# The internet of things in community safety and crime prevention for South Africa

Nomusa Dlodlo[1], Paul Mbecke[2], Mofolo Mofolo[3], Martin Mhlanga[4]
CSIR – Meraka institute
Pretoria, South Africa
Email: {ndlodlo[1], pmbecke[2], mmofolo[3], mmhlanga[4]}@csir.co.za

***Abstract*— One of the major tasks of the South African government is to reduce crime levels on a year-to-year basis. The use of information and communications technologies (ICTs) is capital in facilitating the process to finding solutions to crime. This paper is about taking advantage of a particular subset of ICTs that is referred to as the internet of things (IoT) in the fight against crime, and that is community safety and crime prevention. The paper identifies not only the sectors of the economy that fall under community safety and crime prevention such as police efficiency and accountability, situational crime prevention and social crime prevention, but also a number of IoT applications that can be of value in these sectors. By drawing on the characteristics of identified IoT applications, the research came up with the architecture of an integrated IoT system for tracking of parolees who have violated their bail conditions, as a case study.**

**Keywords— internet of things, community safety, crime prevention, policing, information and communication technologies**

## I. INTRODUCTION

Crime is a prominent issue in South Africa (S.A.). During 2010/2011 year alone, a total of approximately 2.1 million serious crimes were registered in South Africa (Crime report 2010/2011, 2011). A study by the Centre for the Study of Violence and Reconciliation concluded that the country is exposed to high levels of violence as a result of the following factors [29]:

- The normalisation of violence as a justifiable means of resolving conflict
- The vulnerability of young people linked to inadequate child rearing and poor youth socialization
- The high levels of inequality, poverty, unemployment, social exclusion and marginalization
- A subculture of violence and criminality ranging from individual criminals to organised gangs
- A criminal system that is unreliable

One of the major tasks of the S. A. government is to reduce crime levels on a year-to-year basis. The use of information communication technology (ICT) is capital in facilitating the understanding of and assisting the process to find solutions to crime. This paper is about taking advantage of a particular subset of ICT that is referred to as the internet of things (IoT) in the fight against crime.

CASAGRAS defines the IoT as [2]: "A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving internet and network developments. It offers specific object-identification, sensor and connection capability as the basis for development of independent federated services and applications These are characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability". The International Telecommunications Union (ITU) states that the goal of ICT is to connect all objects to form a ubiquitous network which is called the IoT. This network covers all everyday objects such as watches, keys, household appliances, cars and buildings [29], When embedded with chips and sensors, these objects can think, feel and talk with each other. Together with the infrastructure of the internet and mobile networks these objects can communicate with humans and enable the humans to monitor and control them anytime, anywhere and enjoy their intelligent spaces. The IoT in 2020: roadmap for the future [14] defines the IoT as "things having identities and virtual personalities, operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental and user contexts".

The objective of this paper is to showcase the integration of IoT in community safety and crime prevention. It draws on the characteristics of identified IoT applications to come up with the architecture of an integrated IoT system to track parolees who have violated their bail conditions. This paper is organised as follows: The next section is the problem statement. We explore community safety and crime prevention concepts in section three. In the fourth section we explore internet of things

concepts while in the fifth section are applications of the IoT that can be adopted in community safety and crime prevention in S.A. The sixth section is on the architecture of the system while the last section is a summary of the paper.

## II. PROBLEM STATEMENT

Crime is a big threat to the safety of South African communities. This study is an extension to the efforts that South Africa is making towards crime prevention and community safety. The study proposes enhanced adoption of IoT in community safety and crime prevention. The question that this research answers therefore is:

*'What role can IoT technologies play in community safety and crime prevention in South Africa?"*

The objectives of the research are:

- To inform and support policy on the adoption of IoT in community safety and crime prevention
- To facilitate an understanding of the subject area through examples of IoT applications that can be adopted in community safety and crime prevention initiatives
- To develop an architecture for a system that tracks parolees as a case study of the application of on IoT in community safety and crime prevention

A literature survey was conducted through internet searches to identify applications that could be adopted in the South African environment for law enforcement, situational crime prevention and social crime prevention. From the identified IoT applications, certain characteristics were identified which contributed to the development of the architecture of the system that constitutes our case study on the tracking of parolees.

