A Secure Context-aware Content Sharing Kiosk for Mobile Devices in Low-Resourced Environments

Achilley Kiwanuka Ssebwana and Engineer Bainomugisha

***Abstract*—Despite the explosion of mobile subscribers in Sub-Saharan Africa, there is still a challenge of delivering the appropriate content to the users taking into account of various Internet connectivity constraints and emerging security requirements. Although technologies for information sharing are steadily growing, the communication infrastructure that provides the backbone of third or fourth generation connectivity requires a lot of capital and is often limited by geographical coverage. Motivated by these challenges and constraints, this paper presents a design of the *Secure Context-aware Content Sharing Kiosk*, an enhancement to the previous Content Sharing Kiosk approaches with support for secure online and offline content distribution and sharing. A hybrid of a role and lease-based security and privacy model was embedded in the design to control distribution of information across different recipients. The lease-based security and privacy model combines the strengths of the role-based security and privacy models by allowing mobile content users to have control over the content sharing through pre-defined conditions of content leasing. Such conditions include time and location thereby enabling users able to lease out information to other users on the network. Upon expiry or violation, the leased information expires. In order to renew access to such information, users are able to request for the renewal of the lease from the content owner. The designed Kiosk was validated using a case study for content sharing in a hospital setting. The research results of this paper, contributes new knowledge in the line of design and development, and can be re-used in other settings with minimal customization, including remote regions with intermittent Internet coverage.**

***Index Terms*—Mobile kiosk, content sharing, context-aware, low-resourced environments, open sharing toolkit, lease-based, privacy, security, integrity.**

I. Introduction

There are about half billion mobile subscribers in Sub-Saharan Africa of which about 239 million people are regular mobile Internet users [1], [2]. A mobile phone is a primary means to connect to the Internet for the majority of Internet users in Sub-Saharan Africa. The proliferation of mobile phones coupled with the growing Internet connectivity has accelerated access to essential services in areas such as healthcare, education, entertainment and financial services [1], [3]. The number of unique mobile subscribers in Sub-Saharan Africa is expected to grow to over 600 million by 2025, equivalent to about half of the population [2]. The steady growth of mobile subscribers and Internet users can be attributed to a range of factors including reduction of Internet costs, availability of cheap smartphones, infrastructure, and enabling policies.

The growth of mobile technology uptake has a huge impact on the economy generating over 8.6% of the total Gross Domestic Product (GDP) in Sub-Saharan Africa and adding over 3.5 million jobs to the economy. This is projected to grow to 9.1% (or $185 billion) of GDP by 2023 [2]. The increase of mobile phone subscribers has resulted in increased demand for digital services and more so for locally developed content and services. For instance it is reported that there were over 390 million users registered for mobile money services [1].

With such benefits in place, mobile devices have become a very important aspect of society. This is evident with the current information spaces created as a result of mobile devices, social media impact on society in terms information sharing about health, education, businesses, entertainment, jobs, politics, and religion, among others. Social media spaces such as Facebook, has over 16 million subscribers in the East African region [3]. The increased demand for digital content and services calls for research into innovative approaches to meet the ever changing user needs and optimized for the unique technology constraints.

Although such personal technologies are steadily growing, the communication infrastructure that provides the backbone of 3G/4G connectivity requires a lot of capital and is often limited by geographical coverage. The majority of the population remain unconnected, with 40% of the low and middle income population projected to remain offline by 2025 [1]. This leaves a lot of phone users with connectivity problems, as countrywide coverage in developing countries is not yet attained. This creates a need for the provision of communication facilities to people in sparsely populated areas, but such infrastructure provision, Internet availability is less profitable. We argue that the approaches for content delivery need to be diversified to include support for content and information sharing in a peer-to-peer fashion, with or without Internet connectivity. However, sharing content in such a manner raises new content distribution requirements and security challenges that are further described below.

A. Motivation and Case Study

Consider a case study, where a patient visits a hospital setting. Upon arrival, they get access to the hospital network, and access the queuing application, on their smartphone mobile devices. Based on the queuing details entered, nurses are able

This paper was submitted for review on 31st December 2019. The authors would like to thank the anonymous reviewers for the suggestions and feedback to improve the paper. This work was partially supported by the Sida/Bright project 317 in the context of the Sweden/Makerere Research programme 2015-2020.

A. K. Ssebwana and E. Bainomugisha are with the Department of Computer Science, Pool Road, Plot 56, Makerere University, Uganda (e-mail: ssebwana@gmail.com, baino@cis.mak.ac.ug)

to take the required assessment and their details are queued for the doctor. At this point, the doctor conducts an assessment and sends the patient to the laboratory to conduct the necessary tests. When tests are completed, the patient is sent back to the doctor where he/she is able to receive the prescription, then they queue for drugs, and eventually exit the hospital premises.

In such a scenario, the context-aware Kiosk sharing application would be of benefit. Furthermore, information related to the required tests done, and the results are shared with the patient, depending on their condition. Patients are sent to the lab to conduct tests, based on the doctor's assessment. All this information is relayed to the patient's mobile device, but access is only allowed while the patient is still in the hospital.

B. Requirements of a Secure Context-aware Content Sharing Kiosk

The above scenario motivated the design of a Secure Context-aware Content Sharing Kiosk design and development key requirements which are:

1) Spontaneous Kiosk Discovery: The context-aware Kiosk application should be able to publish its content and discover content available at other devices within the same environment with or without Internet access. For instance, when a user launches an application that is built using context aware application, they should be able to see nearby devices and share content when needed. The context aware application should allow users to create and share content using their device. For instance, in the above scenario, patients and healthcare workers in the same space should be able to discover each others devices and freely share information in a peer-to-peer fashion, should they choose to do.

