International Journal of System Dynamics Applications
Volume 11 • Issue 3

Introducing Fog Computing (FC) Technology to Internet of Things (IoT) Cloud-Based Anti-Theft Vehicles Solutions

Eissa Jaber Alreshidi, University of Ha'il, Saudi Arabia

ABSTRACT

Securing vehicles, especially against theft, has become a significant concern. Smart antitheft solutions have emerged to provide better protection. However, most existing smart vehicle antitheft solutions use GSM and GPS technologies to track stolen vehicles, and these technologies are not sufficiently efficient in tracking vehicles in real time. Hence, there is a need to optimise solutions to incorporate new technologies such as internet of things (IoT), fog computing (FC), and face recognition (FR) technologies. This paper introduces the new concept of fog computing to existing tracking systems and presents the design and the development of the internet of things (IoT) cloud-based vehicle anti-theft system to pinpoint the exact location of the stolen vehicle in real time. The proposed system extends the existing tracking systems to include advanced features influenced by advanced computing technologies such as fog, cloud, IoT, and FR. Furthermore, it sheds light on the benefits of using FC combined with cloud computing (CC) to provide a more accurate and reliable tracking system.

KEYWORDS

Cloud Computing (CC), Face Recognition (FR), Fog Computing (FC), Global Positioning System (GPS), Global System for Mobile Communications (GSM), Internet of Things (IoT), Smart, Tracking, Vehicle

1. INTRODUCTION

Vehicle thefts have become a significant concern globally, especially in countries suffering social and financial crises and extreme poverty and unemployment (Haider, Khan, & Denai, 2017). This has led to the development of myriad vehicle antitheft solutions, all with their advantages and disadvantages (Ahmed, Marhoon, & Nuri, 2018). Vehicle tracking anti-theft solutions are categorised into three main types: door lock devices, alarm systems, and vehicle tracking systems. Furthermore, they can be classified into active and passive solutions (Monawar, Mahmud, & Hira, 2017). Passive tracking solutions store the GPS location, the state of the vehicle and its directions. These passive solutions store data locally. Once a stolen vehicle is found the tracking device is removed and its content is downloaded onto a computer for assessment. Active tracking solutions are able to collect the same data as passive tracking solutions with the difference that they are able to transmit the data collected in real-time via satellite or cellular network to a data centre for assessment (Feldiansyah Bakri, Nor Erne, Rika, & Hasanuddin, 2018; Monawar et al., 2017).

Typically, anti-theft vehicle systems have steering wheel locks to prevent vehicles theft, alarm systems and GPS trackers. These technologies, however, suffer from technical limitations and significant security gaps, which is why vehicle theft remains prevalent (Constantinescu & Vladoiu,

DOI: 10.4018/IJSDA.287114

2013). These technical limitations and security gaps are a direct result of the lack of upgrades and adaptability of these systems to the latest smart technologies such as Fog Computing, Cloud Computing, and IoT concepts. Furthermore, they are expensive to buy and maintain (Ramani et al., 2013). To address the limitations of existing antitheft vehicle tracking systems, this research proposes an enhancement design for existing anti-theft systems that incorporates relatively new advanced computing technologies such as Fog Computing (FC), Cloud Computing (CC), the Internet of Things (IoT), and Face Recognition (FR).

This research introduces the new concept of FC to existing tracking systems and presents the design and the development of an IoT Cloud-based vehicle anti-theft system to pinpoint an accurate location of the stolen vehicle in real-time. This study extends the existing efforts in tracking systems to include advanced features influenced by advanced computing technologies such as Fog, Cloud, IoT and FR. Moreover, it highlights the benefits of using FC combined along with CC to provide a more accurate and reliable tracking system. This paper is structured as follows: Section 2 provides the background for this research; Section 3 presents the methodology used in this study; Section 4 describes the results obtained and presents a discussion while Section 5 concludes the study and makes recommendations for future research.

2. BACKGROUND

This section provides the background of this study and a literature review focused on the following areas: (2.1) smart vehicle antitheft systems; (2.2) Internet of Things (IoT); (2.3) Cloud Computing (CC); (2.4) Fog Computing (FC); and (2.5) Face Recognition (FR).

2.1. Smart Antitheft Systems for Vehicles

Smart Antitheft Systems started to be developed in the early 1990s. Almost all such systems use GSM and GPS modules to deliver information about vehicle location to the owner. For example, (Verma & Bhatia, 2013) implemented a vehicle tracking system using GSM and GPS that alerts the user of a vehicle when it is stolen and allows them to access the location of the vehicle. (Katta, Dutta, Gogoi, Gayan, & Rabha, 2014) attempted to develop an anti-theft system using a GSM and GPS module which sends the location of a vehicle to the owner when the vehicle is in motion. (Bhatt, Kalani, Parmar, & Shingala, 2015) proposed the use of wireless technology in the vehicle that provides information on request via GSM modem. If the vehicle is tampered with, the command on the microcontroller is triggered and a message is sent to the owner. When the owner receives the message they can message the microcontroller to stop the vehicle.

(Jose, Prasad, & Sridhar, 2015) proposed an intelligent vehicle monitoring system using GPS together with Google Maps and Cloud Computing as a solution for vehicle theft. It collects information about a vehicle through various sensors to provide valuable information including vehicle location, speed, fuel level, driver conditions and other vital vehicle components. This information is transmitted in near-real-time via satellite to a maintained cloud server. That information is then accessible to authorised users in real-time anytime and anywhere through a web portal. (Nalina, Sandesh, Sequiera, & Jayarekha, 2015) present a cloud-based multi-vehicle tracking and locking system to provide vehicle owners the possibility to track any vehicle in real-time. Owners can lock the system in the event of malicious activity such as burglary.

(Geetha, Priyadarshini, Sangeetha, & Sanjana, 2017) describe a project that uses only GSM modules and thus keeps costs down. The system uses other components to allow the owner to trigger the microcontroller to start/stop the vehicle when stolen. The system sends SMS messages to the owner and the police station. It allows the owner to send commands via SMS to the system which are then processed by the microcontroller. (Pal & Pal, 2017) focus on vehicle simulations and present an easy technique to simulate car data to showcase the current platforms available in the domain. (Plangi, Hadachi, Lind, & Bensrhair, 2018) present a real-time system that makes use of all the embedded

Table 1. The main technologies used in anti-theft vehicle tracking systems

	Used Technologies				
Researchers	IoT	GSM	GPS	CC	FC
(Verma & Bhatia, 2013)	X	√	√	X	X
(Katta et al., 2014)	X	√	√	X	X
(Bhatt et al., 2015)	X	√	√	X	X
(Jose et al., 2015)	X	√	√	√	X
(Nalina et al., 2015)	X	√	√	√	X
(Pal & Pal, 2017)	√	√	√	X	X
(Plangi et al., 2018)	√	√	√	X	X
(Koubâa & Qureshi, 2018)	√	√	√	√	X
(Hamid et al., 2019)	√	√	√	√	X
(Usman, Yusuf, & Sajiyus, 2019)	X	√	√	X	X
(Kadiri & Adegoke, 2019)	X	√	√	X	X

sensors in a smartphone using multi-sensor fusion. Their work aims to provide a real-time system capable of tracking, positioning, and anticipating the movement of vehicles in real-time. (Koubâa & Qureshi, 2018) present a "DroneTrack" which is a real-time object tracking system. It uses a drone that tracks a moving object over the Internet. Alongside the "DroneTrack" they introduce a "Dronemap planner" which is a cloud-based system that controls, communicates, and manages drones over the Internet. Table 1 presents the most commonly used technologies in anti-theft vehicle tracking systems. It is evident from the list that GPS and GSM are considered compulsory technologies in any tracking system, while technologies such as Cloud and IoT are used to improve the performance and usability of these tracking systems. Nevertheless, Fog Computing has not been implemented or introduced by any mentioned studies in table 1.

2.2. Internet of Things (IoT)

IoT is a technology that connects whole intelligent entities within a specific network, i.e. the Internet. It comprises all type of computer technologies, both hardware and software. Its main target is the development of applications for devices to enable the control and monitoring of a particular domain. It has been extensively adopted in many domains including home machines; smart homes and cities (Alyami & Alreshidi, 2019); industrial business processes and health applications (Rabie & Ahmed, 2017); agriculture domain (Alreshidi, 2019b). The IoT connectivity incorporates people, machines, tools and locations to achieve different intelligent functions that range from data and information exchange to data sharing (Bibri, 2018; Fatma, Rabie, Mohamed, & Moawad, 2017). IoT is used in smart anti-theft systems to control and monitor products. Using IoT technologies in smart anti-theft would allow the following tasks: (1) searching; (2) tracking; (3) monitoring; (4) controlling; (5) managing; and (6) evaluating.

