Proof of Concept of the Online Neighbourhood Watch System

Stacey Omeleze[1(✉)] and Hein S. Venter[2]

[1] ICSA Research Group, Computer Science Department,
University of Pretoria, Pretoria, South Africa
someleze@cs.up.ac.za
[2] Computer Science Dept.,
University of Pretoria, Pretoria, South Africa
hventer@cs.up.ac.za

Abstract. Potential digital evidence captured by an onlooker at a crime scene when stored in a repository can be used during criminal investigations, or as admissible evidence in a court of law. However, to employ the captured and stored potential digital evidence (PDE) some challenges are required to be dealt with, such as, retaining the forensic soundness of the captured PDE, adequate measures to secure the PDE and measures to protect the privacy rights of the PDE uploader (citizens).

In previous work, the authors proposed a conceptual model termed online neighbourhood watch (ONW). The ONW model allows community members to use their mobile devices in capturing PDE, store the captured PDE to a repository to be used in neighbourhood crime investigation in South Africa. But, the focus of this paper is to present a proof of concept of the ONW model. The proof of concept outlines the functional and architectural requirements specifications of the ONW system and evaluates the performance of the underlying functional requirements using mathematical proofs in testing the forensic soundness of the captured and stored PDE. Furthermore, using the information security services mechanisms, the forensic soundness indicators (FSI) are generated. The FSI ensures originality, authenticity and admissibility of PDE from the ONW system.

Keywords: PDE · Forensic soundness · ONW system · Digital evidence · Information security services · Repository

1 Introduction

The high rate of crime in South Africa demands a proactive community response to tackling the menace of these crime. Mobile devices are among the most used electronic devices [1], mobile devices can therefore be used as crime fighting, monitoring or prevention device when its camera, voice-recording and image-capturing functions are employed as a real-time potential digital evidence (PDE) capturing tool. In previous work, the authors modelled the online neighbourhood watch (ONW) conceptual model [8,9], that enables community members

R. Glitho et al. (Eds.): AFRICOMM 2015, LNICST 171, pp. 78–93, 2016.
DOI: 10.1007/978-3-319-43696-8_9

in South Africa to use their mobile devices in capturing potential digital evidence (PDE) of crime. The mobile devices capture images, audio and video recordings of criminal activities in their neighbourhoods stored to be used that can be used to convict the criminals.

The purpose of this paper is to provide a proof of concept for the ONW model. This is to identify the practical aspects of the conceptual model, determine the challenges that are not readily seen during the conceptual modelling and explain the design and development process of the ONW system. The proof of concept entails the development of an application termed uWatch. uWatch is a crowdsourcing medium that involves community members to use their mobile devices to in generating potential digital evidence (PDE) of crime. It also includes a web application termed neighbourhood watch system. The ONW system utilised by the law enforcement agents (LEA), digital forensic investigators (DFI) or the judiciary to access and download the stored PDE during neighbourhood crime investigation or prosecution. The ONW system employs the information security services mechanisms to maintain confidentiality, integrity, authentication, authorisation and non-repudiations (CIAAN) of captured and stored PDE [15]. The CIAAN mechanisms are used in conjunction with the forensic soundness indicators (FSI) properties to verify the forensic soundness of PDE captured with the ONW system, while maintaining chain of custody, chain of evidence, and protecting the privacy rights of the uploader (citizen).

2 Digital Forensics

Digital forensics is drawn from the field of forensic science which has been developed in conjunction with the biological sciences. It is used to determine the path of digital data during a digital forensic investigation, whether for criminal or civil proceedings in a court of law or private inquiries in order to re-construct incidents to establish what happened.

Cohen [2] defines digital forensics as a subject that started between art and craft containing a scientific body of knowledge with an underlying scientific methodology and consisting of four basic elements. These elements are the study of previous and current theories and methods, conducting experiments to prove the theories, identification of inconsistencies between theories and the repeatability of these experiments in correlation with expert witnesses. Evidence determines the flow of major decisions, in criminal or civil investigations. It establishes that an incident occurred to initiate any form of investigation. Hargreaves [4] defines digital evidence as a reliable object that can uphold or refute a hypothesis in legal or civil proceedings. That means, for the admissibility of digital evidence, its integrity must be proven with a certain degree of reliability

For electronic data to be used as evidence, it must be in its originally uncontaminated state and maintain evidential weight. Using the information security service mechanisms [15] and upholding legal standards of evidential weight [3,14], the forensic soundness of digital data can be achieved. Forensic soundness of digital data is ensured when confidentiality, integrity, authentication, authorisation

and non-repudiation are in place using the information security services mechanisms of cryptography, digital signatures, cryptographic hash functions and access control [11,13,15].

In order to legally employ the captured potential digital evidence (PDE) to either commence investigations or be used as 'real' evidence in a criminal or civil proceeding, the stipulations and guidelines from various acts must be adhered to. These acts include the Electronic Communications and Transactions (ECT) Act, Act 25 of 2002 [3], the Privacy of Personal Information (POPI) Act, Act 4 of 2013 [12] and the Regulation of Interception of Communications and Provision of Communication-Related Information (RICA) Act, Act 70 of 2002. These acts deal with the protection of an individuals privacy but also spells out when individuals and criminals lose those rights when national security is at stake. This has major implications for the ONW system and how PDE can be used.