2) User Specified Content Sharing Conditions: A content sharing condition-bound "contract" should be established by both parties involved in exchanging information. Upon expiry, the content owner should retain ownership of the content. For example, in the case of a doctor and patient, the patient can grant a lease to the doctor to permit access key patient data while the patient is within the hospital premises and would automatically revoke the lease/access upon the exit. Contextual conditions for data sharing can be pre-defined by the developers or users. For instance devices on the same Wi−Fi network can have one binding condition, those within a specific geographical location and distance would constitute another.This makes it possible to share information either in read-only or read-write mode. Upon violation of such conditions, content access is revoked by the application.

Furthermore, it should be possible for users to *renew the lease of the shared content.* When a lease expires, the content owner or any other user with the appropriate content rights should be able to issue a renewal. In the above example, the patient could initially issue a time-based lease access to the doctor (e.g., 10 minutes) while at the hospital premises. If the patient wishes to extend the access to the doctor beyond 10 minutes, the Kiosk should provide such support.

3) Transitive and Propagated Security and Privacy Mechanisms: It should be possible for the content owner to determine whether the information will be read-write or read-only. With that in mind, content users are restricted on how they use the information. In the above example, suppose a patient shares key personal information with a healthcare worker (both using their mobile devices), it should be possible for the patient (content owner) to specify whether the healthcare worker can, for instance, share the patient's content with a fellow healthcare worker. The content owner should also have means to specify whether the recipient of the content can edit the information.

II. Overview of the Context-aware Content Sharing Kiosk

This section presents a secure context-aware content sharing Kiosk that is designed to address the requirements in Section I-B. The Kiosk facilitates secure exchange of information through the integration of role and lease based privacy and security model. This is implemented to facilitate information sharing through the use of roles and activities to assign privileges to different content users. Through the assignment of a timeline, a particular user is able to access content shared for a specified time. Upon either expiry or violation, the user has options of renewing the lease. There are conditions underlying renewal of the lease. Such conditions include having the content owner or issuer of the lease being on Wi−Fi(established network). In scenarios where the content owner is not on Wi−Fi, or a Virtual Private Network (VPN) established from the smartphone devices to the application kiosk network, there should be another user with privileges to issue a content lease to another person or contact the content administrator, to share the information accordingly. Short of those two options, a user will lose access to the content.

The remainder of this section, explains the core components and functionalities of the Kiosk, and how the different components interact with each other. Fig. 1 shows the architecture and key properties of the context-aware content sharing Kiosk.

A. Online and Offline Support of the Kiosk

The application supports content distribution when the Internet is available (online) but also supports application users when Internet is not available (offline). This is achieved through the use of the online Kiosk web-application database to synchronize content onto the client devices running the Kiosk. With this design, users are able to share content on smartphones, using available wireless technologies such as Bluetooth and Wi−Fi. While offline, devices running the Kiosk have local storage that is based on SQLite, a self-contained and highly reliable database. Users are able to initiate connections using their local hotspots or Bluetooth connections, devices are paired, and content is leased into their local SQLite databases.

B. Discovery of Client Kiosks and Device Connections

Based on the mechanism of content sharing selected by the Kiosk user, available devices are selected for content distribution onto another device. Should Bluetooth be selected, the Kiosk identifies available Bluetooth enabled devices using

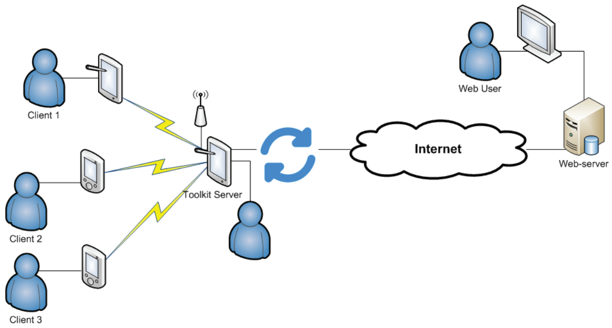


Fig. 1. Client server architecture.

intent filters.Once content sharing is initiated, the Kiosk application requests pairing with the client device, once successful, content is shared onto the other device, and is accessed through an Hypertext Markup Language (HTML) viewer application. The Kiosk sharing mechanism is implemented on top of the Android Operating Systems (OS) intents and intent filters to enable the discovery and opening of the corresponding Kiosks.

C. *Content Replication Across Devices*

To achieve the necessary data replication on another device, there is a transition from client-server infrastructure to a peer-to peer infrastructure which facilitates content sharing or distribution for users in close proximity. The structure of the Kiosk is modeled in such a way that, once there is a Wi−Fi connecting the two devices, the Kiosk Internet Protocol (IP) address will be identified and displayed on the device running the Kiosk Fig. 1. Pairing of devices follows and users are able to share information through replication on to the other device local SQ-Lite database. This Information is accessed in the Kiosk its-self. There is no need for the Kiosk user to have other information viewers to access such information. Information housed in the Kiosk can be exchanged securely from one user to another.

Furthermore, permissions set by the user sharing are inherited by the recipient device. A user who initiates the exchange is able to identify the IP address of the nearby connected device, and information is shared successfully. Mobile application developers can easily integrate the toolkit components facilitate content distribution.

III. Hybrid Lease and Role-based Privacy Model

The Context-aware Kiosk incorporates a hybrid of lease and role-based security model. In this model, each content element is represented as an object whose access and sharing is restricted and controlled by means of a *lease* and a *role*. A lease is a contract that gives its holder specified rights over "property" for a limited period of time [12]. In the context of this paper, content is the property. A role is a collection of privileges that enable access to system information by an authorized user [18]. The role based security and privacy model is used to control user permissions whereas the lease based security and privacy model is used to control information sharing.