2.3. Cloud Computing (CC)

Cloud Computing (CC) is a rapidly growing area within the IT domain (Armbrust et al., 2010; Kumar, Byung Gook, HoonJae, & Kumari, 2012). It provides easy access to the Cloud provider's storage infrastructure and high-performance processors over the Internet (Jiyi, Lingdi, Xiaoping, Ya, & Jianqing, 2010) (Repschlaeger, Wind, Zarnekow, & Turowski, 2012). NIST (Mell & Grance, 2009) defines CC as "*a model for enabling convenient, on-demand network access to a shared pool* *of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*". CC can be seen as a high virtualisation system for datacentre infrastructure distributed over a wide geographical area, linked together with high bandwidth network cables to provide a different virtualised service. CC delivery services can generally be divided into three different models: (1) Infrastructure-as-a-Service (IaaS); (2) Platform-as-a-Service (PaaS); and (3) Software-as-a-Service (SaaS) (Chornyi, Riediger, & Wolfenstetter, 2010; Marinos & Briscoe, 2009). CC is divided into four main layers: (1) hardware; (2) infrastructure; (3) platform; and (4) application (Alreshidi, 2019a; Zhang, Cheng, & Boutaba, 2010). CC is often considered to be the most effective method of storing data generated by IoT devices (Auxilia, Raja, & Kannan, 2020; Channe, Kothari, & Kadam, 2015).

2.4. Fog Computing (FC)

Fog Computing (FC) can be seen as an extension of Cloud Computing and links objects from the infrastructure to the network's edge devices, enabling a new variety of applications and services. Fog equipment could be any device with an internet connection and local processing capabilities. According to (Bonomi, Milito, Zhu, & Addepalli, 2012), Fog Computing is *"a highly virtualized platform that provides compute, storage, and networking services between end devices and traditional Cloud Computing Data Centres, typically, but not exclusively located at the edge of network"*. FC has the following defining characteristics: low latency, location awareness, mobility, heterogeneity, supports a large number of nodes, predominant role of wireless access, has a wide geographic distribution and a strong presence of streaming and real-time applications. These characteristics render FC the appropriate platform for several critical Internet of Things (IoT) services and applications such as Smart Buildings, Smart Grid, Smart Cities, and Connected Vehicle (Bonomi et al., 2012).

2.5. Cloud Computing (CC) vs Fog Computing (FC)

Cloud and Fog concepts share quite a few similarities but have some different parameters. The architecture of the Cloud is centralised and contains big data centres that can be located worldwide far from client devices. The architecture of Fog Computing is distributed and contains millions of small nodes located closer to clients' devices. The Cloud establishes direct communication with devices in real time and it is performance consuming while Fog acts as a middle layer between data centres and hardware and, hence, is closer to end-users. In terms of processing, the Cloud processes data in remote data centres but Fog allows data to be processed and stored on the edge of the network that is close to the source of information and this is vital for real-time operations.

Nonetheless, the performance and storage capabilities of the Cloud are more potent than Fog computing. Fog has a massive number of connecting nodes, while the Cloud has a few large server nodes. Another significant difference is that the Cloud provides high latency, but in Fog Computing, the latency is meagre. Internet connectivity is vital for both. The Cloud system is likely to collapse if there is no internet connection, while in Fog the risk of failure is much lower due to the use of various protocols and standards. Finally, due to its distributed architecture, Fog is a more secure system than the Cloud.

2.6. Face Recognition (FR)

Face Recognition (FR) has long been employed in smart systems (Abellan-Nebot & Subirón, 2010) given that it is used in intelligent machines that facilitate everyday life (Russell & Norvig, 2016). It covers many areas, including deep learning, computer vision, data mining, image processing and neural networks (Kale & Patil, 2019; Patrício & Rieder, 2018). Face Recognition technologies are now emerging to assist and improve efficiency and tackle many of the challenges facing the tracking process.

Most anti-theft systems that use GSM and GPS have recently moved to adopt Cloud-based solutions. Given the limitations of the Cloud, Fog would be a better choice, especially when adopting

IoT technologies. This research aims to lay the foundation for the adoption of new concepts, i.e. Fog Computing, in the domain of smart vehicle anti-theft systems.

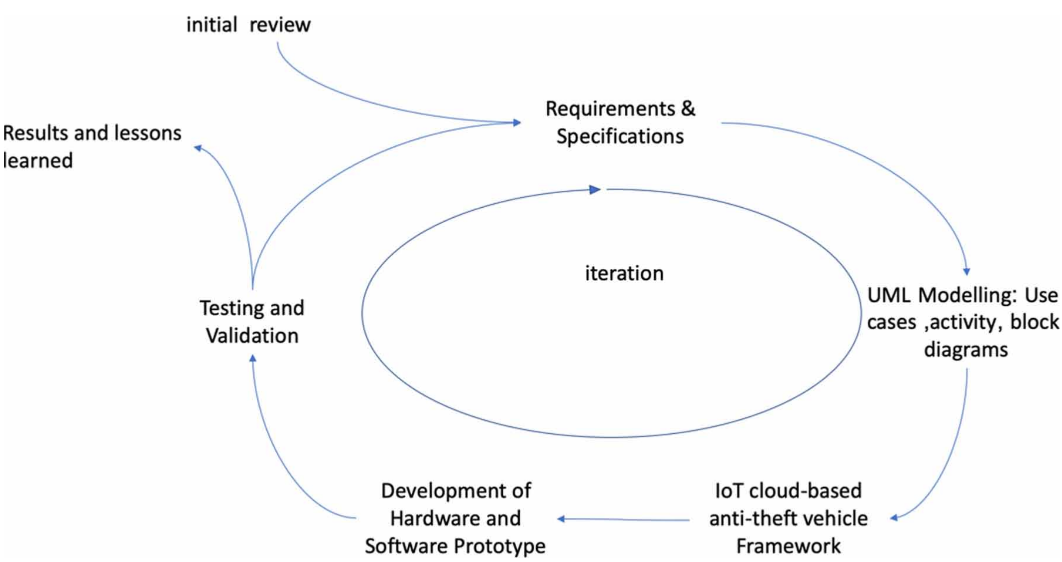
3. METHODOLOGY AND ADOPTED SMART ANTI-THEFT SYSTEM FRAMEWORK

This section demonstrates the adopted research methodology and presents a holistic of the overall framework of the smart anti-theft system underpinned by advance computing technologies.

3.1. Research Methodology

This section describes the methodologies employed to develop an anti-theft tracking system underpinned by advanced computing technologies. The research commenced with a critical review focused on the following elements: i.e. IoT, CC, FC, and FR. An iterative software engineering approach in the form of UML diagrams was adopted to underpin the development of the proposed system (Brian, 2020; Narendranath & Eric, 2019). The first stage involved collecting the set of requirements and specifications to develop the smart antitheft vehicle tracking system. The second stage involved modelling these requirements via UML language to present them through a use cases diagram, an activity diagram, and a block diagram. A hardware and software prototype was then built for the proposed system and a framework proposed for integrating advanced computing technologies with the smart anti-theft vehicle system. Initial testing and validation were carried out to examine the functionalities of the system, as well as the capabilities of the Cloud and Fog environments. Figure 1 shows the iterative lifecycle of the development of a smart anti-theft vehicle system.