## III. CONCEPTS IN COMMUNITY SAFETY AND CRIME PREVENTION

South Africa's National Crime Prevention Strategy (NCPS) acknowledges the importance of social, developmental and environmental causes of crime and therefore the necessity of addressing social, developmental and environmental factors that promote crime. The strategy requires the development of wider responsibility for crime prevention and a shift in emphasis from reactive "crime control", which deploys most resources towards responding after crimes have already been committed, towards proactive "crime prevention" aimed at preventing crime from occurring. Crime prevention is defined as "all activities which reduce, deter, or prevent the occurrence of specific crime types (i) firstly by altering the environment in which they occur, (ii) secondly by changing the conditions which are thought to cause them and (iii) thirdly by providing a strong deterrent in the form of an effective criminal justice system. Crime prevention can be approached through many ways with several different entry points for understanding and intervention (prevention and reduction of crime). The three most important ways are: law enforcement, situational crime prevention and social crime prevention [28].

Social crime prevention focuses on the reduction of socio-economic and environmental factors that influence people to commit crimes and become persistent offenders. Historically shaped poverty and underdevelopment provide key contextual factors in understanding increasing crime levels in South Africa according to the national crime prevention strategy (NCPS) [18]. However, it recognises that there is no single cause of crime in South Africa. Broader socio-economic and environmental factors such as rapid urbanisation, high levels of unemployment and inequality, social dislocation, family disintegration, alcohol abuse, no access to public goods and services, to name but a few, all, negatively influence safety and security making people vulnerable to crime.

## IV. APPLICATIONS OF IOT IN COMMUNITY SAFETY AND CRIME PREVENTION

For each of the community safety and crime prevention areas of police efficiency and accountability, partnerships between the police and community and social crime prevention initiatives, a number of IoT applications are identified as follows:

### *A. Police efficiency and accountability*

This section looks at IoT technologies that assist improve police efficiency and accountability

- Biometric identification

Biometric identification consists of methods for uniquely recognising humans based upon one or more physical or behavioural traits. Physiological characteristics include fingerprint, face recognition, DNA, palm print, handwriting, iris recognition and odour. Behavioural characteristics include voice and gait, to name but a few.

Police agencies across the world are using mobile biometric fingerprinting for forensic identification. Fingerprint scanners identify suspects and victims more quickly. The devices use cellular technology. Fingerprints are scanned and instantly matched against a database containing over a million prints for comparison. Scanners can be used to:

- Identify a suspect in a crime scene
- Identify victims of motor vehicle accidents
- Identify suspects carrying false or no identity documents
- Identify a homicide victim instantly without having to wait for autopsy results

SmartFinger is a fingerprint recognition technology by IDEX in Norway [25]. SmartFinger film is an ultra-thin and

bendable fingerprint sensor that is suited for identification (ID) and financial cards. The software runs on low-end processors, which means it can be embedded in units of many types, shapes and forms. By integrating the sensor, fingerprint data and software on the card, the cardholder's identity can be verified without the fingerprint data leaving the card. The user does not need to set the fingerprint on an external fingerprint read, and one also avoids the need for a large centralised database. The SmartFinger technology includes the patented fingerprint imaging principle, sensory scheme and chip design. The technology is customisable for one-time password devices, smartcards, ID cards, access control devices and biometric tokens.

The U. S. automated fingerprint identification system (AFIS) [1] is a searching system and also a biometric identification methodology that uses digital imaging technology to obtain, store and analyse fingerprint data. A state database holds fingerprint records. Fingerprints are scanned and uploaded. The software allows the examiner to mark the locations of the ridge characteristics with a marker. The examiner also defines the pattern type and marks the location of the core area. These markers make a constellation with which the computer users use to look for similar patterns on the database fingerprints. The software scores candidates from best to worst depending on how well markers correspond (which is determined by a complex algorithm).

FingerTec's Online Fingerprint identification (OFIS) [10] provides the ideal verification method for secure online access. OFIS runs in a web browser/server environment, where users enrol fingerprints through a scanner linked to a PC. For verification, the scanner reads the user's fingerprint and transmits the encrypted data to the remote backend server through the internet/intranet/WAN/LAN. The server compares and verifies the fingerprint against the stored fingerprint templates.

The patrol car for the Los Angeles country sheriff's department can gain on-the-spot access to the internet and the sheriff's intranet for mobile fingerprint identification, photos, police records, warrants and background checks as well as taking advantage of a global positioning system (GPS) and mapping system which will route police to arrive at calls faster.

Vein recognition technologies (fingers, hands, eyes) read the pattern of veins which is visible under the skin or in the back of the eye for identification. These patterns cannot be photocopied.

The Morpho Touch machine stores the profiles of wanted suspects. A fingerprint captured is compared against the contents of the database. It is widely used by cops at roadblocks, during patrols and searches for criminals [17].

The DNA profile of individuals is added to the bio-bank. Sensor Commons is a future state whereby data is available in real-time, from a multitude of sensors that are relatively similar in design and method of data acquisition and that data is freely available whether as data sets or by application programming interface (API). It is not only lots of data from sensors but also relatively similar in design and method of data acquisition.