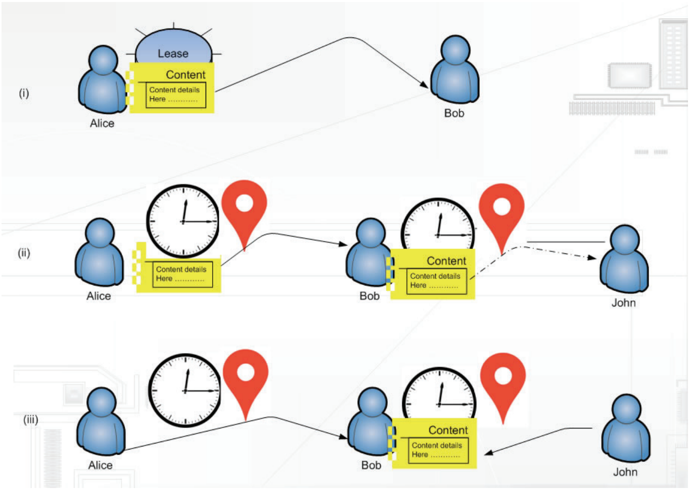


Fig. 2. Lease based Security and Privacy Model

A. *Lease−based Security and Privacy Model*

A lease is a condition that is associated with an object that specifies the boundaries of access for the content. An example of a lease can be time (e.g., 10 minutes). Upon expiry or violation of the specified conditions, users no longer have access to such information unless they renew their lease as shown in Fig. 2.

From the Fig. 2 (i), content is sent from sender node to receiver node. A lease is associated with the content being shared by the two users or devices communicating. The sender node is regarded as the issuer of the lease, whereas the receiver node is the recipient of the lease. To further illustrate the lease-based security and privacy model, we present different scenarios of leasing.

1) Time-based Lease for Content Sharing: In a time-based lease for content sharing, a lease is for a time period. The time specifies how long the content can be available for access. On expiry of the time the content will no longer be available unless the issuer of the content renews the lease. In case of a scenario in Fig. 2(i) consider two users Alice and Bob. Suppose that Alice tries to exchange information with Bob, then, Alice will issue a lease to Bob on the content Alice is sharing. Upon expiry, Alice will retain ownership of the content. This is illustrated in Fig. 2 (i). Fig. 2 (i) and is summarized in the steps below:

i) Alice exchanges information with Bob (A⇒B)
ii) If the lease expires, Alice, retains control over the information from Bob (A⇐B)

2) Condition-based Lease Model: In a condition-based lease for content sharing, time can be one of the conditions for content sharing. Another condition can be location and are determined by the user or the developer. Suppose that Alice tries to exchange information with Bob, then, Alice will issue a condition based lease to Bob for the content Alice is sharing. Upon violation of any of the conditions, Alice will retain ownership of the content. This is illustrated in Fig. 2(ii).

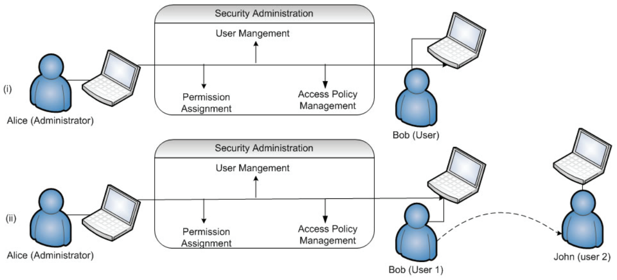


Fig. 3. Role-based security and privacy model.

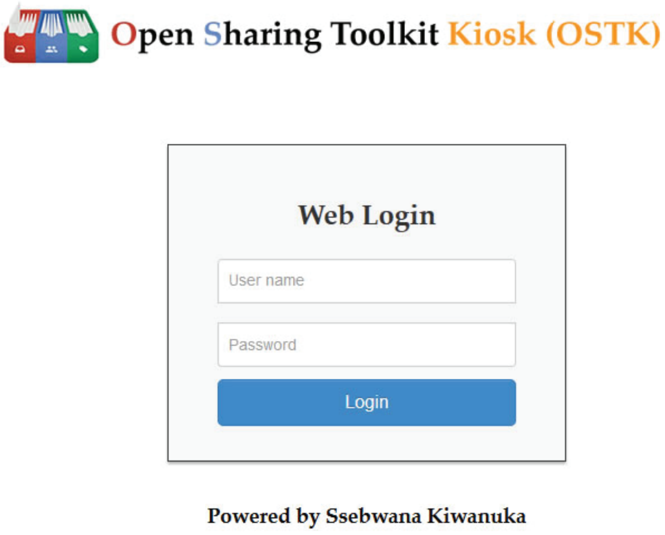
3) Subleasing: Subleasing is possible when a user who has been issued with a lease, is given permission to share the same lease, or determine conditions of sharing the same information with other users. For instance, time or condition based leases for content sharing, can be modified further to allow content sharing with other users. The main content lease in this case overrides the rest of the subleases given to other content users. Upon elapse of the main lease, the rest of the sub-leases will no longer be applicable. The issuer of the content, the *sublessee* is able to sublease within the limits of the main lease. Suppose that Alice grants a lease to Bob with share access (sub-leasing), then, Bob will issue a sub-lease to John on the content Bob has permissions to sublease. Upon expiry or violation of the specified conditions, Bob will retain ownership of the content. Upon expiry of the main lease, Alice will regain control of the information that was shared. This is illustrated in Fig. 2 (ii).

4) Lease Renewal: Lease renewal comes into play when the time specified for the lease expires. Furthermore, it is possible to request renewal of the lease, in case the location where the information was tagged to be viewed is violated. In case of such scenarios, users are able to request a lease renewal in order to have access to the information once again. It is possible to request lease renewals in case the issuer of the lease is still available on Wi–Fi, or a user with the same privileges is on the Wi–Fi. This is illustrated in Fig. 2 (iii).

B. Role–based Security and Privacy Model

We adopt the definition from role-based security Systems, where a role is defined as *a collection of privileges that enable access to system information by an authorized* user [18]. A role is distinct from the user (or role holder) and a role encapsulates all the required functionality for the associated authorized user to performance the expected operations.