Figure 1. IoT Cloud-based smart anti-theft vehicle system development methodology



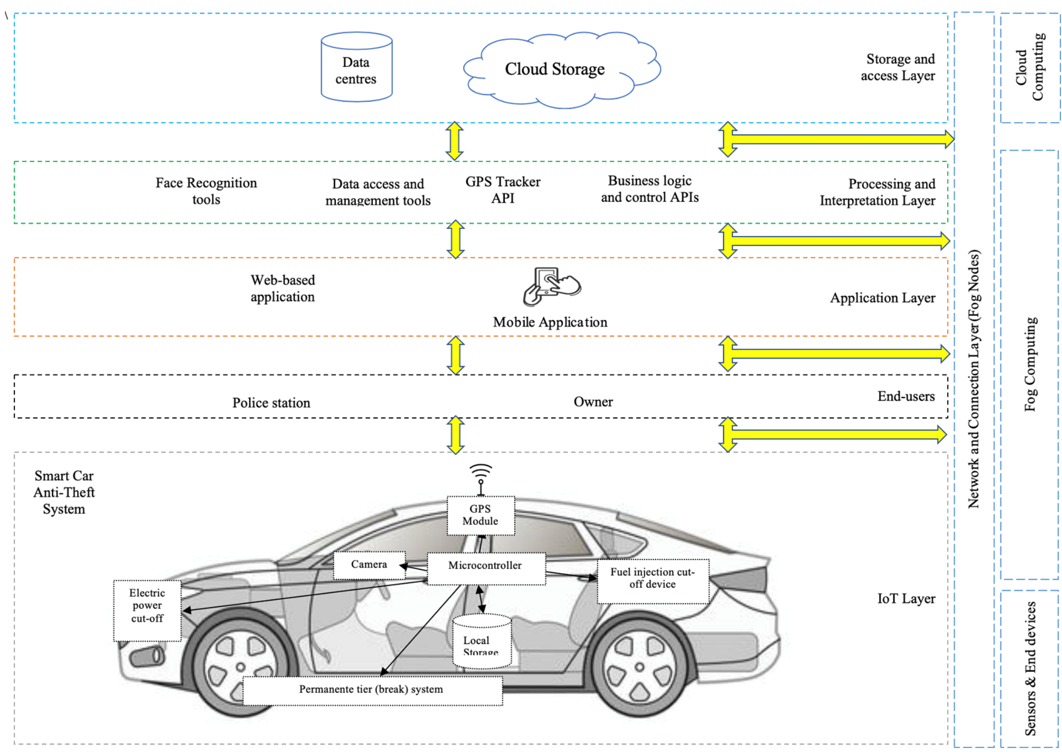
3.2. Overall View of the Smart Anti-Theft System Framework

This study introduces new concepts for smart anti-theft vehicle systems. Some of the concepts, including IoT, FR and CC, have been introduced in previous research; other concepts, such as FC, have only recently been introduced. The following framework illustrates the overall smart anti-theft system in relation to these advanced computing technologies. It consists of the following main components and layers:

- **Cloud Computing:** This component provides storage and access for data received and retrieved from edge (IoT) devices. It contains the storage and access layer.
- **Fog Computing:** This component would act as the intermediate component between CC and the Edge component. It consists of the following layers:
  - ***Processing and Interpretation layer:*** This layer deals with the processing and interpretation of collected data from edge devices (IoT). It hosts all APIs and software of the smart system such as face recognition tools, GPS tracking API and Maps API.
  - ***Application layer:*** This layer is responsible for hosting different types of system applications as web-applications or mobile applications.
  - ***End-users***: This includes end-users such as owners and police stations.
- **Edge Computing (Sensors & End Devices):** This component includes IoT and hardware devices with sensors and actuators.

The Network and Connection layer provides connectivity among all the layers mentioned above. Hence, it can be considered as a standard layer. This layer can include any transmission or network device ranging from local networks to GSM towers and GPS satellites. Figure 2 illustrates the integration of advanced computing technologies with a smart anti-theft vehicle system.

Figure 2. Framework for integrating advanced computing technologies with an IoT Cloud-based anti-theft vehicle system



4. SYSTEM DESIGN AND TECHNICAL REQUIREMENTS

This section presents the analysis and initial outcomes based on the review process of the existing smart anti-thefts systems. It first shows key UML diagrams of the developed smart anti-theft system, i.e. use cases diagram, activity diagram, and block diagram. Secondly, it illustrates the recommended technical requirements for the proposed system. Then, it demonstrates the assembled and implemented technical smart anti-theft system alongside with screenshots of the developed web-based application for an IoT Cloud-based vehicle anti-theft system. Finally, it shows how to extend the IoT cloud vehicle anti-theft system with an embedded face recognition system.

4.1. UML Use Cases Diagram

The UML use cases diagram given in Figure 3 highlights the most significant use cases for the proposed system as identified in the literature. It presents the main use cases that should be included in the anti-theft smart system namely: "*authorisation*", "*contact owner*", "*tracking*", "*get vehicle information*", "*stop vehicle*", "*store and update information*" and "*use camera*". It is important to note that this list is not comprehensive and more use cases that can be added to the system based on the end-user's requirements.

4.2. UML Activity Diagram

The activity diagram presented in Figure 4 illustrates the flow of the proposed IoT Cloud-based anti-theft vehicle system. The first step towards using the system is to log in using a valid username and password. Once authorised, the owner can confirm that the vehicle is stolen and the tracking mode is activated. The tracking mode allows the owner to perform the following tasks: (a) get vehicle information: GPS location, trips history, vehicle information; (b) contact owner: make a call, send SMS to owner, owner information; (c) vehicle control: permanent lock, (d) use camera. The system will use fog nodes to transmit the data between the end-user and the Cloud infrastructure based on the task selected.

4.3. UML Black Diagram for the Proposed Smart Anti-Theft System

The proposed IoT Cloud-based anti-theft vehicle system illustrated in Figure 5 comprises a microcontroller GSM module, a GPS module, a camera, local memory and a trigger in the driver's circuit for ignition, fuel, and breaks. The microcontroller is coded to be active when the owner accesses the system portal. The owner can activate the tracking mode of the vehicle allowing them to start the tracking mode of the vehicle location via GPS/GSM modules. These modules are connected to the connection nodes through a valid SIM. This SIM sends updated information regarding the stolen vehicle's location to the owner. Apart from providing this real-time information to the owner the system stores it on the Cloud and a local storage medium, i.e. a local memory card. The storage card will store information as a back up in case the connection between the system and the connection nodes is lost. It will update itself with the latest information when the connection is regained. The system also allows the owner to access the hidden camera facing the driver and take a picture or record a video. The picture/video can be uploaded in real-time onto a face recognition system authorised by the police authority that would contain thousands of images against which the image can be compared. This facilitates the search process for the thief and if there is a match this can be used as evidence in court. The owner is also able to override the car board remotely to perform actions to force the vehicle to stop. These actions include fuel cut off, power cut, and permanent lock.

4.4. Technical Requirements for Prototype Implementation

This section illustrates the technical implementation of the proposed IoT Cloud-based anti-theft vehicle system. Many sensors and other devices were used in this experiment. These are described below:

Figure 3. IoT Cloud-based anti-theft vehicle system's UML Use cases

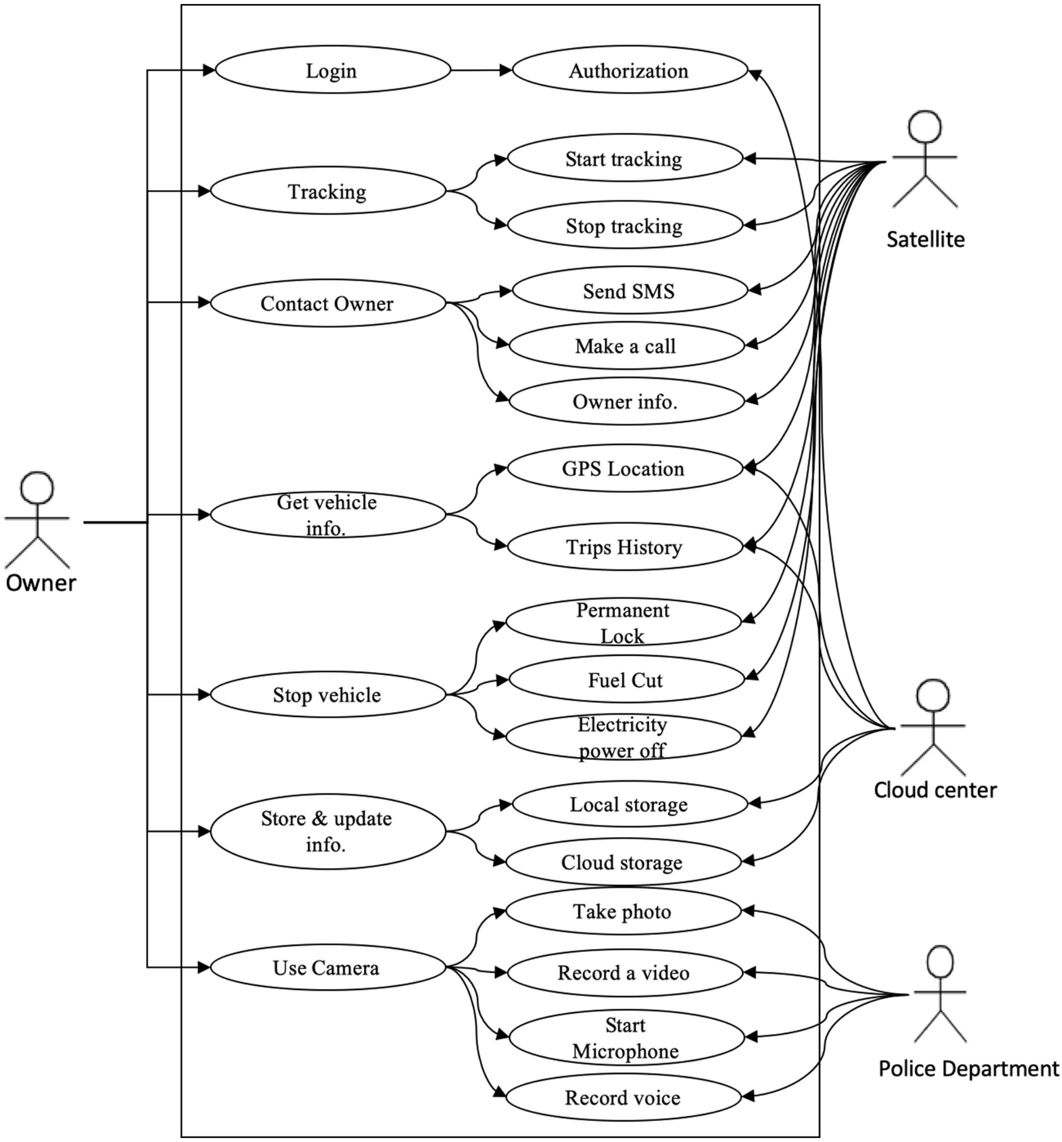


Figure 4. UML Activity Diagram

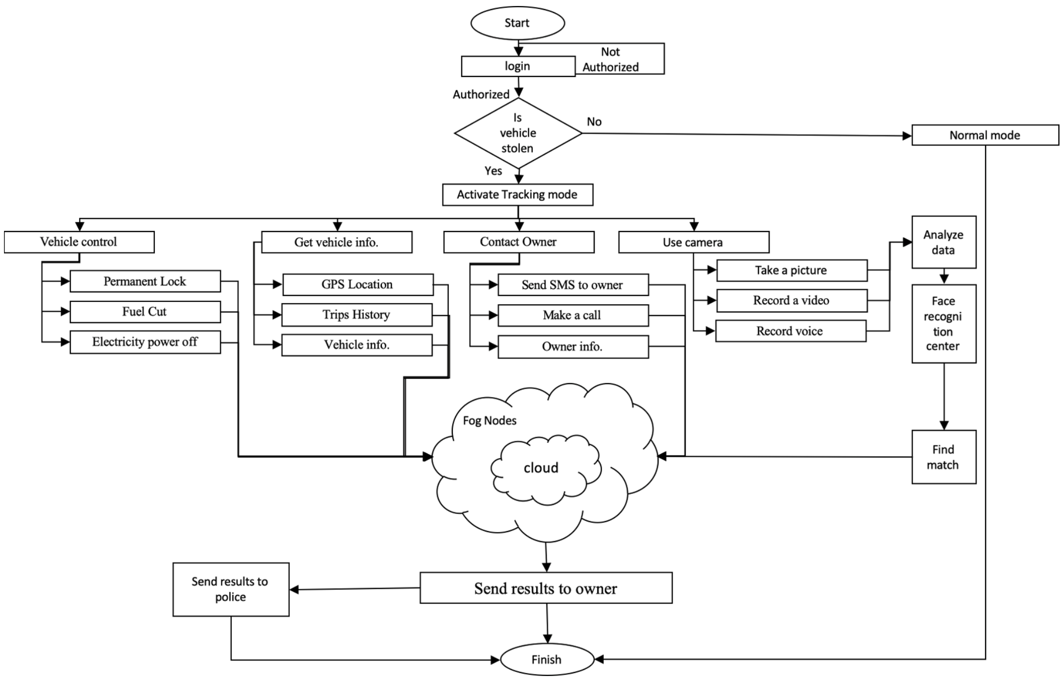
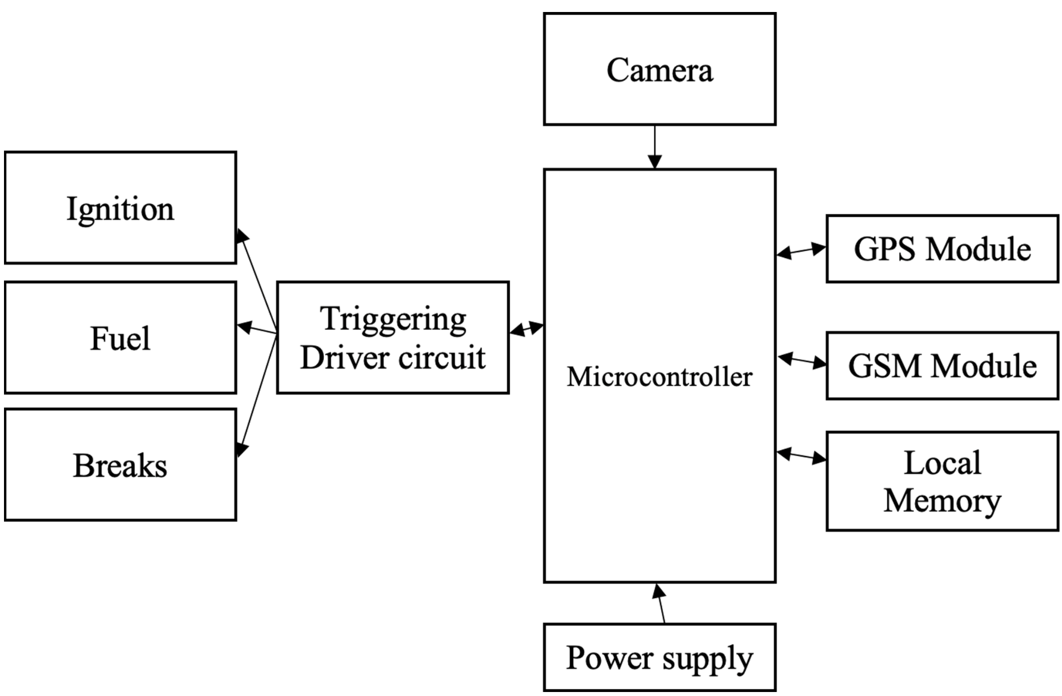


Figure 5. Initial UML block diagram for the proposed IoT Cloud-based anti-theft vehicle system architecture



- **Arduino UNO:** an open-source electronics platform with a single-board microcontroller that comes with an embedded system programming software suite. It is possible to view Arduino as a tiny programmable computer to collect inputs and process outputs between the connected devices and external components such as sensors, buttons, motors, LCD. The hardware consists of an Atmel AVR processor and on-board I/O support. Its complete microcontroller board is based on the ATmega328 microcontroller. The software uses a standard programming language for writing the code and a boot loader that runs on the board. It works by writing and sending a set of instructions to the microcontroller on the board to perform the required jobs. In the last few years, Arduino platforms have been heavily used by thousands of IoT projects, ranging from simple projects to complicated scientific projects. It has a wide community of users who together are creating massive knowledge and projects that can be reused and re-developed to accommodate the end-user's requirements (Arduino, 2020). Table 2 lists the key specifications of the Arduino UNO microcontroller.

Table 2. Arduino UNO Microcontroller Specifications

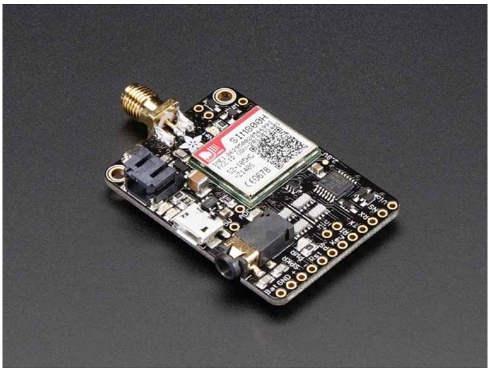
Arduino UNO Microcontroller	Description
Rated operating voltage	5v
Recommended input voltage level	7V to 12V
Input/output digital pins	14
Analogue Input pins	8
DC current per the I/O pin	40 mA
DC current of 3.3v pin	50 mA
Flash memory	32 KB
SRAM	2 KB
EEPROM	1 KB
Clock speed	16000 KHZ

- **SIM800H GSM module:** a quad-band GSM/GPRS module that works on the following frequencies: GSM850MHz, EGSM900MHz, DCS1800MHz and PCS1900MHz. It is a GPRS multi-slot class 12/ class 10 and supports the GPRS coding schemes CS-1, CS-2, CS-3 and CS-4. It can meet almost all the space requirements in user applications, such as the smartphone, the PDA and other mobile devices using a small effort of the configuration process. It has 88 pin pads of LGA packaging and offers all hardware interfaces between the module and users' boards (Adafruit, 2020a). Table 3 lists the key specifications of the SIM800H GSM module.