Eurosmart is working on standardisation and harmonisation of the workflow and technologies used in the border control process, in order to achieve the right level of interoperability, an equivalent level of security at all borders and a common interface for all travellers. E-passports are biometric passports. The passports provide passive authentication, basic access control security and biometric face image. The European Union (EU) member states are moving to biometric passports with extended access control security protecting access to fingerprint images. E-gate programs are running in 20 countries. They use biometric identification/authentication. At present 3 major biometric technologies are widely used, i.e., fingerprint, face, iris, vein pattern [8].

By scanning on the bar code of a driver's licence, motor car licence or liquor licence, its validity can be automatically verified. Information is transmitted wirelessly to a central database, for verification and response obtained on the same device. This will cut down on accidents due to unlicensed motorists, unauthorised liquor outlets which are normally the hub of crime and carjacking.

- Fraud detection

In South Africa currently, for fraud detection, some banks are linking to the Home Affairs National Identification System (HANIS) which enables biometric identification of current and prospective clients. This service enables banks to verify and authenticate client identity, thus limiting identity fraud.

- Alcohol detection

South Africans consume 5 billion litres of alcohol per year according to the Medical research Council. More that 60% of hospital trauma cases were the result of drunkenness. Half of the road accidents were as a result of drunkenness. Therefore police have got a heavy burden in their hands to control alcohol abuse that leads to higher crime levels. There are a number of IoT devices that can assist [9].

Sensors that measure blood alcohol content by smelling your breath have been around since 1938 when the Drunkometer was invented.

In New Mexico, the Driver Alcohol Detection System for Safety (DADSS) breathalyser-based interlocks in vehicles are attached to the ignition that prevents a car from starting

pending breathing into a tube for a minute to determine blood alcohol levels [7].

Touch spectrometry technology seeks to measure blood alcohol levels via near infrared light which penetrates the epidermis to analyse the composition of the fluids present in the dermis layer of the skin.

Matt Legget invented a jacket that can tell if one is too drunk to drive. They blow into a nozzle that is hidden in the collar. Inside the jacket is an Arduino microprocessor, an alcohol sensor and a series of LEDs. A breathalyser situated in the jacket pocket analyses the breath samples and then lights. The LED glows only when alcohol is detected and the brighter the glow the worse.

Drager interlock XT [6] is a breath alcohol measuring instrument with a vehicle immobiliser. It prohibits a driver who has consumed alcohol from starting the motor car. The Drager interlock XT comprises 2 main components: the breath-alcohol measuring with the measuring system, which is situated the vehicle and the control unit which is installed under the dashboard and allows or prevents current being supplied to the vehicle starter system.

- Surveillance

Closed circuit television camera (CCTV) are used to monitor activities in many important public places like airports, rail stations, business offices, city centres, sports events. They are used to capture and record images for security and surveillance purpose. CCTV cameras can be wired or wireless. However, there are many advantages of wireless CCTV over wired CCTV. One of the benefits of a wireless camera is, it is free from interruption caused by the wires. Wires could be damaged or wrongly configured that could cause the interruptions of the camera function. Unlike wired cameras, a wireless camera can record and store more hours of surveillance on a single disk. The installation process for wireless is easier as there are no wires to configure and set up. Wireless cameras can also take pictures with a higher resolution.

In S.A., ATM bombings have increased 300% in the past 5 years and cost banks millions of Rands in replacing the machine. Banks and cash-in-transit services are increasingly embracing surveillance, off-site monitoring and intelligent alarms. There are over 15,000 ATMs in South Africa. Digital camera surveillance and recording systems are designed for use in both mobile and static applications. These solutions have modern video compression formatting, which is able to deliver high quality video streaming and play back and they support GPRS, GPS, GSM and dial-up connections with modems, as well as the use of TCP/IP for continuous monitoring. In emergency the latest systems are able to send a signal via up to 5 different methods of communication, in order to ensure the alarm signals reach the central monitoring station as quickly as possible. Alarms can now be integrated with lighting systems, so that during an alarm situation the lights are automatically switched on, thereby ensuring that CCTV can obtain the best possible clarity, greatly improving the chances of a successful apprehension.

- Anti-hijack

Insurance companies, South African Police Service (SAPS) and Business Against Crime are working together on an anti-hijack system. An anti-hijack system is an electronic device fitted to motor vehicles to deter criminals from hijacking them. A lockout system is activated when the vehicle drops below a certain speed or becomes stationary. A transponder system will disable a vehicle once the driver leaves the immediate vicinity of the vehicle. The flame blaster is a container of petroleum gas which is activated by pushing a button located near the foot pedals, resulting in 3 metre long jets of burning liquid.

