اونيۏرسيتي تيکنولوݢي مارا

UNIVERSITI
TEKNOLOGI
MARA

Authentication and Access Control

Web Information Security (CSC796)

Name: Siti Syahirah bt Ibrahim

Student Id: 2020559949

Lecturer Name: Assoc. Prof. Ts. Dr. Suriyani Ariffin

1.0 IOT DEFINITION

There's numerous way researchers define the term Internet of Things (IoT) yet, it can be concluded as multiple technological objects interacting with each other without any human interaction through wireless or internet connection. (Tan & Wang, 2010) (Feng Xia, 2012) These technological devices are smart and has unique identifier (UID) which allows them to transfer and receive data through network. (Parul Goyal, 2020)

IoT ecosystems varies based on the usage or implementation of machine or device. **Sensors** are the most famous detector in IoT implementation. Sensors will gather data based on events that are predefined and send these data through **Internet Gateway**. There are multiple methods of passing data such as Wi-Fi, wired LAN or the Internet to avoid network slow down. Next, **Edge IT** is an intermediary stage that analysis to reduce traffic to data centre and take care of bandwidth limitation does not exceed data centre's capability. **Data Center or Cloud** is the destination where report generated based on data submitted. These four are the main phase on how IoT ecosystems works in general.

2.0 AUTHENTICATION AND ACCESS CONTROL

Authentication and Access controls are two different things ins IoT, yet both plays crucial roles in safety of the systems. Access control are ability for certain users to perform only certain task as programmed based on their roles towards the system. Authentication is ability to secure data and limit data to allow authorised user only. (Feng Xia, 2012) In any work fields, authentication and access control technology are the central elements in addressing security of a network. Different devices or technology has different authentication concept which developers needs to build a bridge to combine these communication protocol.

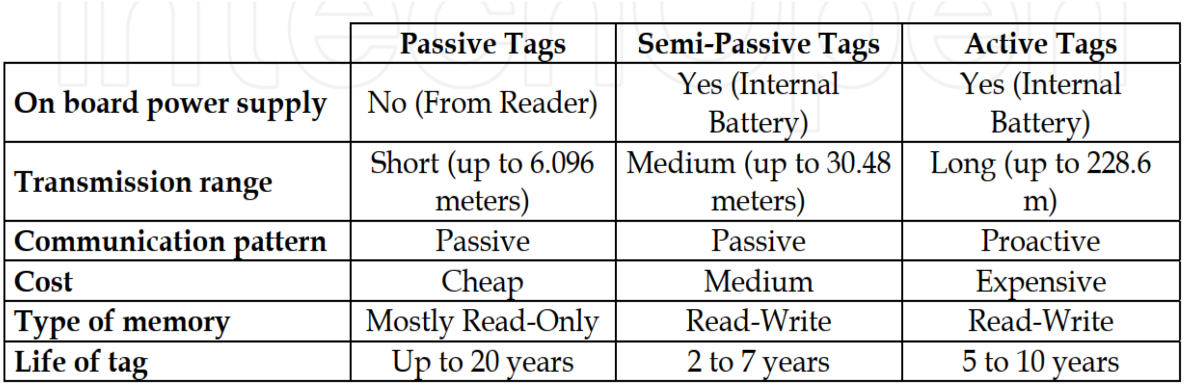
There's numerous authentication protocol available, such as two-factores authentication which implemented by most social media nowadays, Single Sign-On (SSO), Message Queuing Telemetry Transport (MQTT), Blockchain, (Hiral S. Trivedi, 2020) Hash Function, (Prosanta Gope, 2018) Public Key Infrastructure (PKI) and SSL. Each are used on different digital platform while serving different purpose towards the system. The purpose for both communication partners to implement authentication protocol is to have solid communication in the high layer

3.0 FUNCTION BASED ACCESS CONTROL ON RFID FOR VEHICLE TRACKING

RFID is radio frequency Identification which use radio wave tagged on object to transmit data. (Prosanta Gope, 2018) This paper will be revised on implementation of RFID on toll booth which is aftermath from evolvement of IoT. (AungMyint Win, 2014) This paper also will discuss existing framework propose by other researchers and proposed another framework methodology to increase security authentication of RFID usage in Toll booth by analysing the difference in access requirements of different levels of user's role.