- **The Global Positioning System (GPS) Module:** a built MTK3339 chipset that can track up to 22 satellites on 66 channels. It has an excellent high-sensitivity receiver with -165 dBm tracking and a built-in antenna. It can update up to 10 locations per second for high speed, high sensitivity logging or tracking. It uses a low 20 mA during navigation and an ultra-low dropout 3.3V regulator so it can be powered by 3.3-5VDC in, 5V level safe inputs. It has an enable pin to turn off the module using any microcontroller pin or switch. There is also an optional slot for a CR1220 coin cell to keep it running. When in operation it has a bright red LED that blinks at

1Hz while it searches for satellites and blinks once every 15 seconds when the satellite is found (Adafruit, 2020b). Table 4 shows the Ultimate GPS Breakout V3 Specifications

Table 3. SIM800H GSM Module Specifications



GSM SIM800H	Description
Processing Performance	• Quad-band 850/900/1800/1900MHz •GPRS multi-slot class 12/10 • GPRS mobile station class B • Compliant to GSM phase 2/2+
Supply voltage	3.8V- 5V
Recommended supply voltage	4V
Power consumption	• sleep mode < 2.0mA • idle mode < 7.0mA • GSM transmission (avg.): 350 mA. • GSM transmission (peek): 2000 mA. • Module size: 25 x 23 mm.
Weight	1.35 g
SIM card socket	Micro SIM
Supported frequencies	Quad Band (850 / 950 / 1800 /1900 MHz)
Antenna connector	IPX
Working temperature range	-40 do + 85 ° C

Table 4. Ultimate GPS Breakout V3 Specifications

Ultimate GPS Breakout V3	Description
Performance	-165 dBm sensitivity, 10 Hz updates, 66 channels
Supply voltage	• 5V friendly design and only 20mA current draw • RTC battery-compatible
Recommended supply voltage	• Built-in data logging • PPS output on fix • Internal patch antenna + u.FL connector for external active antenna • Fix status LED
Power consumption	sleep mode < 2.0mA idle mode < 7.0mA GSM transmission (avg.): 350 mA. GSM transmission (peek): 2000 mA. Module size: 25 x 23 mm.
Weight	1.35 g
SIM card socket	Micro SIM
Supported frequencies	Quad Band (850 / 950 / 1800 /1900 MHz)
Antenna connector	IPX
Working temperature range	-40 do + 85 ° C

- **5V 4-Channel Relay board:** a board to drive a high-power load that cannot be controlled by the microcontroller, due to the limitations of the current and voltage microcontroller. This board includes four relays. Each relay provides 2 pole changeover contacts NO and NC. However, it can increase the current limit of each output because the 2 changeover contacts have been put in parallel. Four LEDs indicate the on/off state of each relay. It is able to control various appliances and other equipment with the larger current. It can be controlled directly by Microcontroller (Raspberry Pi, Arduino, 8051, AVR, PIC, DSP, ARM, ARM, MSP430, TTL logic) (Sunfounder, 2020). Table 5 shows a 5V 4-Channel Relay board with its technical specifications.

Table 5. 5V 4-Channel Relay board specifications

5V 4-Channel Relay interface board	Description
Current	15-20mA
High-current relay	AC250V 10A ; DC30V 10A
Microcontroller interface	Raspberry Pi, Arduino , 8051, AVR, PIC, DSP, ARM, ARM, MSP430, TTL logic
Inputs	Opto-isolated
Size	75*55*20mm
Relay output status	Indication LEDs

Table 6. OV7670 camera specifications

OV7670 camera		Description
Array Element (VGA)		640 x 480
Power Supply	Digital Core	1.8VDC +10%
	Analog	2.45V to 3.0V
	I/O	1.7V to 3.0V
Temperature Range	Operation	-30°C to 70°C
	Stable Image	0°C to 50°C
Output Formats (8-bit)		YUV/YCbCr 4:2:2, RGB565/555, GRB 4:2:2 , Raw RGB Data
Lens Size		1/6”
Chief Ray Angle		24°
Maximum Image Transfer Rate		30 fps for VGA
Sensitivity		1.1 V/Lux-sec
S/N Ratio		40 dB
Scan Mode		Progressive
Electronics Exposure		Up to 510:1 (for selected fps)
Pixel Size		3.6 µm x 3.6 µm
Dark Current		12 mV/s at 60°C
Image Area		2.36 mm x 1.76 mm
Package Dimensions		3785 µm x 4235 µm

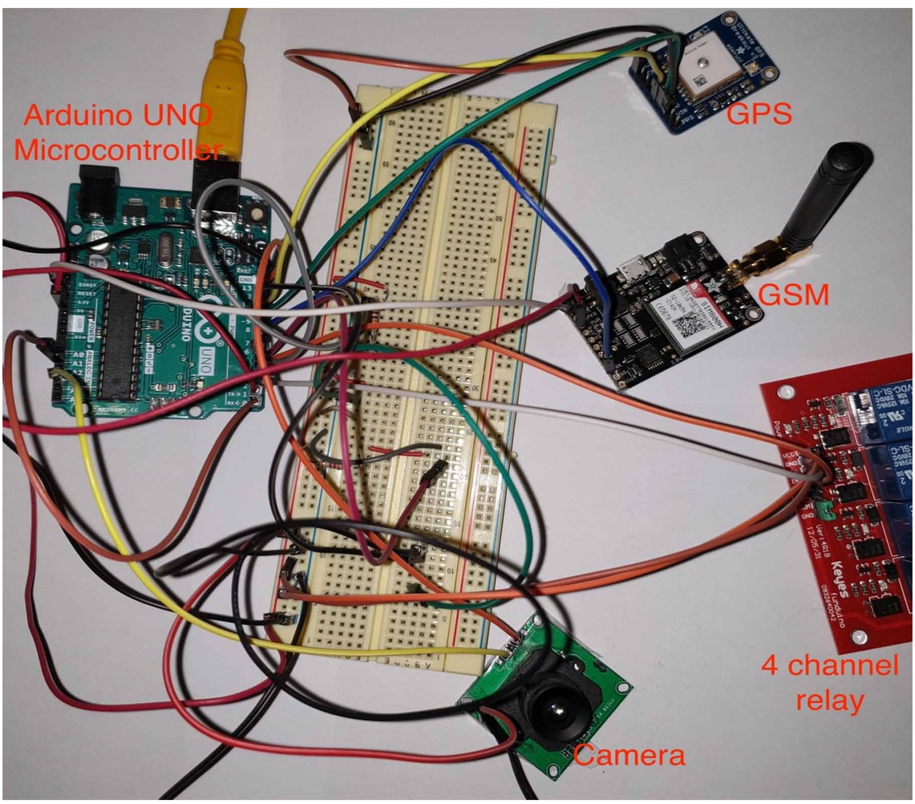
- **OV0706 Camera:** This camera uses a surveillance camera digital image processing chip-OV0706 which is designed for image acquisition and processing application. Because it is based on the TTL communication interface, it can easily be connected with an Arduino microcontroller, to read image and data via a UART serial port. This would allow the developer to process the acquired images. It can process video images using the following technologies: auto white balance (AWB), automatic exposure (AE) and automatic gain control (AGC). With some configuration, it can support advanced technologies, e.g. image enhancement processing under low illumination, image noise intelligent forecast and suppress, self-definition of the detection area and sensitivity, JPEG decoder supported real-time encoding of the image, supported motion detection and OSD display function of screen characters and pattern overlay (Omnivision, 2005). Table 6 lists the specifications of the OV7670 camera.

- **Fog Nodes:** represent the method of connectivity between the edge devices and Cloud computing. These devices include satellite, routers, cellular or mobile Wi-Fi.

4.5. The Complete View of the Implemented Technical System

This section presents the hardware that was needed to build the proposed system and the assembling process. Figure 6 shows the main components used in the developed IoT Cloud-based anti-theft system which are: the microcontroller, the GSM, the GPS, the camera and the relays that will be connected to the engine ignition cut-off and fuel supply cut-off.

Figure 6. Technical implementation of an IoT Cloud-based vehicle anti-theft system



4.6. Web-Based Application for an IoT Cloud-Based Vehicle Anti-Theft System

Following the assembly of the hardware components, an online application was developed for the system. The system allows end-users to monitor important data relating to the vehicle. The online facility offers the client the ability to perform a number of tasks via a web application (as described in the aforementioned use cases in Section 4.2). Figure 7 shows the initial web-based application. It highlights the main functions of the IoT Cloud-based anti-theft system.