3 Methodology

In developing the proof of concept of the ONW system, the methods employed include: *(i)* The use of set theory to formulate a proof of forensic reliability of PDE captured and stored in the ONW repository, which is then implemented using programming languages. *(ii)* The use of programming languages framework, APIs, and IDEs in the implementation of the ONW system which consists of the uWatch application and neighbourhood watch system. The languages include PHP web socket for a dynamic lightweight and high efficiency server-end, JavaEE, Python-Django framework, and Bootstrap framework that allows the authorised PDE downloader the use of any device ranging from mobile device to table or desktop computers. The bootstrap framework allows for a responsible web front design and performs usability functions. *(iii)* The use of Android development platform for the uploader's application-side. *(iv)* MySQL and SQLite databases are used for the uploader's application-side and downloader's-side respectively. The database storage are in forms, converted to JASON objects.

4 The ONW System Design

In designing the ONW system, the benefit of implementing the ONW conceptual model as well as the quality of captured PDE is portrayed using the functional and non functional (architectural) requirements and the constraints mapped out to achieve the ONW system's objectives. Part A of the ONW system is designed as a mobile device application. Part B is designed as a web application to be used by the downloader. Part B also deals with the retention of confidentiality, integrity, maintaining access management of the authorised users, and the verification of PDE authenticity in order to determine its admissibility.

4.1 Functional Requirements

Functional requirements focuses on the behaviour and capabilities that describe the use cases, capturing the roles of the various users of the system [7]. The use cases are mapped to roles describing the functions that each role holder performs - see Fig. 1. The primary actors of the ONW system are the PDE uploader, the LEA/DFI, judiciary and the system manager. Each role performs a functions of a case as follows: *(i)* Capture potential digital evidence; *(ii)* Verify the forensic soundness of the captured potential digital evidence; *(iii)* Store potential digital evidence, while making it available to the authorised users (i.e. LEA, DFI and judiciary); *(iv)* Maintain access management to the stored PDE, in order to protect the privacy of the citizens and abide by the rule of law [14].

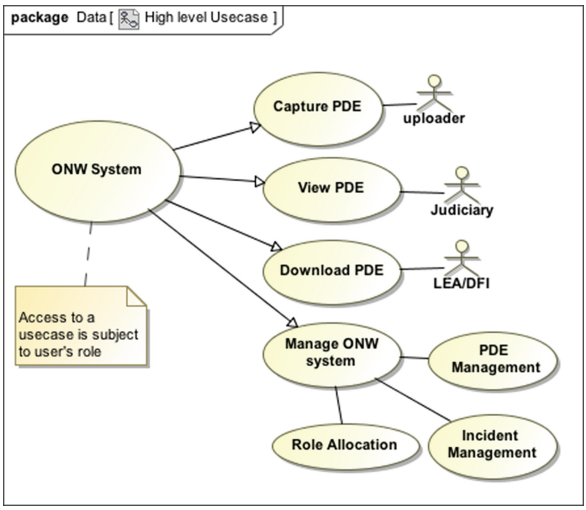

Fig. 1. High-level use case of the ONW system

Uploader: The uploader role is attributed to a human user (citizen). The citizen uses a mobile device to capture PDE which is uploaded to the ONW repository and then receives notifications. The notifications are meant to update uploaders on PDE-sourcing efforts to motivate citizens in neighbourhood crime minimisation. The notifications are provided by the ONW system as usage statistics and citizens status such as, when an uploaded PDE passes the forensic soundness checks, and when a citizen's uploaded PDE is utilised as real evidence during crime investigation or in a court of law.

The Judiciary: The judiciary role is carried out by any member of the judiciary such as the court clerk or legal counsel to the plaintiff or defendant, especially in situations where stored PDE is to be utilised as real evidence to shed light on a case before the court. The Judiciary may require to view the PDE, which is then made available to all parties involved. For the ONW system to attain its set

goals of usefulness and admissibility in any court of law, the role of the judiciary is essential as it ensures that all processes operate within legal boundaries.

The Law Enforcement Agent and Digital Forensic Investigator: As depicted in Fig. 1, the actor role of the Law Enforcement Agent (LEA) is bound to that of the Digital Forensic Investigator (DFI) who may assume both roles when required. The function of the LEA is to download PDE from the ONW repository to corroborate the first respondent's report, the physical crime scene and possible eye-witness testimony of the alleged incident. The LEA uses the date, time, location or incident type to determine whether PDE is valid or applicable to a case under investigation. The LEA also manages the ONW system along with the system administrator. For example, PDE retrieved to investigate a case relating to an assault crime must be focused on assault related crime search criteria using date, time, and location to correlate the incident to other assault crimes.

Manage the ONW System: Manage the ONW System functions includes incident record management and role allocations. These functions are shared responsibilities between the LEA and the system administrator. The ONW system validates PDE, returns exception, success or failure of transaction notifications, performs PDE forensic soundness check, controls access management, adds or removes roles, and audits log maintenance. The system management ensures that PDE is accessed by the LEA according to the attributes of the case.

4.2 Architectural Requirements

Architectural requirements provide the infrastructure within which the system components can realise the functional requirements [7]. The ONW system's architectural requirements include the system access channel requirements, architectural responsibilities, quality requirements and the architectural constraints. Each of which is used in correlation to the architectural patterns and strategies to promote the quality requirements of the system. The ONW system's access channels are via web - i.e. HTTPS using RESTful with secure message channels and mobile application interface for the uploader (citizen).