In a real-time GPS tracking system, a "locate" is when a GPS tracking device sends location coordinates to the tracking system to be marked on a map and recorded with a street address if available. This recorded location with any associated data such as date, time, speed, direction, etc is called a "locate". Locates can be generated one of 3 ways:

- Motion-activated tracking is when the unit only turns on when it senses motions or vibrations and sends out locates at a predefined rate for the time it is in motion and shuts down when no more motion is detected
- Constraint tracking is when a tracking device continues to send locates regardless of whether there is any motion
- Location on request is when you only get a location if you send the device a request for it to send back its location

The more locates you get the more dots you see on the map. The GPS logger on the other hand is a solution to monitor behaviour of the driver over a period of time. You can only do this by retrieving the GPS logger for the history.

S.A.'s Inkwazi Vehicle Tracking system [13] is a commercial vehicle tracking system. It monitors vehicle activity and reports changes, in real time, to a monitoring control room. It determines accurate geographic position through GPS and communicates using GSM, SMS and data calls. The unit has an option of adding satellite communication which can be used should the GSM system be unable to communicate.

Cash-in-transit vehicles are fitted with GPS and satellite tracking components and also by making on and off-site video surveillance of vehicles a reality. A joint operational centre to monitor cash delivery vehicles and respond to attacks is in place.

- Crime statistics

Crime figures in South Africa are currently in a bit of a mess. An example can be borrowed from the US. The New York Times released an interactive map titled Mapping Homicides [15]. The data is compiled from open-record requests and major crime reports from the NY police department, including most homicides in addition to new accounts, court records and additional reporting. The map is updated as new information becomes available. Users can filter the data by month and time of day, race, sex and age of victim or perpetrator, weapon used and the district the crime happened.

The Trulia crime maps [27] in the US cities are interactive geo-located heat maps visualising where crime happens most, what types of crimes those are and when they actually happened. The map includes more than 5 million data points aggregated from more than 1000 different sources. Neighbourhood blocks are coloured according to crime density.

- Rapid response

An internet of things application to search optimal routes for rapid response police cars, taking into account the effects of traffic is tenable. With the help of RFID tags in police cars and wireless sensor nodes on the road, the police dispatch control centre can collect real-time traffic conditions where wireless sensor nodes are located. The report messages are sent to the control centre. Based on information from sensor nodes, the control centre forecasts the optimal path to provide the fastest route to a crime scene.

- Keeping track of dockets

To trace dockets and evidence in picture form, a lesson can be borrowed from UCL. The UCL's centre for advanced spatial analysis's 'Tale of Things" project encourages users to "tag objects with digital media using barcodes". Users can upload an image of the object and an associated memory in the form of text, audio or video to the project's website using a dedicated iPhone application. Once the user has entered this information they receive a unique bar code which they can attach to the object. Objects are tagged using RFID tags and QR codes. This code can be read by taking a photograph from a mobile phone or webcam, linking the object back to its entity on the website. The tags will enable future generations to have a greater understanding of the object's past and offer a new way of preserving social history [26].

- Firearm detection

A metal detector is a device which responds to metals that may not be readily apparent. An oscillator producing an alternating current passes through a coil producing an alternating magnetic field. Eddy currents are induced in the metal, producing an alternating magnetic field of its own. If another coil is used to measure the magnetic field, the change in the magnetic field due to the metallic object is detected.

- Copper theft detection

As copper prices increase, the occurrence of copper wire theft increases as well. Reliable detection of theft activity is done by monitoring locations through sensors to detect unauthorised access. It can also be done at electrical-switch locations to continually monitor the response to high-frequency pulses while detecting changes in wire properties of the circuit. It reduces theft rates by quickly responding to unauthorised access alerts.

- Money laundering

Money laundering refers to concealing money earned by illegal means such as drug trafficking, fraud and smuggling, just to name a few. It aims to make illegal transactions appear legitimate and legal. Some steps include transferring money between bank accounts, breaking up large amounts of money into small deposits, or buying acceptable forms of money such as money orders. Anti-money laundering software can detect money laundering practices and generate a report. The software alerts employees when there is a risk and maintains a constantly update watch list of business and people. It checks for purchases over a certain amount. The risk factors are suspicious spending and depositing trends [30].

### *B. Partnerships between police and community*

This section looks at partnerships between the police and community in the fight against crime

- Safe neighbourhoods

Access that national sex offender registry at your fingertips, using GPS technology to locate all the sex offenders in your area. Offender Locator [24] and Offender Monitor [23] in the US helps find sex offenders in the neighbourhood, get informed with detailed records, and receive e-mail alerts of new activity. The information comes from the Home Affairs databases. It includes the convicted crime, birth date and physical profile.