Inline with the role-based access control systems [22], the first steps for the role-based security and privacy model involve identifying the users and the roles they can perform. From the Fig. 3(i), Alice is the administrator and has the ability to assign user roles to other users of the system. A user is able to access the kiosk objects by executing the assigned role. In this implementation different user roles to select from are defined at design time. In Fig. 3(ii), Alice grants read write permissions to Bob. In this case Bob is able to issue and manage such permissions to another user such as John. As such, permissions shared with users will have read-write permission, and users are allowed to share with other users. Suppose that Alice grants permissions to Bob with share access, then, Bob will be in position to share such privileges with John. This is illustrated in the Fig. 3 (ii).


Open Sharing Toolkit Kiosk (OSTK)

Web Login

User name

Password

Login

Powered by Ssebwana Kiwanuka

Fig. 4. Login page for the kiosk.

IV. Validation

To validate the context-aware content sharing Kiosk presented in II and Sections III, the hospital case study implemented in Section I-A. The Kiosk application for the hospital setting includes the Kiosk web app and client mobile app as discussed in the remainder of this section.

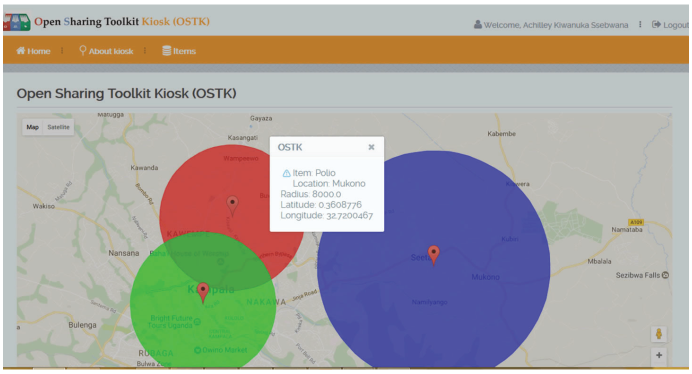
A. Kiosk Web Application

The data was gathered to establish the existing information sharing applications and how they work in the dissemination of information to users. This helped in designing of the Kiosk inclusive of most of the functionalities that help in dissemination of information to all intended recipients. Navigation into the Kiosk is described as follows: Once the Kiosk Web application is started, it opens the login page which is shown in Fig. 4. The Kiosk administrator, is be able to login given the correct authentication. Once the Kiosk web-application opens, the super administrator can perform all the administrative roles in the Kiosk as shown in Fig. 4.

Once the user logs into the Kiosk, they view a brief description of the information in the Kiosk and the general health of the system on the home page as shown in Fig. 5.

As a follow up on the Kiosk web–app, a user is able to compose information and can prepare it for download by other client applications or devices. On the web, users accessing the media–hub are able to view content, share, preview and modify it based on the permissions assigned to the user by the application administrator, as shown in Fig. 6.

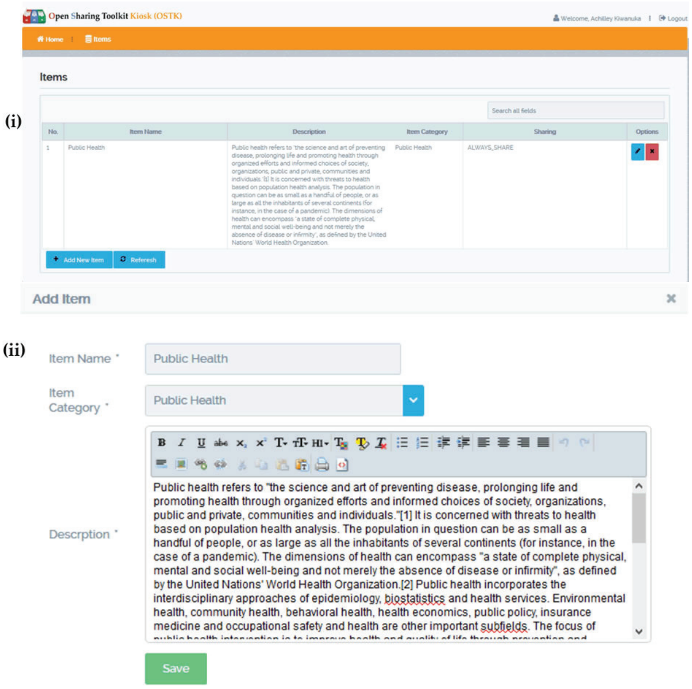
From the content editor Fig. 6, content authors without programming skill are able to author content and share it with other Kiosk users.



OSTK

Item: Polio
Location: Mukono
Radius: 8000.0
Latitude: 0.3608776
Longitude: 32.7200467

Fig. 5. Kiosk home page.



No.	Item Name	Description	Item Category	Sharing	Options
1	Public Health	Public health refers to 'the science and art of preventing disease, prolonging life and promoting health through organized efforts and informed choices of society, organizations, public and private, communities and individuals.'[1] It is concerned with threats to health based on population health analysis. The population in question can be as small as a handful of people, or as large as all the inhabitants of several continents (for instance, in the case of a pandemic). The dimensions of health can encompass 'a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity', as defined by the United Nations' World Health Organization.	Public Health	ALWAYS_SHARE	

Add Item

Item Name * Public Health

Item Category * Public Health

Descrption * Public health refers to "the science and art of preventing disease, prolonging life and promoting health through organized efforts and informed choices of society, organizations, public and private, communities and individuals."[1] It is concerned with threats to health based on population health analysis. The population in question can be as small as a handful of people, or as large as all the inhabitants of several continents (for instance, in the case of a pandemic). The dimensions of health can encompass "a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity", as defined by the United Nations' World Health Organization.[2] Public health incorporates the interdisciplinary approaches of epidemiology, biostatistics and health services. Environmental health, community health, behavioral health, health economics, public policy, insurance medicine and occupational safety and health are other important subfields. The focus of

Fig. 6. Media hub content editor.

B. Kiosk Mobile Client Application

Kiosk mobile application synchronizes information composed on the web-version of the Kiosk and utilizes it for the major purpose for which it was composed, file sharing. In this version, this is where online and offline content sharing is achieved. Online content sharing caters for the applications such as Gmail, WhatsApp, Facebook among others. Offline content sharing caters for Wi−Fi and Bluetooth enabled devices. In line with the hybrid of lease and role-based security and privacy model, the security model is applied to offline file sharing.