ONW System's Architectural Responsibilities. The ONW system's architectural responsibilities are the architectural requirements that the system must support through which the system is evaluated. The ONW system is based on a layered architectural pattern, supported by other architectural patterns such as, model view controller (MVC), microkernel architectural patterns, pipes and filters architectural patterns and decorator patterns. The MVC is used at the access layer to ensure separation of concerns, while pipes and filters and microkernel architectural patterns are used to support the business logic layer and the persistence layer to ensure security, reliability and stability of the system. Furthermore, these ensure that the functional requirements (i.e., capture PDE; ensure confidentiality, integrity, authentication, authorisation and non-repudiation (CIAAN); store captured PDE; manage access of stored PDE)

are realised using architectural requirements. These architectural requirements include the use the following features: *(i)* Web interface which is employed to separate the business logic from the access layer, this is in order to avoid direct access to the content of the back-end system. It maintains control of events from the business logic (I/O) to the persistence layer. *(ii)* The persistence layer supports Object Relational Mapper. *(iii)* Transactional processes associate components or users to activities within the system using interceptor patterns. *(iv)* The microkernel adapters enable the addition of external systems and flexible communication channels between the access layer, business logic and the persistence layer. *(v)* Ensuring confidentiality, integrity, authorisation, authentication and non repudiation (CIAAN) of captured PDE. *(vi)* Ensuring that the ONW quality requirements (i.e., security, auditability, usability, auditability and pluggability) are realised.

5 Explaining the ONW System

In developing the ONW system, two aspects were the focus: the uploader's part (mobile application-side) which is termed uWatch application and the downloader part called Neighbourhood watch system. The uWatch application is developed using the Android development platform. The neighbourhood watch system, which is a web application is developed using Python Django framework with BootStrap framework, and JavaEE. The choice is based on the architectural responsibilities of the system. For example, the Django framework accommodates databases, such as MySQL, and reference architecture framework like JavaEE and PHP server, thereby allowing for easy storage of audio, video or images.

5.1 uWatch Application

uWatch uses the existing functions of Android devices (i.e. camera and microphone) in the PDE capturing processes. It enables members of a community to capture images, videos and audios of criminal behaviour within their neighbourhood and upload the captured PDE to the ONW repository. The uploaded PDE is analysed by the law enforcement agents and other authorised users during neighbourhood crime investigations.

As shown in Fig. 2, at the launch of uWatch, the user is prompted to select which form of PDE they wish to capture (i.e., photo image, video or audio) of the alleged criminal activity. At the selection of any of the option buttons in Fig. 3 the built-in camera or audio features of the Android device is activated to commence PDE capturing. PDE can be captured by an eye-witness with or without WIFI or cellular network data connectivity. This is achieved using the queue service event where offline captured PDE is posted to a remote url using ThreadPoolExecutor. The remote url also provides similar services of capture-to-upload-later, when there is a slow or unsuccessful transaction to the ONW repository. The type of incident and the location where the incident occurred is selected by the citizen (see Fig. 3). The location selection is used by the LEA

Fig. 2. User interface of the uWatch application

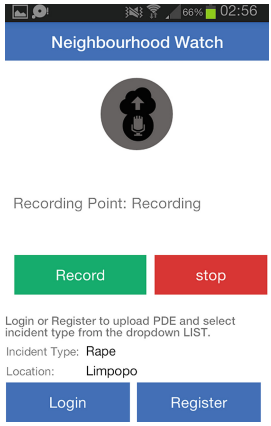

Fig. 3. Audio-capturing Process using uWatch application

to cross-reference geographical locations. The location selection enhances PDE originality checks. However, to upload the captured PDE, the citizen is required to log-in, meanwhile, authentication is not required to capture PDE, it is only required at PDE upload to the ONW repository. Finally, the stored output is stored as $\{Z\} = (E_{ncrypt} \wedge (DGsign) \wedge (Geolocation, timestamp) \wedge (\#PDE_p)$. An acknowledgment feedback mechanism is in place to notify uploader and components at successful or failed forensic soundness checks, when PDE uploaded by the citizen is download for investigation, or used as real evidence.

5.2 Neighbourhood Watch System

The neighbourhood watch system is the downloader-side of the ONW system. It's users are the system administrator, LEA, DFI, the judiciary or other authorised users who utilise sourced PDE during crimes or civil investigations or as real evidence in a court of law. Meanwhile, only an authorised user with access credentials is able to download PDE from the ONW repository by creating a caseName, caseNumber and caseType.

The neighbourhood watch system is developed with the Django framework which is used due to the framework's abstraction level in web development using Bootstrap framework to absorb Hypertext Mark-up Language (HTML), Cascading Style Sheets (CSS) and Javascript at the usability design process [5]. On the transactions between the uWatch application and the neighbourhood watch system, servlets initialise a call function from the access layer to the persistence layer through the business logic layer. It converts forms to JSON schema parse through the HTML using RESTful Web service and PHP cluster. The JSON objects format is used because it is faster to parse, lighter, flexible with PHP, and it presents data in a more readable format over the XML message transfer protocol.

5.3 Usability

The usability of the ONW system is realised using a decorators pattern and the Bootstrap framework to enhance better user experience, easy operation with little to no training required for downloaders or citizens to utilise the system. Figure 4 shows images, videos and audios captured and stored as PDE in the ONW repository. Each captured PDE holds location co-ordinates, the provinces (for example Eastern cape - see Fig. 4), time and date, type of alleged crime and the checksum value of the PDE. While on the uWatch application (Android side) SQLite is used to send PDE both online or offline to a queue that is synchronised as JSON objects via HTTPS.