Safer Streets UK is a website where you can tell your local council and police teams where you feel safe or unsafe in your local area and view local safety information. It enables one to:

- Share their views on safety with local authorities, police and community
- View information on safety initiatives provided by local agencies

- Share information which helps local agencies decide how to address safety issues
- Find out more about work being done to tackle crime

SafeRoute US [22] is an Android-based application that gives GPS-enabled crime statistics and safety levels for every city in the US where enough crime data to report is present. The application even takes it a step further to provide safety levels (safe, moderate, dangerous) for every zip code in select major cities. As long as the android device is GPS-enabled, SafeRoute will detect exactly where you are and tell if the area is safe, moderate or dangerous. You can press "crime details" to see detailed crime statistics from the city.

Microsoft's bad neighbourhood detection system is for pedestrian route production. It gathers data, analyses the data and user requirements and generates a route. The user inputs the destination and constraints or requirements they have such as terrain, wheelchair accessibility, avoiding neighbourhoods that exceed a certain threshold of violent crime statistics. The system then analyses potential routes and supplies instruction in the form of a scrolling map, turn-by-turn direction or spoken guidance.

Mind Your Street [16] is an online community which uses social networking to employ situational crime prevention techniques. When implemented, these effectively reduce the opportunity for crime. This site allows individual households and neighbourhoods to identify their real security needs and to make improvements in a highly convenient and cost-effective manner. Hardware such as CCTV may be purchased online and easily integrated into the set-up when required.

For household security, the IoT would resolve the tracking problem by analysing the number of people in a specific area through external sensor equipment. The system would then reminds the people via voice to identify themselves if there is more than one person outside the door. Only when all people pass the authentication would the system turn off the defences and open the door. The system will take action as alarm and vocal warnings if any one of them does not pass the authentication.

A bird's eye satellite view in Google maps can be used to make neighbourhood watch patrol assignment maps, see if a neighbourhood parameter fence has any damage, etc. The services that take advantage of Google Maps, like SpotCrime, which is a free service that shows a detailed history of crimes in and around a neighbourhood can also be utilised.

Social media is a great way to share information with neighbours. You can create a neighbourhood watch Facebook group and set it to 'private" where only those people who are part of the neighbourhood watch team have access. Restricting access is so that criminals do not get information on security measures being taken.

There is a neighbourhood watch site called Home Elephant that integrates Facebook. Home Elephant lets you easily join with neighbours to create an online neighbourhood watch complete with crime watches, lost and founds, a neighbourhood calendar and other great features. Access to Home Elephant is free and they even have a free iPhone/iPad application that provides cell-phone-based neighbourhood alerts as well as quick picture uploading of sketchy happening. Neighbourhood Watch can take pictures of suspicious people and upload it to social media to let other be on the lookout.

Neighbourhood watch IP cameras that record 24/7 can be aimed at neighbourhood entrances, exits and cross streets. The streams from cameras can be viewed via most web browsers without the need for any special software. A home computer can record video from multiple cameras and store it. If there are any incidents in the area, video footage can be shared with law enforcement.

Most alarms have their signals monitored by an armed response company who work with local police when there is a break-in. The alarm and MMS camera alarm system have all zones named and emergency phone numbers programmed. All that is needed is place sensors in areas that need protection. When movement is detected by a wireless motion detector, the siren sounds. Alert to cell phones from a landline or GSM, SMS device, MMS to email functions are also available. A standard alarm system uses motion sensors that keep watch over doors, windows and indoor areas.

In crowd control, more and more people are choosing their mobile devices as their first choice for online activity. Increasing access to the sensors on these devices for location and readings on surroundings has made these tools a primary input for data collection activities. In the geospatial real, OpenStreetMap [20] spatial data building effort uses a community of contributors in a crowd sourcing project that spans the globe, using contributors to take charge of their neighbourhood and continuously adapt as their surroundings change.

Results from cases heard at Birmingham Magistrate's court are being put on Twitter by West Midlands Police. This is meant to make the public aware of the cases police deal with.

- Safer schools

For safer schools CCTV cameras, perimeter fences, metal detectors and alarm systems need to be in place. An alarm system can have GPS coordinates, so that when it goes off the control centre can easily locate the site. Electronic fences can either be wireless of in-ground. Wireless fences have an

electronic base unit that emits radio waves up to a certain range. A receiver and transmitter send an alert to the relevant body. In-ground fence picks up radio waves and beeps once someone crosses the fence. Perimeter security can have fibre optic stretched along the fence. An anomaly such as a bend or twist in the fence, no matter how slight, would show a slight variation in the colour of light (different wavelengths contained in white light reflect at different angles). An optical time reflectometer (a type of radar for light) attached to the fiber optic would locate the spot, within about a meter, where the twist or bend took place and a search light could be instantly aimed at the point [11].