Touch 'n Go Sdn Bhd has deployed RFID tag solution based that allows users to pass through toll booth in Malaysia. (KHADIJAH KAMARULAZIZI, 2005) This tag is linked with user's Touch 'n Go e-Wallet, where the toll fares will be deducted. (Touch 'n Go, n.d.) However, this functionality is restricted to toll fares only as the RFID used is passive tag which only has read-only functionality, as the current systems only read RFID tag id, and match with database to find user's account, and deduct the balance from the user's e-wallet. (KHADIJAH KAMARULAZIZI, 2005) This paper proposed a newer solution which benefits both company and users as its functionality allow vehicle tracking which would reduce vehicle theft, allows authorities to track vehicle much better while implementing the current system.

There's three type of RFID tag existed, which are active RFID, passive RFID, and semi passive RFID. (KHADIJAH KAMARULAZIZI, 2005) Figure 1 shows the difference between each RFID tag. The main factors is due to the cost is cheapest with longest life-tag.



	Passive Tags	**Semi-Passive Tags**	**Active Tags**
On board power supply	No (From Reader)	Yes (Internal Battery)	Yes (Internal Battery)
Transmission range	Short (up to 6.096 meters)	Medium (up to 30.48 meters)	Long (up to 228.6 m)
Communication pattern	Passive	Passive	Proactive
Cost	Cheap	Medium	Expensive
Type of memory	Mostly Read-Only	Read-Write	Read-Write
Life of tag	Up to 20 years	2 to 7 years	5 to 10 years

Table 1: Characteristic of passive, semi passive and active RFID tags. (Mehdia Ajana El Khaddar, 2011)

This paper proposes the usage of active tags in replace of the current tags. These tags are embedded onto the vehicle upon registration of vehicles which makes its easier for authorities to identify stolen vehicle, or fake vehicles on the road. Each car will have unique RFID tag upon car registration, where user needs to deposit some amount into user's account which will need to be activated upon car registration.

For toll detection, each time the car approaches a toll booth, infrared sensors will detect the presence of RFID tag and activate the RFID circuit to read the RFID. All tolls are connected with LAN, to allows centralised database and server. As RFID is reader is fast, users do not have to stop at the booth reducing traffic. (S.Nandhini1, 2007)

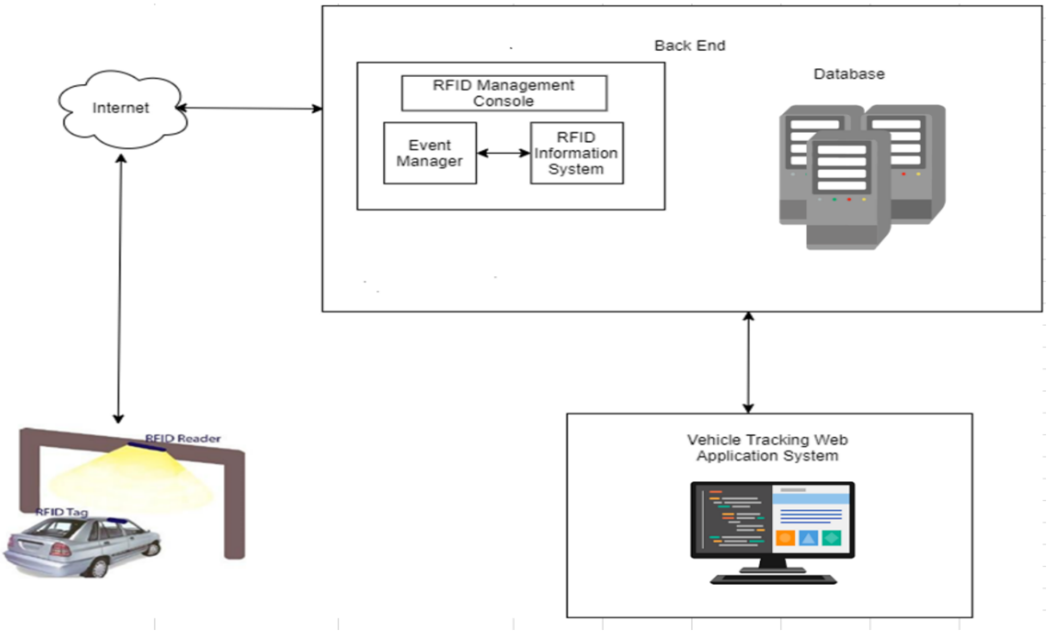
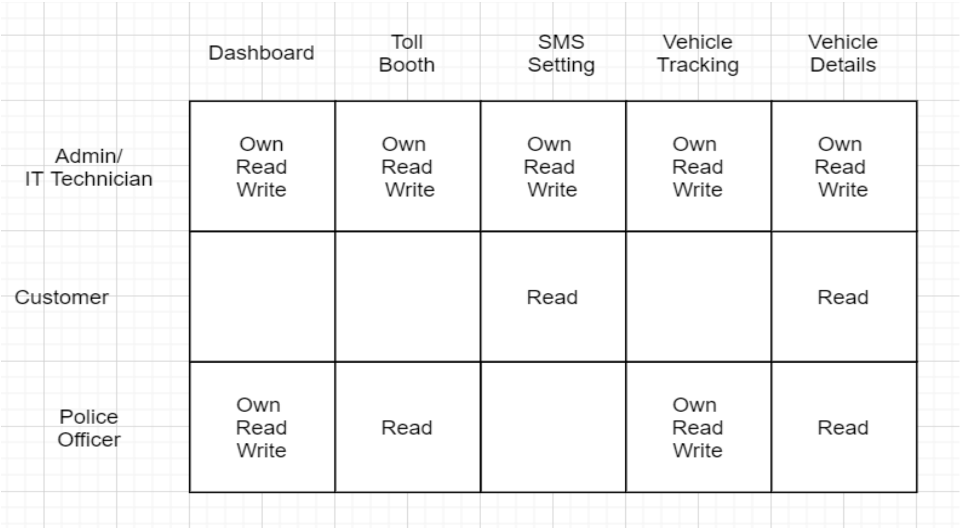


