic Payment System", European Journal of Business and Management, Vol.8, No.8, 2016.

[13]. Zhen Qina , Jianfei Suna , Abubaker Wahaballaa , Wentao Zhenga , Hu Xiongb, Zhiguang Qin, "A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing", Computer Standards & Interfaces, Volume 54, November 2016.

[14]. BurhanUl Islam Khan, Rashidah F. Olanrewaju, Asifa Mehraj Baba, Adil Ahmad Langoo, Shahul Assad. (2017). A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations, International Journal of Advanced Computer Science and Applications, Vol. 8, No. 5.

[15]. Swapna Khandekar, Richard Kolk and Jingyuan Liang. (2017). Secured Payment Protocol, Communications on Applied Electronics (CAE), Volume 6 – No.6.

[16]. S Fatonah, A Yulandari and F W Wibowo. (2018). A Review of E-Payment System in E-Commerce.

[17]. M. Kavitha, D. Atchaya, S. Pavithra. (2019). Intelligent Vehicle Technology and Combustion Fuel Alert Using IOT, International Journal of Recent Technology and Engineering (IJRTE), Volume-8.

[18]. Chaithranjali R S, Lakshmi M, Vandana H S, Khateeja Ambareen, "A Secure Transaction Scheme with Certificateless Cryptographic Primitives Based Mobile Payments", International Journal of Engineering Research & Technology (IJERT), Volume 7, Issue 10, Special Issue – 2019.

[19]. Kamran AHSAN, Hanifa SHAH, Paul KINGSTON. (2010). RFID Applications: An Introductory and Exploratory Study, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1, No. 3.

[20]. Sergei Evdokimov, Benjamin Fabian,Oliver G¨unther, Lenka Ivantysynova, Holger Ziekow. (2010). RFID and the Internet of Things: Technology,Applications, and Security Challenges, Technology, Information and Operations Management, Vol. 4, No. 2.

[21]. Kumar Chaturvedula. (2012). RFID Based EmbeddedSystemfor Vehicle Trackingand Prevention of Road Accidents, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 6.

[22]. Christoph Jechlitschek. (2013). A Survey Paper on Radio Frequency IDentification (FRID) Trends.

[23]. H. Khali, A. Araar, E. Zennal Abdulla. (2014). Suitability of Passive RFID Technology for Fast Moving Vehicle Identification", Journal of Emerging Trends in Computing and Information Sciences, Vol. 5, No. 1.

[24]. Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler, "Security in Electronic Payment Systems", ResearchGate, March 2000.

[25]. Fourcan Karim Mazumder, Israt Jahan, Utpal Kanti Das, "Security in Electronic Payment Transaction", International Journal of Scientific & Engineering Research, Volume 6, Issue 2, February-2015.

[26]. "Basics of Digital Signatures & PKI", Ascertia Limited, pages 1-4.

[27]. Sherman S. Chow, "Removing escrow from identity based encryption", in Proc. 12th Int. Conf. Pract. Theory Public Key Cryptogr., 2009, pp. 256–276.

[28]. Lin Cheng, Qiaoyan Wen, Zhengping Jin, Hua Zhang, "On the security of a certificateless signature scheme in the standard model.

[29]. Pravat Kumar Sahoo, Mrutyunjaya Lenka, "Development of certificate less digital signature scheme & its application in e-cash system".

[30]. Chunnu Khawas, Pritam Shah, "Application of Firebase in Android App Development-A Study", International Journal of Computer Applications (0975 – 8887) Volume 179 – No.46, June 2018.