- Public education

Communities have to be educated on community safety and crime prevention issues. From alcohol and substance abuse, youth leadership development, to road safety, family violence, child protection and sexual offences, the partnerships between the police and the community should discuss such issues.

Public information can be disseminated via public portals. Educational or awareness information can then be accessed in a protected environment such as via kiosks or in public facilities such as libraries or health clinics via video, and even from home via cell phone.

Public billboards on electricity poles can also be another technology that is adopted. Public billboards mounted on trees will be the future. When trees use carbon dioxide for synthesis they give out oxygen. Oxygen supports combustion and hence can be harvested for electricity generation. This is called the green economy. Electronic sensors can also be implanted on trees to relay information.

A "baraza" is a Swahili word for an organised meeting/council with a question and answer service to educate members of the community. Instead of physical meetings of citizens, municipalities can set up "virtual barazas" for public education and communication. The communication can be via cell phone, microphone communication from the municipalities or the Internet.

Through social networks a youth counselling service can be set up. Users subscribe to a chat service in which counsellors sit on the other side of the network. They consult on substance abuse, rape, suicide, etc.

### *C. Social crime prevention initiatives*

The International Centre for the Prevention of Crime (ICPC) defines social crime prevention as "anything that reduces delinquency, violence and insecurity by successfully tackling the scientifically identified casual factors of crime" Similarly the South African government's 1998 white paper on Safety and Security states that social crime prevention aims to "reduce the social, economic and environmental factors conducive to particular types of crime". Some of the casual factors include gender inequality, the proliferation of firearms, psycho-social factors and so on.

Crime line is an anonymous crime tip-off line to blow the whistle anonymously. SMS are sent from the citizens anonymously. The number is not is not a crime emergency line. It is a public-private partnership run by civil society [4].

Childline is used by Kenya, Mozambique, Zimbabwe, Namibia and Guinea Conakry. It is to help children who face abuse and are in need of care and protection. VoIP phones with 100% call recordings are available 24 hours x 365 days. It receives about 20,000 calls per month, and resolves 80% of the calls received. The network is connected via fibre optic cable, the data management is formalised with a knowledge base, there is free flowing reporting with automated file extraction and 20 plus call centre systems [3].

Crowd sourcing can assist collect information from the communities. Vista data vision is an application to help, manage, visualise and analyse sensor data from real-world objects. Using Vista Data Vision's applications it is possible to store logged data from devices and display and publish it to the web. Vista Data Vision also provides an interface that allows users to view the data from logged devices via a Google Map.

Street lighting is important in the fight against crime. The establishment of a mesh of street lights, will ensure that when one of the lights is off, the mesh connects wirelessly to the control centre to alert staff on the problem, rather than rely on power line transmission. Alternatively the working light takes over the functionality of the one that is off.

GIS technologies can be adopted to detect vegetable cover. Alerts are sent to the relevant municipal department to cut grass when it is of a certain height. Also to detect building and bare land to ensure appropriate planning and avoiding vacant land and open spaces, which are potential crime areas.

## V. ARCHITECTURE

This section consists of subsections on identified characteristics and the architecture of a biometric identification system and another on the architecture of the parolee monitoring system.

### *A. Characteristics identified*

By going through the systems that have been identified in the previous literature, the following characteristics of the systems which will feed into our architecture were identified.

- Biometric identification based on physical and behavioural traits including fingerprint, face

recognition, DNA, palm print, handwriting, iris recognition, voice and gait

- Scanning technologies such as RFID, motes, QR codes, etc, to scan and digitalise these biometric traits
- Comparison algorithms for the matching the digital traits against the biometric data that is collected on all individuals
- Mobile communication technologies such as GPS, GPRS and GSM
- Detection and tracking technologies
- Predictive and decision-making capabilities to interpret the data
- Mechanisms for notification of users.

### *B. Biometric Identification System Architecture*

Before a person is released on parole, their biometric details are captured onto a National Biometric System that is managed by the Department of Home Affairs. The data, which is either fingerprint, palm print signature, photo of face, DNA, document, etc. is captured by way of a mobile scanner, that is, it can be captured from anywhere at any time. It is then passed on to the central server in the Home Affairs Department through a GSM/GPRS network. GPRS is a packet-oriented mobile data service on 2G and 3G cellular communications to transmit internet protocol (IP) packets to external networks such as the internet. GSM is a global system for mobile transmission for 2G digital cellular networks. See Figure 1 for the details.