C. Online and Offline Content Leasing

Online file sharing is possible when there is Internet connectivity. Kiosk users are able to view content authored in the media hub and view connected devices. Depending on the state of Internet connectivity, and they are able to view content which is already synchronized from the web-application, download what is not yet synchronized and share it on emails or over Internet. This is achieved by clicking the **`Reload from Server`** button on the Kiosk mobile application (Fig. 7). In line with the hybrid of lease and role-based security, and privacy model,only users authorized to share content online and on particular applications, authorized as illustrated in Fig. 7.

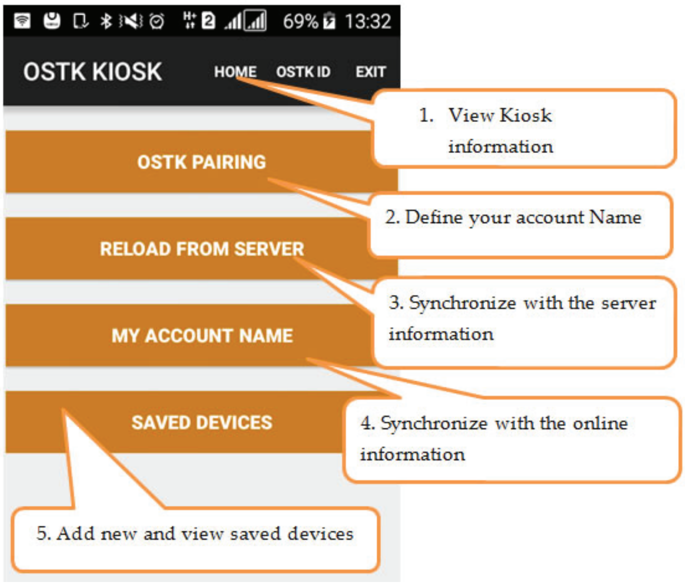
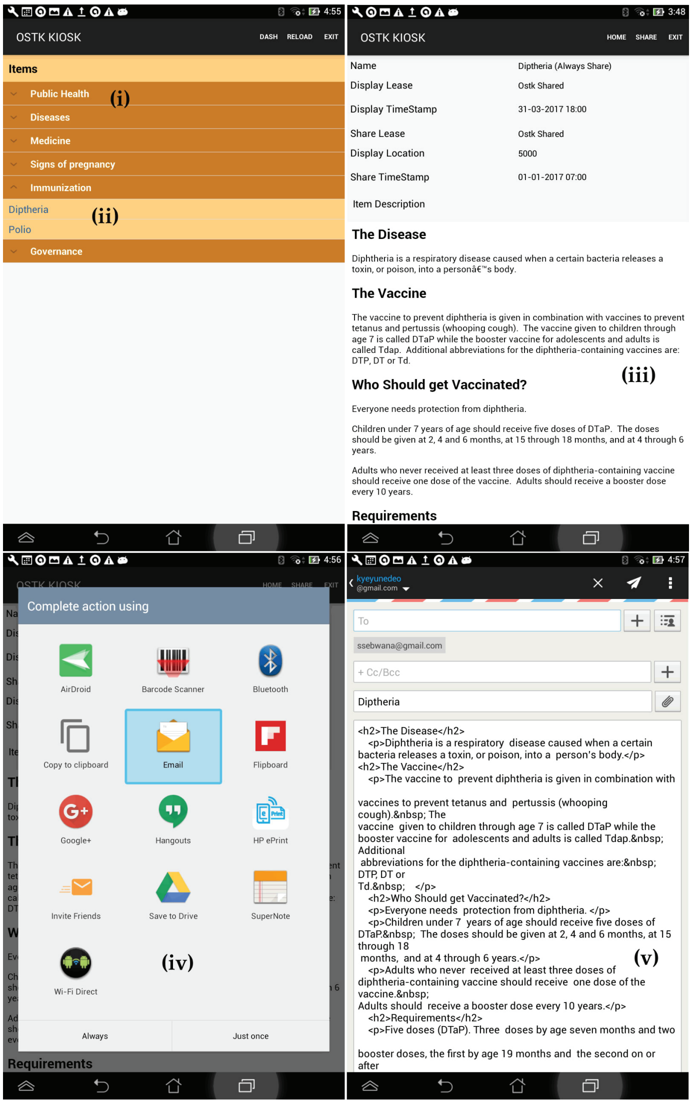

69% 13:32
OSTK KIOSK
HOME
OSTK ID
EXIT
OSTK PAIRING
RELOAD FROM SERVER
MY ACCOUNT NAME
SAVED DEVICES
1. View Kiosk information
2. Define your account Name
3. Synchronize with the server information
4. Synchronize with the online information
5. Add new and view saved devices

Fig. 7. Kiosk mobile synchronization and data view.

Content on the Kiosk mobile application is organized in three layers, namely: content categories (Fig. 8 (i)) ,subcategories (Fig. 8 (ii)) and actual details (Fig. 8 (iii)). Information is grouped according to categories. Upon clicking on the category, the subcategories are displayed and upon clicking on the subcategories, the user is able to view information about a subcategory. This is possible whether there is Internet connection or not. Ability to share content with another user, downloading is determined by the issuer of the lease or the user role. This illustrated in Fig. 8 (i), (ii), and (iii) respectively.

As illustrated in Fig. 8 (iii) a Kiosk user is able to view information that is available on the Kiosk, and can go ahead to `share` it with other Kiosk users and applications that require Internet connectivity to share information. Such applications include social media applications such as Facebook, Twitter and WhatsApp among others. This is illustrated in Fig. 8 (iv).

In scenarios where information is shared on email, upon selection of the mail application, the user is prompted to specify their email address, the content from the Kiosk is transferred to the email editor and the user is able to send it out to recipient(s) as shown in Fig. 8 (v). Once information sharing is carried out, applications such as Gmail, control of such information using the hybrid of lease and role security and privacy model is no longer possible.