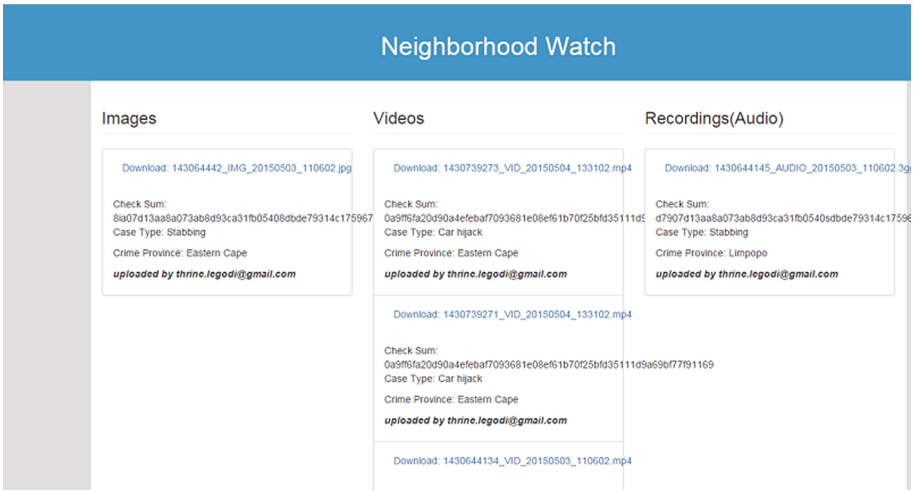

Fig. 4. Stored PDE with metadata in the ONW repository

5.4 Auditability

The auditability functions of the ONW system is maintained using MySQL trigger, PDE validation and global interception. Trigger automates the audit-log, while rules are created by the rule engine and specified at system's configuration to allow traceability of authorised user's actions.

5.5 PDE Storage

For PDE storage, the neighbourhood watch system uses MySQL and PHP to enable the insertion of binary data to database tables, and specifying the required PDE using rules based on the case under investigation [9]. The platform and scalable functionalities of MySQL enable the ONW system to handle concurrent user base, while captured PDE is stored as a JSON object. At any given state, the

uploaded optimised PDE object is in the form of: $\mathcal{Z} = \{N\} \wedge \{M\} \wedge \{x_j\}$ (i.e., Encryption $(E_{ncrypt} \wedge (Cryptographichash - (\#)) \wedge$ (Digital signature) $\wedge (PDE_p) \wedge$ (Geo location) $\wedge$ (Date/timestamp) $\wedge$ (Device type) $\wedge$ (Wifi connection identifier)). The upload and stored PDE data includes the AES encrypted version of the checksum value of the PDE, which is digitally signed in collaboration with the timestamp, to determine the time of PDE acquisition, and the geo-location showing where PDE was acquired in correlation with other metadata like the device type, wifi connection or GSM data connection. This process ensure consistency with the chain of evidence and the chain of custody, so as to ascertain what operations were performed during the acquisition and storage process.

5.6 Security - Forensic Soundness Indicators

PDE captured using the ONW system is only useful for neighbourhood crime investigation or as real evidence in any court of law when the captured PDE is forensically sound. To ensure the originality and authenticity of PDE, the forensic soundness indicators (FSI) are introduced. FSI are used to indicate the level of soundness (originality, authenticity and validity) of captured PDE. It is the process that merges information security services mechanisms of confidentiality, integrity, authentication, authorisation and non-repudiation (CIAAN) [15] with PDE FSI properties to ensure the reliability of PDE captured and stored using the ONW system. Throughout this paper, the FSIs refers to CIAAN mechanisms and the PDE properties of forensic soundness. The mechanisms employed to implement CIAAN are: *(a)* Confidentiality - which is realised using *encryption*. *(b)* Integrity is realised using *cryptographic hash function*. *(c)* Authentication is realised using *session authentication, username and password*. *(d)* Non-repudiation is achieved using *digital signature*. While the PDE FSI properties used to address forensics soundness in conjunction with the CIAAN mechanisms are: *(a)* Timestamp *(b)* Geographical location tag. *(c)* Device type. *(d)* International mobile equipment identifier (IMEI). *(e)* Wifi connection identifier. *(f)* GSM data connection.

Testing Forensic Soundness of PDE using Mathematical Illustration To ascertain the reliability and forensic soundness of captured and stored PDE, a test is carried out using set theory and elementary logic algebra [6,10]. The conducted test is focusing on identifying the *minimal-state* of forensic soundness of any captured and stored PDE is denoted as set $\{\mathcal{W}\}$ and the *optimal-state* is set $\{\mathcal{Z}\}$ as depicted in Figs. 5 and 6 respectively.

Figures 5 and 6 is described as follows: The elements of PDE is defined as the set of $X\epsilon$ {video, audio, and photo}, where video, audio or photo is referred to as $\{x_1\}$ or $\{x_2\}$ or $\{x_3\}$ respectively. For clarity, $\{x_1\}$ is video, $\{x_2\}$ is audio and $\{x_3\}$ is photo. The FSIs are represented as the set of $\{Y\}$, which consist of $Y\epsilon$ {encryption, cryptographic hash, digital signature, geo-location, timestamp, device type, IMEI identifier, wifi connection identifier or GSM data connection}. Where set $\{Y\}$ is further decomposed to consist of sets $\{N\}$ and $\{M\}$ i.e., $\{Y\} = \{N\} \wedge \{M\}$. Where set $\{N\}$ represents the FSIs focusing on