Figure 7. Web interface for smart anti-theft system

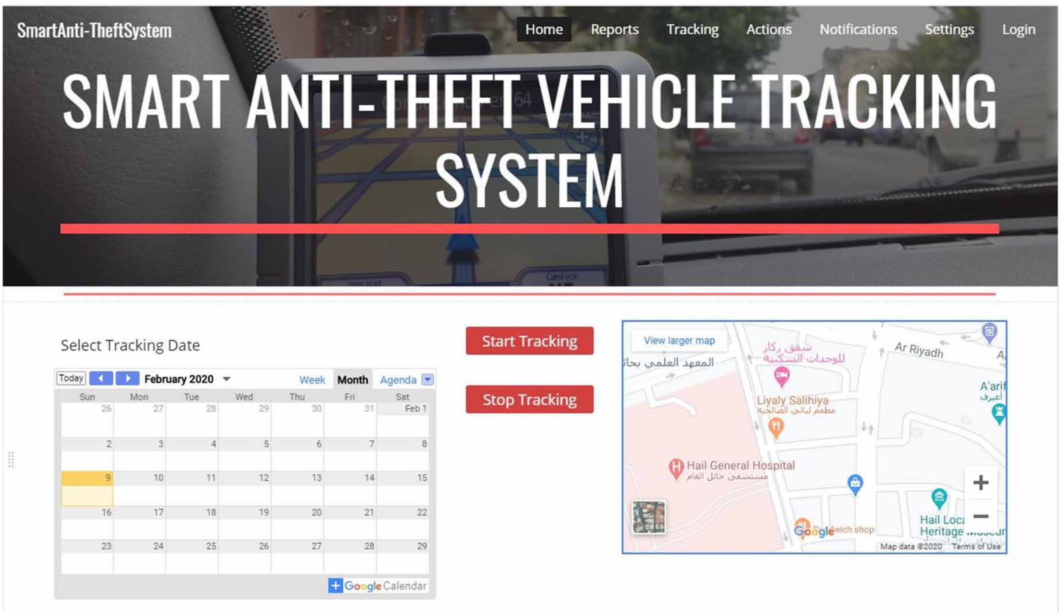


Figure 8 illustrates the trip history of the vehicle on a certain date over a specified period of time. This history can be viewed over the web-based application and the end-user can store the information and create a history report that would contain essential information about the stolen vehicle such as vehicle status, fuel status and engine status.

Figure 9 shows the GPS and GSM functionality when the GPS connects to satellites and then calculates the position in terms of latitude and longitude and time and date before using GSM to send the information in an SMS to the owner of the vehicle.

4.7. Embedded Face Recognition System

By using the installed tiny hidden camera on the smart system, the owner can acquire an image of the person behind the driving wheel. This image can be sent to the face recognition system used by a local authority such as the Police to look for a possible match. The camera provides tangible evidence of the theft. Figure 10 illustrates the workflow of the embedded face recognition system within the smart vehicle anti-theft system.