OSTK KIOSK

Name	Diptheria (Always Share)
Display Lease	Ostk Shared
Display TimeStamp	31-03-2017 18:00
Share Lease	Ostk Shared
Display Location	5000
Share TimeStamp	01-01-2017 07:00

Item Description

The Disease

Diphtheria is a respiratory disease caused when a certain bacteria releases a toxin, or poison, into a personâ€™s body.

The Vaccine

The vaccine to prevent diphtheria is given in combination with vaccines to prevent tetanus and pertussis (whooping cough). The vaccine given to children through age 7 is called DTaP while the booster vaccine for adolescents and adults is called Tdap. Additional abbreviations for the diphtheria-containing vaccines are: DTP, DT or Td.

Who Should get Vaccinated?

Everyone needs protection from diphtheria.

Children under 7 years of age should receive five doses of DTaP. The doses should be given at 2, 4 and 6 months, at 15 through 18 months, and at 4 through 6 years.

Adults who never received at least three doses of diphtheria-containing vaccine should receive one dose of the vaccine. Adults should receive a booster dose every 10 years.

Requirements

ssebwana@gmail.com

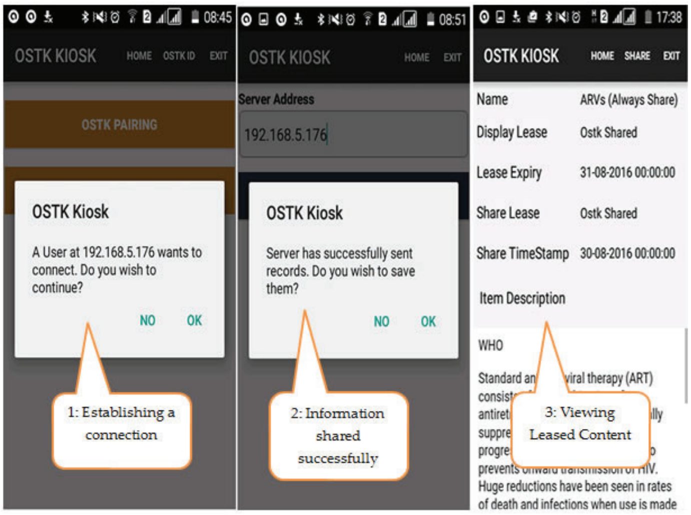
Diptheria

```
<h2>The Disease</h2>
   <p>Diphtheria is a respiratory  disease caused when a certain
bacteria releases a toxin, or poison, into a  person's body.</p>
<h2>The Vaccine</h2>
   <p>The vaccine to  prevent diphtheria is given in combination with

vaccines to prevent tetanus and  pertussis (whooping
cough).&nbsp; The
vaccine  given to children through age 7 is called DTaP while the
booster vaccine for  adolescents and adults is called Tdap.&nbsp;
Additional
 abbreviations for the diphtheria-containing vaccines are:&nbsp;
DTP, DT or
Td.&nbsp;   </p>
   <h2>Who Should get Vaccinated?</h2>
   <p>Everyone needs  protection from diphtheria. </p>
   <p>Children under 7  years of age should receive five doses of
DTaP.&nbsp;  The doses should be given at 2, 4 and 6 months, at 15
through 18
 months,  and at 4 through 6 years.</p>
   <p>Adults who never  received at least three doses of
diphtheria-containing vaccine should receive  one dose of the
vaccine.&nbsp;
Adults should  receive a booster dose every 10 years.</p>
   <h2>Requirements</h2>
   <p>Five doses (DTaP). Three  doses by age seven months and two

booster doses, the first by age 19 months and  the second on or
after
```

Fig. 8. Sharing kiosk information on e-mails.



OSTK Kiosk

A User at 192.168.5.176 wants to connect. Do you wish to continue?

1: Establishing a connection

Server Address

192.168.5.176

OSTK Kiosk

Server has successfully sent records. Do you wish to save them?

2: Information shared successfully

Name	ARVs (Always Share)
Display Lease	Ostk Shared
Lease Expiry	31-08-2016 00:00:00
Share Lease	Ostk Shared
Share TimeStamp	30-08-2016 00:00:00

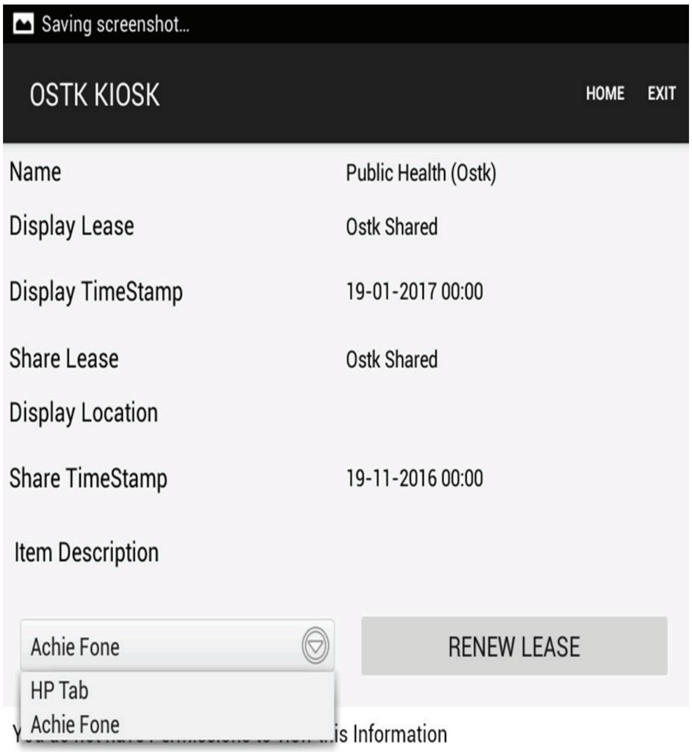
Item Description

WHO

Standard an… viral therapy (ART) consist… …lly antiret… suppre… progre… …o prevents onward transmission of HIV. Huge reductions have been seen in rates of death and infections when use is made

3: Viewing Leased Content

Fig. 9. Leasing content to another device.