Figure 1: Framework of RFID for vehicle tracking

The figure shows the additional vehicle tracking features of the RFID. The main idea of implementation, for tolls deduction balance from e-Wallet are not touch and kept the same. Yet, the same reader is used to send vehicle location to be save in the database. All these data are passively stored and constantly be replace upon newer location detected. Location detection features are controversial as its features means human are being watch and track wherever we goes, thus, access control are crucial in maintaining the first layer of security beside systems security itself.

The diagram below shows the access control representation.



	Dashboard	Toll Booth	SMS Setting	Vehicle Tracking	Vehicle Details
Admin/ IT Technician	Own Read Write	Own Read Write	Own Read Write	Own Read Write	Own Read Write
Customer			Read		Read
Police Officer	Own Read Write	Read		Own Read Write	Read

Table 2: Access Control Matrix Example

As shown in the table, each subject will have particular access to the IoT network object. These accesses reflect by user's roles in the system. Admin or IT Technician has full control of the system as they are actors with much knowledge in managing the systems. Customer, on the other hand has only Read ability to know sufficient data regarding their RFID tag such as balance account. SMS setting are required for registration and additional authentication method. Police, despite being an authority, still have limit access to avoid and hacking possible if the access control is not limited. They can own and write on important features such as Dashboard and Vehicle Tracking. These to allow them to find vehicle and track them, by dialling certain reactor at the sensor and such.

As access control and authentication comes together, fixed only one features does not ensure the systems will be fully un jeopardize. This may open to more research as active RFID has different safety requirement compare to passive RFID.

References

AungMyint Win, C. M. (2014). RFID Based Automated Toll Plaza System . *International Journal of Scientific and Research Publications, Volume 4*, 1-7.

Feng Xia, L. T. (2012). Internet of Things. *INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS*, 1101–1102.

Hiral S. Trivedi, S. J. (2020). Design of secure authentication protocol for dynamic user addition in. *Computer Network*, 107335.

KHADIJAH KAMARULAZIZI, D. I. (2005). ELECTRONIC TOLL COLLECTION SYSTEM USING PASSIVE. *Journal of Theoretical and Applied Information Technology*, 70-76.

Mehdia Ajana El Khaddar, M. B. (2011). RFID Middleware Design and Architecture. *Designing and Deploying RFID Applications*, 305-326.

Parul Goyal, A. K. (2020). Internet of Things: Applications, security and privacy: A survey. *Materials Today: Proceedings*.

Prosanta Gope, R. A. (2018). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. . *Future Generation Computer Systems 83*, 629–637.

S.Nandhini1, P. (2007). Automatic Toll Gate System Using Advanced RFID and GSM Technology. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 13002-13007.

Tan, L., & Wang, N. (2010). Future Internet: The Internet of Things. *3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)* (pp. V5-376-V5-380). Chengdu: IEEE Xplore.

Touch 'n Go. (n.d.). *TNG RFID*. Retrieved from Touch 'n Go: https://www.touchngo.com.my/CMS/Home/Products/Personal/TNGRFID/