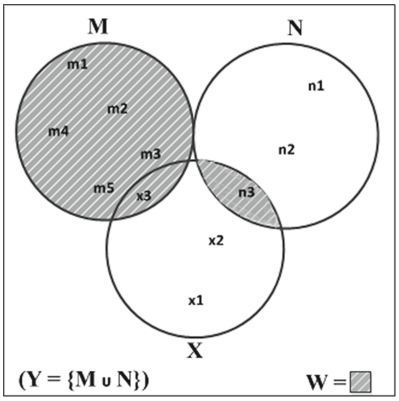

Fig. 5. Is set $\mathcal{W} = \{\{\}(n_3 \cap x_3) \cup \mathcal{M}\}$

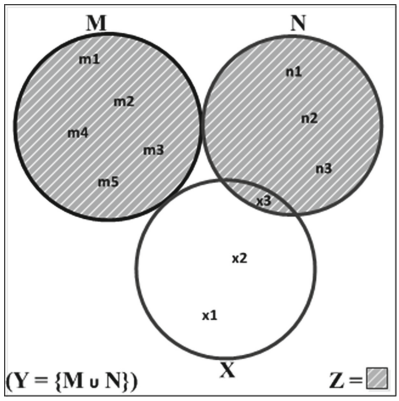

Fig. 6. Is the set of $\mathcal{Z} = \{\{\}(\mathcal{M} \cup \mathcal{N}) \cap x_3\}$

CIAAN mechanisms - $\{N\}$ consists of $\{n_1\}$ or $\{n_2\}$ or $\{n_3\}$ where $\{n_1\}$ represent encryptions, $\{n_2\}$ cryptography hash and $\{n_3\}$ digital signature respectively. Set $\{M\}$ consists of geo-location, timestamp, device type, IMEI identifier, wifi connection identifier or GSM data connection which represents $\{m_1\}$, $\{m_2\}$, $\{m_3\}$, $\{m_4\}$ and $\{m_5\}$ respectively, where $\{m_5\}$ can be either wifi connection identifier or GSM data connection at any given set of $\{M\}$. Therefore the set $M = \{m_1, m_2, m_3, m_4, m_5\}$.

To test for the forensic soundness of the captured PDE, the shaded portions of sets $\{\mathcal{W}\}$ and $\{\mathcal{Z}\}$ as depicted in Figs. 5 and 6 is used. Where set $\{\mathcal{W}\}$ consists of exactly one element of $\{X\}$ i.e., either $\{x_1\}$ or $\{x_2\}$ or $\{x_3\}$, this is so because at any given PDE capturing process, the captured PDE data object is either a video, or an audio or a photo image (see Figs. 5 and 6) because the PDE cannot be more than one of these elements at the same time. For example, the illustration in Figure 5 shows that $\{x_3\}$ i.e., photo is used. The selection of at least one or more elements of set $\{N\}$ i.e., $\{n_1\}$ and/or $\{n_2\}$ and/or $\{n_3\}$ and the selection of a complete set of $\{M\}$ is necessary to obtain the set $\{\mathcal{W}\}$. For example in the illustration of Fig. 5 the whole elements of set $\{M\}$ is include, recall that the set $\{M\}$ is $\{m_1, m_2, m_3, m_4, m_5\}$ and the selection of $\{n_3\}$ i.e., digital signature is employed to generate set $\{\mathcal{W}\}$. An illustration that shows the processes employed to determine the validity of PDE captured in its most minimal-state of forensic soundness of any given PDE is denoted as set $\{\mathcal{W}\}$ - is as follow:

Proof. - to Illustrate - the processes of obtaining the minimal - state of PDE $\{\mathcal{W}\}$. Let set $X = \{x_1 \vee x_2 \vee x_3\}$ - that is, select a video, or audio or photo. Let set $N = \{n_1 \vee n_2 \vee n_3\}$ - that is, select at least one of cryptographic hash and/or encryption, and/or digital signature. Let set $M = \{m_1 \wedge m_2 \wedge m_3 \wedge m_4 \wedge m_5\}$ that is, the product of geo-location, timestamp, device type, IMEI identifier, wifi connection (i.e., select all elements of $\{M\}$).

Therefore the set $\mathcal{W} = \{x_1 \vee x_2 \vee x_3\} \wedge \{m_1 \wedge m_2 \wedge m_3 \wedge m_4 \wedge m_5\} \wedge \{n_1 \vee n_2 \vee n_3\}$ - which means set $\{\mathcal{W}\}$ is the collection of one element of set $\{X\}$ i.e. $\{x_3\}$, at least one element of set $\{N\}$ i.e., $\{n_3\}$ and a complete set of $\{M\}$ - substituted as shown in Fig. 5 resulting in $\mathcal{W} = (M_{x1n1} \vee M_{x2n2} \vee Mx3n3)$.

- Recall that the illustration is to show the minimum requirements of any PDE to be stored in the ONW repository, this therefore means that the first case scenario of forensically sound PDE is $\{M_{x1n1}\}$ that is, a selection of all elements of set of $\{M\}$, selection of one element $\{x_1\}$ which is photo and the selection of one element $\{n_1\}$ that is cryptographic hash. Meanwhile, this process can be the selection of any of $\{M_{x1n1}\}$ or $\{M_{x2n2}\}$ or $\{M_{x3n3}\}$. Each case results in the lowest minimal-forensic soundness-state of any PDE. Following the example of set $\mathcal{W}$ in Fig. 5, $\{\mathcal{W}\}$ is the selection of $\{x_3\}$, $\{n_3\}$ and $\{M\}$, $\{\mathcal{W}\}$ is $\therefore$ $\mathcal{W} = \{M_{x3n3}\}$.