Figure 8. Online tracking system using a web application

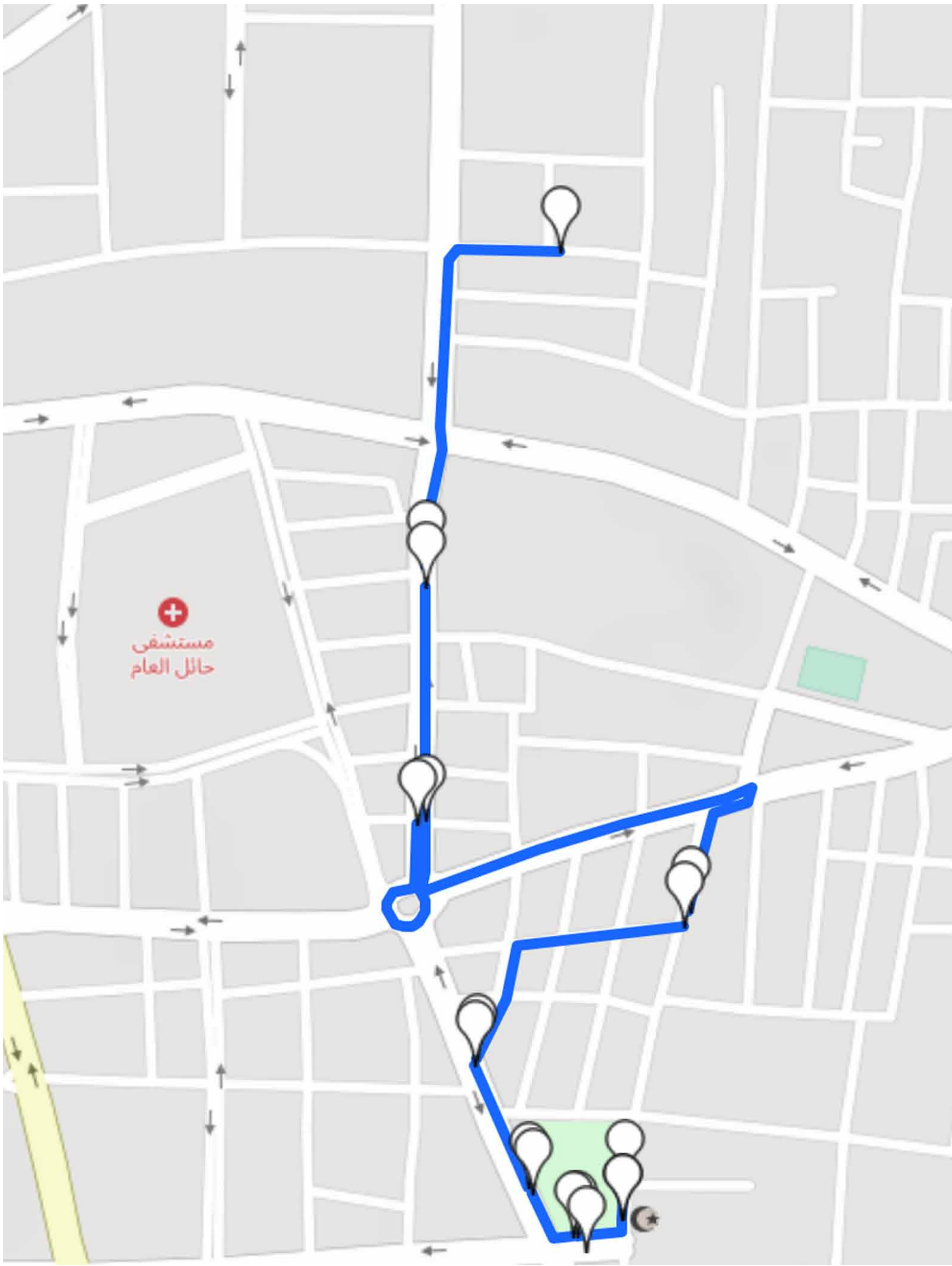


Figure 9. GPS coordinates sent via SMS from the system to vehicle owner via GSM

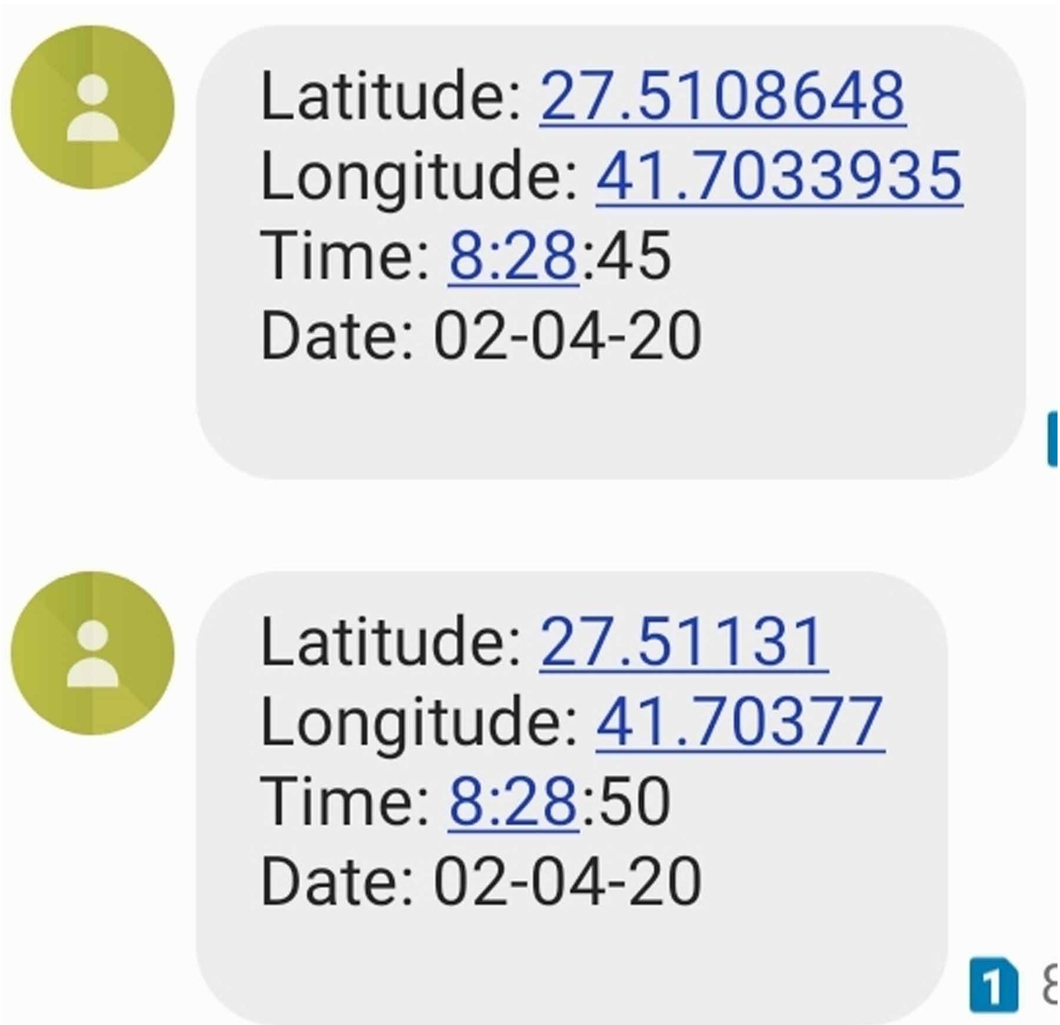
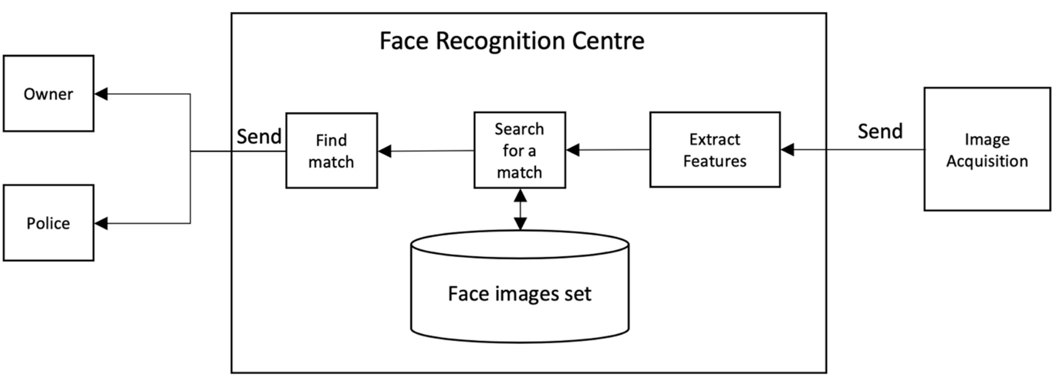


Figure 10. Embedded face recognition system within the IoT Cloud vehicle anti-theft system



5. DISCUSSION

5.1. The Existing Tracking Systems and Future Trends

Smart anti-theft tracking systems for vehicles have become very important in various applications, ranging from simple applications such as routing to more complex applications such as those used in emergency situations. Most existing systems must include GPS and GSM as main components for the tracking process. IoT technologies are used in these systems to add features such as motion detection sensors and infrared sensors. The integration of Cloud computing extends the performance and storage capabilities of the system beyond local storage. However, Cloud computing suffers from some limitations they can be overcome with the introduction of Fog Computing. Furthermore, the use of emergent Artificial Intelligence technologies, especially image processing and computer vision, will facilitate the process of identifying the thief using the image of their face captured through a hidden camera. To date, there has been a great deal of research invested in the development of this function. However, further work needs to be carried out to improve real-time tracking systems in terms of performance, accuracy, and effectiveness.

5.2. Advantages and Disadvantages of Cloud, Fog, and IoT

Connecting the smart vehicle system to the Cloud provides access, scalable storage, and high computing services for different devices from any location. Integrating Cloud Computing with IoT is cost-effective because Cloud services provide the essential requirements to create user-friendly applications and to analyse and manage the data gathered from connected devices. This allows developers to create and maintain IoT-Cloud applications without extra costs relating to hardware and software.

One of the limitations of IoT devices is their limited storage capacity and processing power. Cloud Computing can help in the following aspects: (a) performance improvement; (b) storage capacity increase, (c) extended processing capabilities; and (d) cost reduction. However, Cloud technologies have downsides, mainly when used with IoT devices. These shortcomings include: (a) high latency: this occurs due to the distance between IoT devices and Cloud services; (b) downtime: which happens in the case of technical issues and network interruptions; and (c) security and privacy: happens when data are transferred via global channels increasing the vulnerability of cyber-attacks and increasing the chance of data loss.

The Fog computing approach provides more benefits for IoT that can overcome the limitations of the Cloud approach. These benefits include: (a) low latency due to its close geographical distance to users; (b) fewer bandwidth issues; (c) connection lost chances are deficient; (d) higher security; and (e) power efficiency due to the small amount of electricity used to power edge devices. The shortcomings of the FC approach are few and include: (a) the formation of complicated systems; (b) extra costs (especially in edge devices: gateways, hubs, and routers); and (c) scalability limitations when compared with Cloud scalability.

6. CONCLUSION AND FUTURE WORK

Anti-theft tracking systems for vehicles were first developed a long time ago. Developments in computer science and engineering require that these systems be updated to become smarter. This paper provided a review of current anti-theft vehicles tracking systems and introduced new concepts, namely IoT, Fog Computing, and Cloud Computing, that are being integrated with existing systems through an IoT Cloud-based anti-theft system framework. The main objective of this study is achieved where an initial technical prototype was developed for testing and validation. This research study provided base information that can be used to tackle most of the issues that IoT devices suffer from when they are connected to the Cloud via Fog nodes. It is envisaged that this information can significantly help improve the performance of the tracking process. This research study provided base information that can be used to tackle most of the issues that IoT devices suffer from when they are connected to the Cloud via Fog nodes. It is envisaged that this information can significantly help improve the performance of the tracking process. Further enhancement and improvement is needed to present accurate and reliable data from connection providers such as Cloud providers and local telecommunication companies. Therefore, it is recommended that future research focus on: (a) extending the functionality of the system via integration of other IoT devices; (b); implementing the embedded face recognition function via the use of appropriate artificial intelligence algorithms and computer vision libraries; (c) investigate the response time of the proposed system as well as investigate further communication methods between the proposed system and the owner instead of SMS; (d) performing more testing and validation to prove the advantages of the Fog Computing approach when compared to Cloud Computing.

REFERENCES

Abellan-Nebot, J. V., & Subirón, F. R. (2010). A review of machining monitoring systems based on artificial intelligence process models. *International Journal of Advanced Manufacturing Technology*, *47*(1-4), 237–257. doi:10.1007/s00170-009-2191-8

Adafruit. (2020a). *Adafruit FONA MiniGSM*. Retrieved from https://learn.adafruit.com/adafruit-fona-mini-gsm-gprs-cellular-phone-module/overview

Adafruit. (2020b). *Ultimate GPS Breakout V3*. Retrieved from https://learn.adafruit.com/adafruit-ultimate-gps/overview

Ahmed, S. M., Marhoon, H. M., & Nuri, O. (2018). Implementation of smart anti-theft car security system based on GSM. *IACSIT International Journal of Engineering and Technology*, *7*(4), 5261–5265.

Alreshidi, E. (2019a). Comparative Review of Well-Known Cloud Service ProviderS (CSPS). *Scince International*, *31*(1), 165–170.

Alreshidi, E. (2019b). Smart Sustainable Agriculture (SSA) Solution Underpinned by Internet of Things (IoT) and Artificial Intelligence (AI). *International Journal of Advanced Computer Science and Applications*, *10*(5), 93–102. doi:10.14569/IJACSA.2019.0100513

Alyami, S., & Alreshidi, E. (2019). *Holistic IoT Architecture for Smart Sustainable Cities Current Perspective and Future Directions.* Paper presented at the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom).