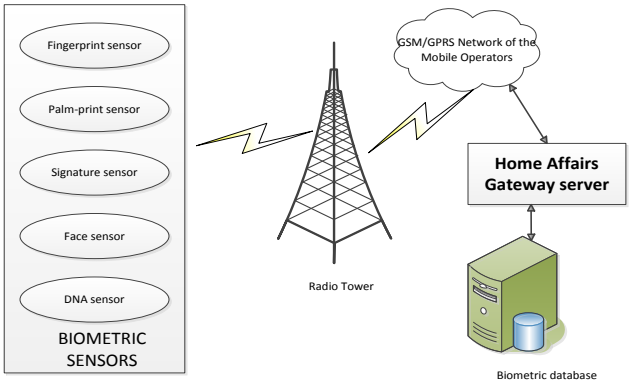


**Figure 1: Biometric identification**

### *C. Architecture of the parolee monitoring system*

When parolees are released they are governed by certain conditions of parole. The parolee is tagged with a tracking device e.g. an radio frequency identifier (RFID) tag in the form of a bracelet. The assumption is that the tracking device is not detachable. This tracking device has a GPS or GSM Sim Card (CHIPSET) for location of the parolee at any point in time. If the data is generated via the GSM CHIPSET it is routed by the mobile operator network to the Correctional Services Department. If it is GPS-enabled, it is routed via satellite to the Correctional Services Department. The Biometric database is connected to the Correctional Services Department systems via a virtual private network (VPN) for security of data. Also the Correctional Services Department links to a database on the conditions of parole for each parolee of a particular ID tag. If the parole conditions (e.g. moving out of a zone of 5 kilometres from residence) are violated then and alarm is triggered on the Correctional Services System and the biometric database releases details of the individual to the monitoring officer for further action. This can be on a desktop computer or on a mobile phone. See Figure 2 for details.

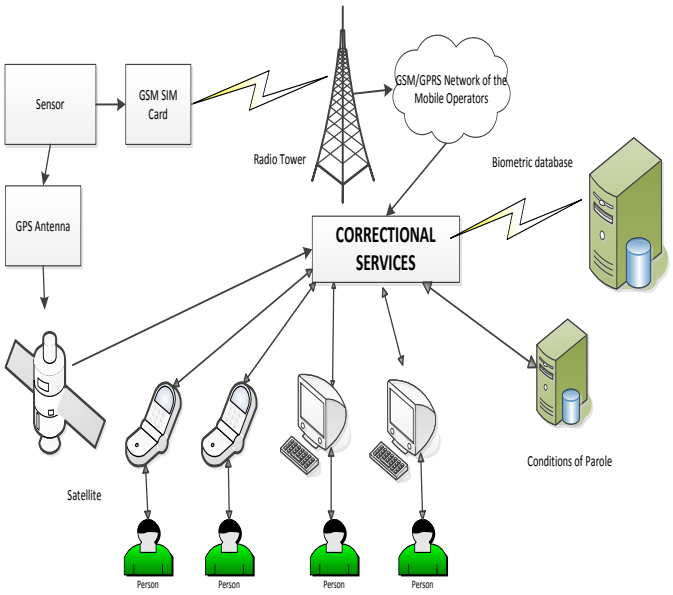


**Figure 2: Parolee monitoring**

## VI. CONLUSION

Although a number of IoT technologies identified in this research may sound familiar, the question of how far they are in use in South Africa still remains. The current national DNA database only holds profiles of certain but not all suspects and convicted criminals. Therefore there are still delays in the criminal justice system if a new offender cannot be identified quickly through DNA profiling. Fingerprint technology is the most common technology in use in South Africa. The South African passport is not yet biometric although it contains certain security features. There is still room for improvement to catch up with the EU's biometric passport which is a more reliable form of authentication.

The IoT is about the integration of a varied range of traditional ICT technologies in applications for various domains. Therefore it offers a new research area for South Africa, with an enhanced potential towards improving community safety and crime prevention. ICTs have had an adoption in many sectors of the economy generally speaking, but IoT is an approach from a different angle. It is about utilising and combining the strengths of each of the various traditional technologies that are integrated into any one application. Lessons are also being drawn from other

international players who are already developing and using IoT technologies.

The research does not cover all aspects of community safety and crime prevention as it is, but only those applications that could be identified. It could do with additions in areas such as performance indicators, crime threat analysis, public order maintenance, etc., to name but a few.