Name	Public Health (Ostk)
Display Lease	Ostk Shared
Display TimeStamp	19-01-2017 00:00
Share Lease	Ostk Shared
Display Location	
Share TimeStamp	19-11-2016 00:00

Item Description

Achie Fone

HP Tab

Achie Fone

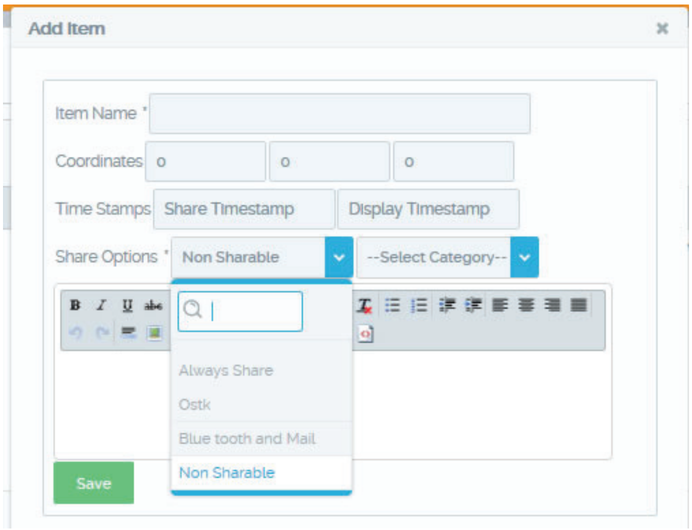
Y… …is Information

Fig. 10. Lease renewal request.

D. Offline File Sharing with Wireless

1) Time-based Content Leasing Using Wireless: Another option of file sharing is carried out by using wireless technology, where the two devices connected to the same network, are able to share files from the Kiosk. If wireless is not turned on,user will receive a prompt to turn on wireless. Once wireless is turned on, the issuer of the content acts as a server and the recipient of the information as a client. This way, the device sharing the information requests for the IP address for the receiving device (Fig. 9). As long as the two or more devices are connected on the same network, they are be able to view their IP addresses using the **`Kiosk ID`** Button. Upon getting it, a user will click the **`Kiosk PAIRING`** button to open the IP address entry and once entered, services are paired and a data sharing session is initiated as illustrated in Fig. 9:

From Fig. 9 the Kiosk Application is leasing content to a Wi−Fi connected device. Depending on the agreed time of the lease, data replication on the client device is confirmed by the toolkit. Towards the end of the lease during which the two parties have agreed to share data, the client device gets a notification message showing that their lease will expire within a short period of grace, such that they can request a renewal as illustrated in Fig. 10: In case a user is authorized to sub-lease content with other users, the user will be in position to sub-lease the same information with others users on the network, in the same way as shown in Figures 9 and 10 respectively. If a user has read-only access, they will not be in position to sub-lease such information with others users on the network, but they may request the issuer of the lease to issue another lease to another interested party.



Add Item ×

Item Name *

Coordinates 0 0 0

Time Stamps Share Timestamp Display Timestamp

Share Options * Non Sharable --Select Category--

Always Share

Ostk

Blue tooth and Mail

Non Sharable

Save

Fig. 11. Condition-based content leasing.

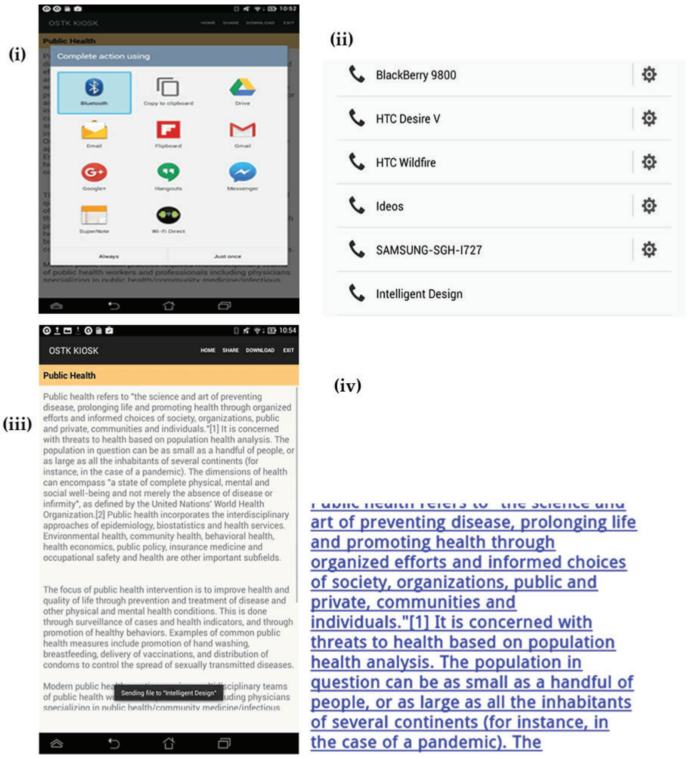
2) Condition-based Content Leasing: In a condition-based lease, time is one of the conditions for content sharing. Other conditions such as location are determined by the issuer of the lease. Users are able to select from among the available conditions before leasing content to users. This is illustrated in Fig. 11.

Unlike with the time-based leasing model, where time determines when the lease will expire. However, with this mode time is considered to be among the conditions for the lease to be active. Other conditions include: location signified by Global Positioning System (GPS) coordinates (World Geodetic System 1984 (WGS84)). Upon violation of any of the other conditions other than time, the content lease is revoked and users no-longer have access to information as illustrated in Fig. 11.