The next possible value of $\{\mathcal{W}\}$ is realised by increasing the number of elements of $\{N\}$ to exceed more than one. Equating the value of $\{n_1\}$, $\{n_2\}$, $\{n_3\}$ to be i, therefore i can be defined as $i = \{n_1, n_2\}$ or $i = \{n_1, n_2, n_3\}$. While set $\{X\}$ can be defined as j, so that, at any given PDE capturing process, j represents video, audio or photo. This is because a citizen can either capture a video or an audio or photo image at any circumstance - $\therefore$ $j = \{x_1\}$ or $j = \{x_2\}$ or $j = \{x_3\}$ which means the selection of either video $\{x_1\}$ or audio $\{x_2\}$ or photo $\{x_3\}$ is equated to j - Therefore, the in-between (mid-level) forensic soundness state of PDE is derived to be - $\mathcal{W} = \{M_{xj} \wedge M_{ni}\}$ where $\{M\}$ is the FSI properties that ascertain the forensic soundness, x_j is the captured PDE and $\{n_i\}$ is the selection of more than one elements of set $\{N\}$.

$\therefore \forall \mathcal{W} \exists \{M_{xjni}\}$ - meaning for all $\{\mathcal{W}\}$ there exist exactly one captured PDE (video or audio or photo), a complete set of $\{M\}$ (geo-location, timestamp, wifi, device description, etc.) and at least one or more elements of set $\{N\}$ (i.e., encryption, cryptographic hash function and digital signature).

In summary the minimal-forensic soundness-state of any given PDE object is $\mathcal{W} = \{M_{x3n3}\}$, while there is an in-between level which is higher than minimal-state, but less than in-between-state of forensic soundness $\mathcal{W} = \{M_{xjni}\}$, while the optimal-state of forensic soundness is $\{\mathcal{Z}\}$. Therefore there are three state of forensic soundness of PDE captured with the ONW system - minimal-state $<$ mid-level-state $<$ optimal-state of forensic soundness - With the Equation $\{\mathcal{W}\} < \{M_{xjni}\} < \{\mathcal{Z}\}$ is the various states of PDE forensic soundness. Recall that the illustration above is focused on showing the minimal-state $\{\mathcal{W}\}$ of PDE, which also derived the in-between-state (mid-level-state) $\{M_{xjni}\}$ of PDE forensic soundness. Next paragraph is the proof to show the optimal-forensic-soundness-state of PDE $\{\mathcal{Z}\}$.

Proof. - to Illustrate the processes of obtaining the optimal-state of PDE $\{\mathcal{Z}\}$. Let set $X = \{x_1 \vee x_2 \vee x_3\}$ - that is, select a video, or audio or photo. Let set $N = \{n_1 \wedge n_2 \wedge n_3\}$ - that is, select all elements $\{N\}$ (i.e., cryptographic hash and encryption, and digital signature).

Let set $M = \{m_1 \wedge m_2 \wedge m_3 \wedge m_4 \wedge m_5\}$ - select all elements of $\{M\}$ (i.e., geo-location, timestamp, device type, IMEI identifier, wifi connection identifier).

Therefore the set of $\mathcal{Z} = (x_1 \vee x_2 \vee x_3) \wedge (m_1 \wedge m_2 \wedge m_3 \wedge m_4 \wedge m_5) \wedge (n_1 \wedge n_2 \wedge n_3)$ - That is the set $\mathcal{Z}$ is the collection of one element of set $\{X\}$ i.e. $\{x_3\}$, all element of set $\{M\}$ and all elements of set $\{N\}$.

$\therefore \mathcal{Z} = \{N\} \wedge \{M\} \wedge \{x_3\}$, which is $\mathcal{Z} = \{MN_{x3}\}$. The elements of set $\{X\}$ can be video, or audio or photo, however, in reference to the example in Fig. 5, the element $\{x_3\}$ is selected. Therefore alternatively the set $\mathcal{Z}$ can be represented as $\mathcal{Z} = \{MN_{xj}\}$ where $\{x_j\}$ can be any selection of video, audio or photo.

Forensic Soundness Validations. The goal is to establish the forensic soundness validation of PDE captured with the ONW system, using the three states of PDE forensic soundness i.e., the optimal-state of PDE $\mathcal{Z} = \{MN_{xj}\}$, the mid-level state $\mathcal{W} = \{M_{xjni}\}$ and the minimal-state $\mathcal{W} = \{M_{x3n3}\}$ of forensic soundness of any PDE. These are used to formulate equations to show the validation process for PDE captured using the ONW system. The elements of $\mathcal{W}$ and $\mathcal{Z}$ are substituted at each case that is, optimal-state, mid-level state and minimal-state of forensic soundness. Taking the first derived illustration of $\mathcal{W}$ (i.e., $\{M_{x3n3}\}$) the substitution is presented as Eq. (1).

$$\mathcal{W} = \{M_{x3n3}\} \tag{1}$$

The predicate of Eq. (1) is the minimal requirements, because only one element of the set of $\{N\}$ that is, $\{n_3\}$ is considered at FSI checking. For example using Eq. (1) to validate photo PDE - set $\mathcal{W}$ becomes: $\mathcal{W} = \{M_{x3n3}\}$ where $\{M\}$ is (Geo location, Timestamp, device type, IMEI identifier and wifi connections), $\{x_3\}$ is the captured photo (PDE_p) and $\{n_3\}$ is the cryptographic hash (#). The output becomes the checksum of the photo PDE ($\#PDE_p$) and the embedded FSI properties ($\{M\}$ (i.e. Geo location, Timestamp, device type, IMEI identifier and wifi connections) - $\#(PDE_p \wedge M)$ is the final output of Eq. (1). However, to increase the forensic soundness of PDE, using only cryptographic hash (#) with the embedded PDE FSI properties $\{M\}$ may require additional factors, thereby enhancing the forensic soundness of the photo PDE (PDE_p). To realise the high strength forensic soundness, Eq. (2) replaces (1) in the forensic soundness validation check.