Arduino. (2020). *What is Arduino.* Retrieved from https://www.arduino.cc/en/guide/introduction

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Stoica, I. et al. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. doi:10.1145/1721654.1721672

Auxilia, M., Raja, K., & Kannan, K. (2020). Cloud-Based Access Control Framework for Effective Role Provisioning in Business Application. *International Journal of System Dynamics Applications*, *9*(1), 63–80. doi:10.4018/IJSDA.2020010104

Bhatt, B., Kalani, P., Parmar, N., & Shingala, N. (2015). Smart Vehicle Security System Using GSM & GPS. *International Journal of Engineering and Computer Science*, *4*(6), 12508–12511.

Bibri, S. E. (2018). The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. *Sustainable Cities and Society*, *38*, 230–253. doi:10.1016/j.scs.2017.12.034

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). *Fog computing and its role in the internet of things*. Academic Press.

Brian, J. G. (2020). The Application of Systems Engineering to Project Management: A Review of Their Relationship. *International Journal of System Dynamics Applications*, *9*(1), 81–106. doi:10.4018/IJSDA.2020010105

Channe, H., Kothari, S., & Kadam, D. (2015). Multidisciplinary model for smart agriculture using internet-of-things (IoT), sensors, cloud-computing, mobile-computing & big-data analysis. *Int. J. Computer Technology and Application*, *6*(3), 374–382.

Chornyi, D., Riediger, J., & Wolfenstetter, T. (2010). *Into The Cloud*. Academic Press.

Constantinescu, Z., & Vladoiu, M. (2013). *Challenges in safety, security, and privacy in the development of vehicle tracking systems.* Paper presented at the 2013 17th International Conference on System Theory, Control and Computing (ICSTCC).

Fatma, H. E., Rabie, A. R., Mohamed, I. M., & Moawad, I. D. (2017). Efficient Data Reporting in a Multi-Object Tracking Using WSNs. *International Journal of System Dynamics Applications*, *6*(1), 38–57. doi:10.4018/IJSDA.2017010103

Feldiansyah Bakri, N., Nor Erne, B., Rika, R., & Hasanuddin, H. (2018). Public Policymaking Framework Based on System Dynamics and Big Data. *International Journal of System Dynamics Applications*, *7*(4), 38–53. doi:10.4018/IJSDA.2018100103

Geetha, M., Priyadarshini, T., Sangeetha, B., & Sanjana, S. (2017). *Anti-theft and tracking mechanism for vehicles using GSM and GPS.* Paper presented at the 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM). doi:10.1109/ICONSTEM.2017.8261289

Haider, A., Khan, A. H., & Denai, M. (2017). *A Smart Wireless Car Ignition System for Vehicle Security*. Advances in Automobile Engineering. doi:10.4172/2167-7670.1000169

Hamid, A. H. F. A., Chang, K. W., Rashid, R. A., Mohd, A., Abdullah, M. S., Sarijari, M. A., & Abbas, M. (2019). Smart Vehicle Monitoring and Analysis System with IOT Technology. *International Journal of Integrated Engineering*, *11*(4). Advance online publication. doi:10.30880/ijie.2019.11.04.016

Jiyi, W., Lingdi, P., Xiaoping, G., Ya, W., & Jianqing, F. (2010). *Cloud Storage as the Infrastructure of Cloud Computing*. Paper presented at the Intelligent Computing and Cognitive Informatics (ICICCI), Kuala Lumpur, Malaysia.

Jose, D., Prasad, S., & Sridhar, V. (2015). Intelligent vehicle monitoring using global positioning system and cloud computing. *Procedia Computer Science*, *50*, 440–446. doi:10.1016/j.procs.2015.04.012

Kadiri, K., & Adegoke, O. A. (2019). Design of a GPS/GSM Based Anti-theft Car Tracker System. *Current Journal of Applied Science and Technology*, 1-8.

Kale, S. S., & Patil, P. S. (2019). Data Mining Technology with Fuzzy Logic, Neural Networks and Machine Learning for Agriculture. In Data Management, Analytics and Innovation (pp. 79-87). Springer.

Katta, K., Dutta, I., Gogoi, D., Gayan, B., & Rabha, J. (2014). Review on Advanced Vehicle Security System with Theft Control and Accident Notification. *International Journal For Research In Emerging Science And Technology, 1*.

Koubâa, A., & Qureshi, B. (2018). Dronetrack: Cloud-based real-time object tracking using unmanned aerial vehicles over the internet. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 13810–13824. doi:10.1109/ACCESS.2018.2811762

Kumar, A., Byung Gook, L., HoonJae, L., & Kumari, A. (2012). *Secure storage and access of data in cloud computing.* Paper presented at the ICT Convergence (ICTC), 2012 International Conference on.

Marinos, A., & Briscoe, G. (2009). Community cloud computing. In *Cloud Computing* (pp. 472–484). Springer. doi:10.1007/978-3-642-10665-1_43

Mell, P., & Grance, T. (2009). The NIST definition of cloud computing. *National Institute of Standards and Technology*, *53*(6), 1–3.

Monawar, T., Mahmud, S. B., & Hira, A. (2017). *Anti-theft vehicle tracking and regaining system with automatic police notifying using Haversine formula.* Paper presented at the 2017 4th International Conference on Advances in Electrical Engineering (ICAEE). doi:10.1109/ICAEE.2017.8255459

Nalina, V., Sandesh, A., Sequiera, R. D., & Jayarekha, P. (2015). *Cloud based multiple vehicle tracking and locking system.* Paper presented at the 2015 IEEE International Advance Computing Conference (IACC). doi:10.1109/IADCC.2015.7154680

Narendranath, S., & Eric, P. (2019). The Dynamics of Product Development in Software Startups: The Case for System Dynamics. *International Journal of System Dynamics Applications*, *8*(2), 51–77. doi:10.4018/IJSDA.2019040104

Omnivision. (2005). *OV7670/OV7171 CMOS VGA (640x480) CAMERACHIP*. Author.

Pal, A., & Pal, M. (2017). IoT for vehicle simulation system. *International Journal of Engineering Science, 4393*.

Patrício, D. I., & Rieder, R. (2018). Computer vision and artificial intelligence in precision agriculture for grain crops: A systematic review. *Computers and Electronics in Agriculture*, *153*, 69–81. doi:10.1016/j.compag.2018.08.001

Plangi, S., Hadachi, A., Lind, A., & Bensrhair, A. (2018). Real-Time Vehicles Tracking Based on Mobile Multi-Sensor Fusion. *IEEE Sensors Journal*, *18*(24), 10077–10084. doi:10.1109/JSEN.2018.2873050

Rabie, A. R., & Ahmed, B. A. (2017). Hierarchal Fuzzy Logic Controller and Internet of Things (IoT) Information: Disease Spreading as a Test Case. *International Journal of System Dynamics Applications*, *6*(3), 59–86. doi:10.4018/IJSDA.2017070104

Ramani, R., Valarmathy, S., SuthanthiraVanitha, N., Selvaraju, S., Thiruppathi, M., & Thangam, R. (2013). Vehicle tracking and locking system based on GSM and GPS. *IJ Intelligent Systems and Applications, 9*, 86-93.

Repschlaeger, J., Wind, S., Zarnekow, R., & Turowski, K. (2012). *A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson Education Limited.

Sunfounder. (2020). *4 Channel 5V Relay Module*. Retrieved from http://wiki.sunfounder.cc/index.php?title=4_Channel_5V_Relay_Module

Usman, F. K., Yusuf, G., & Sajiyus, O. (2019). A Model for Smart Vehicle Tracking: A Review. *Journal of Scientific Research and Reports*, 1–5. doi:10.9734/jsrr/2019/v24i430162

Verma, P., & Bhatia, J. (2013). Design and development of GPS-GSM based tracking system with Google map based monitoring. *International Journal of Computer Science*, *Engineering and Applications*, *3*(3), 33.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18. doi:10.1007/s13174-010-0007-6

Eissa Alreshidi was born in Hail, Saudi Arabia on February 28, 1986. The author is involved in various scientific research activities at the University of Hail, Department of Computer Science and Engineering. Dr. Alreshidi received a PhD degree from Cardiff University, UK and Master's Degree from University of Birmingham, UK. The author is specialized in Computer Sciences and Engineering with an area interest in Smart Sustainable Systems, Cloud Computing, Artificial Intelligent, Knowledge-base Management, Information Modelling and Software Engineering. Currently, the author is also involved in various research and development activities within the University of Hail and abroad as a consultant and as project leader for several projects.