The research shows the potential applications of the IoT that can reduce, deter or prevent the occurrence of crime and ensure community safety. These applications fall under law enforcement, situational crime and social crime prevention. The final result of this document is to inform policy on the adoption of IoT in community safety and crime prevention. The study can also be used by developers of new IoT technologies as a base to building S.A specific IoT technologies for crime prevention and community safety.

## REFERENCES


[1] Automated Fingerpring Identification system (AFIS), http://searchsecurity.techtarget/definition/Automated-Fingerprint-Identification-System, Available online, Accessed 28/7/2013

[2] CASAGRAS, RFID and the inclusive model for the Internet of Things report, EU Project Number 216803, pp 16-23, 2011

[3] Childline, www.childline.org.za, Available online, Accessed 28/7/2013

[4] Crimeline, www.crimeline.co.za, Available online, Accessed 28/7/2013

[5] Crime Report 2010/2011, SAPS

[6] Drager interlock XT, www.ignitioninterlock.biz/products.html, Available online, Accessed 28/7/2013

[7] Driver Alcohol detection System for Safety, http://www.driveralcoholdetectionsystemfor safety.com/, Available online, Accessed 28/7/2013

[8] ePassport and Border Control, Eurosmart: the voice of the smart security industry, 2009

[9] Fact sheet – alcohol use in South Africa, http://www.sahealthinfo.org/admodule/alcohol.htm, Available online, Accessed 28/7/2013

[10] Fingertech's online fingerprint identification systems, http://www.fingertec.com/images/brochure/OfisTA-E.pdf, Available online, Accessed 28/7/2013

[11] Gruber, R., Perimeter security: detect, delay and deny, Master Halco Security Solutions Group, US, 2012

[12] How to start a high-tech neighbourhood watch, http://netsecurity.about.com/od/security101/a/How-To-Start-A-High-Tech-Neighbourhood-Watch, Available online, Accessed 28/7/2013

[13] Inkwazi Vehicle Tracking system, www.marshall.co.za/veh-inkwazi.html, Available online, Accessed 28/7/2013

[14] Internet of Things in 2020: Roadmap for the future, Infso D.4 networked enterprises & RFID Infso G.2 Micro and Nanosystems in co-operation with the Working Group RFID of the ETP EPoSS, Version 1.1, 27 May, 2008

[15] Mapping Homicides, http://infosthetics.com/archives/2009/06/mapping-homicides_in_new_york-City_2003-2009.html, Available online, Accessed 28/7/2013

[16] Mind Your Street, www.mindyourstreet.com/about-mind-your-street.html, Available online, Accessed 28/7/2013

[17] Morpho Touch Machine, www.justiceforum.co.za/community%20prosecutors/11.pdf, Available online, Accessed 28/7/2013

[18] National Crime Prevention Strategy, www.info.gov.za/otherdocs/1996/crime1.htm, Available online, Accessed 28/7/2013

[19] Online Fingerprint Identification System, www.fingertec.com/images/w-brochure/OFIS_e.html, Available online, Accessed 28/7/2013

[20] Open Street map, http://www.openstreetmap.org, Available online, Accessed 28/7/2013

[21] Raunio, B., The Internet of Things, A report from the November 5, 2009 seminar, .SE:s Internet guide, Nr. 16, - English edition, Version 1.0, Sweden, http://www.internetdagarna.se/program-2009/5-november, 2009

[22] Safe Route App, http://market.android.com/details?id=dd.SafeRoute&hl=en, Available online, Accessed 28/7/2013

[23] Sex Offender Locator, http:/techcrunch.com/2009/07/the—iphones-latest-hit-app-a-sex-offender-locator, Available online, Accessed 28/7/2013

[24] Sex Offender Tracker, http://market.android.com/details?id=com.fsp.android.h&feature=search_result, Available online, Accessed 28/7/2013

[25] SmartFinger, www.idex.no/News/Successful-testing-of-IDEX-Smartfinger-film.aspx, Available online, Accessed 28/7/2013

[26] Tales of Things, taleofthings.com/totem/about, Available online, Accessed 28/7/2013

[27] Trulia crime maps, www.geekosystem.com/trulia-crime-maps, Available online, Accessed 28/7/2013

[28] White paper on Safety and Security (1999-2004) pp. 14

[29] Why S.A. is so violent and what we should do about it, Centre for the Study of Violence and reconciliation, 9 November 2010

[30] What is money laundering?, http://wisegeek.com/what-is-money-laundering.htm, Available online, Accessed 28/7/2013

[31] Zhihao, X., Yangfeng, Z., Main-topic- internet of things and its future, http://www.huawei.com/publications/view.do?id=6098&cid=1139&pid=61, Available online, Accessed 28/7/2013