$$\mathcal{W} = \{M_{xjni}\} \tag{2}$$

The predicates of Eq. (2) is derived by adding encryption to the output of Eq. (1), therefore realising the in-between (mid-level) forensic soundness state of captured PDE. Set $\mathcal{W}$ becomes: $\mathcal{W} = \{M_{xjni}\}$ where $\{\mathcal{M}\}$ is the FSIs properties, $\{x_j\}$ is either video, audio or the photo PDE (PDE_p) (Photo PDE is used as in Fig. 5 example), and $\{n_i\}$ is cryptographic hashing of photo PDE and the addition of encryption. By using $\{n_i\}$, the predicate of Eq. (2) enhances the forensic soundness of captured PDE. Where $i = \{n_1, n_2\}$ or $i = \{n_1, n_2, n_3\}$, that is, cryptographic hash is $\{n_1\}$, encryption $\{n_2\}$ and digital signature $\{n_3\}$). The substitution for $\mathcal{W} = \{M_{xjni}\}$ becomes ((Geo location, timestamp, device

type, IMEI identifier and wifi connections - M), x_j is the photo PDE - (PDE_p) with cryptographic hash - (#) and encryption (E_{ncrypt})) - The output becomes $E_{ncrypt}(\#(PDE_p \wedge M))$. Meanwhile Eq. (2) upholds two of the CIAAN mechanisms and all the PDE FSI properties, however there is room for stronger forensic soundness implementation to ascertain photo PDE (PDE_p) validity. Eq. (3) therefore insert all elements of set $\{N\}$ to achieve an optimal-state of the photo PDE (PDE_p) forensic soundness.

$$\mathcal{Z} = \{MN_{xj}\} \tag{3}$$

Equation (3) uses all the elements of set $\{N\}$ and that of set $\{M\}$, therefore Eq. (3) is the most efficient forensically sound process to ensure authenticity and originality of PDE stored in the ONW repository. This makes set $\{\mathcal{Z}\}$ the strongest predicate compared to set $\{\mathcal{W}\}$. For example to employ Eq. (3) i.e. $\mathcal{Z} = \{M\} \wedge \{N\} \wedge \{x_j\}$ the expression becomes adding digital signature ($DGsign$) to the encrypted (E_{ncrypt}) PDE $\{x_j\}$ (photo PDE - (PDE_p)) and $\{M\}$ (Geo location, timestamp, device type, IMEI identifier and wifi connections) and $\{N\}$ (cryptographic hash - (#). That is $DGsign(E_{ncrypt}(\#(PDE_p \wedge M))$.

Equation (3) however makes it possible to add digital signature in conjunction with cryptographic hash and encryption to the photo PDE to enhance its admissibility and ensure its forensic soundness, which is not possible with Eqs. (1) and (2). However, for Eq. (3) to hold, there are trade-offs to efficiency and high cost of resource implementation such as, processing time, architectural requirements specifications that encompasses the requirements of meeting the demands of Eq. (3). Meanwhile, to reduce cost while retaining the forensic soundness of the Photo-PDE, Eq. (2) may be employed. This notwithstanding, for the proof of concept of the ONW system, Eq. (3) is used. This is because using all elements of sets $\{\mathcal{M}\}$ and $\{\mathcal{N}\}$ is the most efficient method to retain forensic soundness, ensures chain of custody and chain of evidence of any PDE captured using the ONW system.

5.7 Measures to Ensure Users Privacy

For citizens to participate in the PDE sourcing process, or utilise the sourced PDE in criminal/civil investigations or in any court of law, their privacy rights of must be preserved as far as possible. Therefore adequate measures are put in place to uphold legal requirements regarding evidential weight, hearsay, rule of relevance and completeness, especially when the individual or witness wishes to invoke the non-compellable clause, as in Sect. 203 of the CPA Act, Act 51 of 1977 [14]. The ONW system is designed to eliminate the need to request uploader's information. However, when such a situation presents itself, the authorised downloader has to adhere to the validation rules put in place. To this effect, the ONW system uses four methods for privacy protection:

(i) The use of the public and private key pair for encryption and decryption of citizen's information like device metadata to ensure confidentiality while

protecting privacy. For example, an authorised downloader requires a corresponding public key to obtain citizen's details or device metadata when needed to corroborate an crime scene documentation or first respondents report during neighbourhood crime investigation.

(ii) The downloader must obtain a formal and legal authorisation, such as a warrant, to obtain the user's information or device metadata.

(iii) The non-compellable witness clause of the Criminal Procedures Act (CPA), Act 51 of 1977, Sect. 203 [14] makes possible for an uploader to choose when to testify or provide his or her personal information.

(iv) The use of a traditional username and password applying password rules to increase user's awareness of the need to use unique username and password. Furthermore, citizen's log-in details are stored on their device, while their details stored in the back-end of the ONW system are encrypted using the public-private key system.

In summary, the profile information provided by the user is encrypted using the PKI system. Moreover, in a situation where an investigator requires the identity of an uploader to verify certain details of an uploaded PDE, the authorised user is then required to go through the legal process for obtaining authority (i.e. warrant) in order to access uploader's information. When the warrant has been obtained, the authorised user is then required to provide a matching key that corresponds to the uploader's encryption key.

6 Discussion

The requirements for privacy rights sometimes conflict with the methods devised to eradicate neighbourhood crime. However, technological innovations and the prevalence of the World Wide Web has made it viable to achieve neighbourhood crime watch using mobile devices' built-in technology like camera and audio functionalities. Using mobile devices as a tool in neighbourhood crime watch is motivated by the rise in neighbourhood crime across South Africa, which demands a proactive means to encourage community members to take part in neighbourhood security. The mathematical proofs are used to illustrate the forensic soundness of PDE captured using the ONW system. It showed the processes employed to determine the reliability of captured and stored PDE $\{X\}$.

The ONW system is required to protect the privacy of the uploader, however, anonymity is not completely guaranteed in the ONW system. This is because, a sourced PDE that has complete anonymity loses its completeness and evidential weight therefore rendering the PDE invalid [3]. According to the ECT Act, evidential weight is determined by establishing a clear origin of any digital evidence. Untraceable PDE loses evidential weight and therefore is inadmissible.

However, to the protect the privacy of citizens, the use of the public private key encryption (PKI) system [11] is employed where the downloader matches a decryption key to obtain access to uploader's information. It adds a third layer of security to the already existing cryptographic hash (first layer) and digital signature (second layer). The legal requirements of obtaining a warrant

is an additional constraint when an uploader's details are necessary. Although according to the Criminal Procedures Act (CPA), Act 51 of 1977 Sect. 203 [14] an uploader may plea the non-compellable witness clause, thereby exempting the witness from testifying.

One assumption of the ONW system is that the uploader is able to capture PDE at a safe distance from the crime scene to avoid self-endangerment. It also assumes an uploader can identify what constitutes a crime. However, the psychological state of mind of the uploader, as well as what constitutes a potential crime, fall outside the of scope of this paper.

7 Conclusion

The ONW system's proof of concept shows the processes employed to ensure that stored PDE retains forensic soundness from the time of PDE capturing to storage and final usage. The various states of forensic soundness made previsions to ascertain the validity of captured PDE. Opting for the optimal-state of PDE forensic soundness, the ONW system provides admissible potential digital evidence of neighbourhood crime.

Acknowledgment. This work is based on the research supported wholly or in part by the National Research Foundation of South Africa (Grant Numbers 88211, 89143 and TP13081227420).

References

1. Aker, J.C., Fafchamps, M.: Mobile phone coverage, producer markets: evidence from west africa. World Bank Econ. Rev. lhu006 (2014)
2. Cohen, F.A.: Digital Forensic Evidence Examination. Fred Cohen and Associates Out of Livermore, 3rd edn. (2009). 9781878109446
3. Government Gazette: Electronic Communications and Transactions Act, Act 25 of 2002. Technical report, PDF Scanned by Sabinet. Accessed 08 February 2014. South Africa Government Gazette - Legislation- South Africa - National/Acts and Regulations/E/Electronic Communications and Transactions Act No. 25 Of 2002/The Act, August 2002
4. Hargreaves, C.J.: Assessing the reliability of digital evidence from live investigations involving encryption. Ph.D. thesis, Deartment of Informatics and Sensors, Cranfield University, UK (2009)
5. Holovaty, A., Kaplan-Moss, J.: The Definitive Guide to Django: Web Development Done Right. Apress (2009)
6. Klir, G., Yuan, B.: Fuzzy Sets and Fuzzy Logic, vol. 4. Prentice Hall, New Jersey (1995)
7. Bass, R.K.L., Clements, P.: Software Architecture in Practice. Part of the SEI Series in Software Engineering Series, 3rd edn. Addison-wesley Professional, USA (2012). ISBN -13: 000-0321815734, ISBN-10: 0321815734
8. Omeleze, S., Venter, H.S.: Towards a model for acquiring digital evidence using mobile devices. In: Tenth International Network Conference (INC 2014) and WDFIA 2014 Plymouth University, UK, pp. 1–14 (2014)

9. Omeleze, S., Venter, S.H.: A model for access management of potential digital evidence. In: 10th International Conference on Cyber Warfare and Security (ICCWS), pp. 491–501. CSIR, University of Vender and Academic Conferences Limited (2015)
10. Pawlak, Z.: Rough set theory and its applications to data analysis. Cybern. Syst. **29**(7), 661–688 (1998)
11. Charles Pfleeger, P., Pfleeger, S.L.: Security in Computing, 4th edn, pp. 35–43. Prentice Hall Publication, Upper Saddle Rivers (2006). ISBN:0132390779
12. Government-Gazette POPI-Act: Privacy and data protection - discussion paper 109 (project 124) - South African law reform commission (2005–2010). Technical report, Accessed 08 August 2014. South Africa Government Gazette - Legislation - South Africa - National/Acts - Privacy and data protection Act No. 4, August 2013
13. Saleem, S., Popov, O., Dahman, R.: Evaluation of security methods for ensuring the integrity of digital evidence. Institute of Electrical Electronics Engineers (IEEE Xplore Digital Library) (2011)
14. Schwikkard, P.-J., Van der Merwe, S.E.: Principles of Evidence. Juta and Company Ltd. (2009). ISBN:978 0 7021 79501
15. Susanto, H., Almunawar, M.N., Tuan, Y.C.: Information security manage-ment system standards: a comparative study of the big five (2011)