In scenarios where users are allowed to sub-lease content to other connected devices, the condition-based lease bearer will be able to select among the available conditions, and be able to sub-lease information to other users. On expiry of the lease, the subleased recipients will lose access to content. To make renewal requests, they will contact the lease issuer as shown in Fig. 12 . The main content lease in this case overrides the rest of the sub-leases given to other content users. Upon elapse of the main lease, the rest of the sub-leases will no longer be applicable. In scenarios of sensitive information, the lease issuer is able to identify information as read-only and by doing so, content will not be shareable to other users by the person who acquired a condition-based sublease with no share access.

E. Bluetooth File Sharing

The next option of file sharing is carried out by using Bluetooth technology, where the two devices will be able to pair and share files. To make sure that data is compatible will all the devices, it is encoded into HTML5, such that it can be transferred between the two devices as shown in Fig. 12. Should Bluetooth is not enabled, the Kiosk will prompt the user to turn on Bluetooth. Once Bluetooth is selected, the next option is to select the device with which the information is to be shared with (Fig. 12 (ii)).



BlackBerry 9800

HTC Desire V

HTC Wildfire

Ideos

SAMSUNG-SGH-I727

Intelligent Design

Public Health

Public health refers to "the science and art of preventing disease, prolonging life and promoting health through organized efforts and informed choices of society, organizations, public and private, communities and individuals."[1] It is concerned with threats to health based on population health analysis. The population in question can be as small as a handful of people, or as large as all the inhabitants of several continents (for instance, in the case of a pandemic). The dimensions of health can encompass "a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity", as defined by the United Nations' World Health Organization.[2] Public health incorporates the interdisciplinary approaches of epidemiology, biostatistics and health services. Environmental health, community health, behavioral health, health economics, public policy, insurance medicine and occupational safety and health are other important subfields.

The focus of public health intervention is to improve health and quality of life through prevention and treatment of disease and other physical and mental health conditions. This is done through surveillance of cases and health indicators, and through promotion of healthy behaviors. Examples of common public health measures include promotion of hand washing, breastfeeding, delivery of vaccinations, and distribution of condoms to control the spread of sexually transmitted diseases.

Modern public hea Sending file to "Intelligent Design" sciplinary teams of public health w uding physicians specializing in public health/community medicine/infectious

art of preventing disease, prolonging life and promoting health through organized efforts and informed choices of society, organizations, public and private, communities and individuals."[1] It is concerned with threats to health based on population health analysis. The population in question can be as small as a handful of people, or as large as all the inhabitants of several continents (for instance, in the case of a pandemic). The

Fig. 12. Completing action using Bluetooth.

From selected and paired devices, a file is sent to their device as shown in Fig. 12 (iii). During transit, the file is encoded into HTML5 file system to enable HTML viewer file format to read the contents of the file as shown in Fig. 12 (iv). Devices have an HTML viewer which can view information over the Internet or over the network or using Bluetooth established networks. All smartphones are Bluetooth enabled. Utilizing the HTML viewer capability is possible on all devices.

F. Supported Technologies and Devices

Currently the Kiosk application is able to support wireless technologies such as Wi–Fi and Bluetooth. Devices are able to access content when they have the Kiosk client application installed on their devices. The Kiosk device user is able to share information from the Kiosk mobile application directly to the client device using the available wireless technology.

G. Supported File Formats (Content Types)

For offline file sharing, HTML5 content type is the major file format because of its applicability to all devices. For online content other file formats such as Portable Document Format (PDF), HTML5, and image formats that can be transmitted over Bluetooth and Wi–Fi may be used. For compatibility reasons with different phones, document conversion is done depending on the device connecting and receiving content from the Kiosk application.

H. Kiosk Security Support Tools

To enhance the security of the Kiosk, static and dynamic analysis approaches are employed to identify any security vulnerabilities. Chin et al [15] proposed use of static analyzers to investigate security issues that come about as a result of packages imported by the application, message passing through intents, data and control flow analysis, data flow policies via app manifest and content providers. Using tools like DroidScope and ComDroid [12], [13], [14], security flaws in the Kiosk.

Furthermore, we use dynamic analysis tools such as CrowDroid, TaintDroid, DroidScope for data and control flow analysis, emulation-based analysis and investigate logged behavior sequence of the developed toolkit [13]–[16].

We implement permissions for enforcing access rights of an application within the Android system. When installing the kiosk application the user must grant all the permissions requested by the app in order for the application to install successfully. Through permission analysis, the toolkit applies the principle of least privilege to only grant users access to information they need. Leasing out of information to users is based on conditions such as location and time using the hybrid of a lease and a role-based security and privacy model.

V. Related Work

Content distribution technologies in Uganda and many other developing countries have evolved through various media including newspapers, Web 1.0, analog and digital television, analog radio broadcasting, tele-centres and most recently to Social media platforms such as WhatsApp and Facebook [5], [7], [17]. The challenges with the modern sharing social media platforms is that they are designed on the client−server architecture which assume Internet connectivity to access content. Such platforms eliminate many users especially in rural areas where there is sporadic Internet access in many locations. Moreover, modern social media platforms do not implement fine-grain user controlled sharing conditions for sensitive information.

Greenhalgh *et al.* developed an interactive toolkit that provides support for Internet in the rural and *in-situ* settings of the U.K. [4]. The study shows that the need for offline content access is not only required by users and communities situated in developing countries but for communities in low−resource settings in both developed and developing countries. The Kiosk was an extension of a previous content authoring and sharing open source system, called PlaceBooks that was specifically developed for rural settings [19]. This work investigates novel security software abstractions that be used to enhance security of such previous Kiosk approaches that did not consider context and security requirements for content sharing.

PirateBox is a Do It Yourself (DIY) file sharing and messaging platform for offline file-sharing and communications over a local area network [21]. It is built with free software and off-the-shelf hardware. Target users of PirateBox are people with advanced Linux skills and thus requires additional development effort to make it usable for end-user devices with user-defined sharing constraints. The project development was discontinued, however, the technology is still available although not being actively maintained. LibraryBox is a related open source platform that is based on inexpensive hardware for sharing and distributing vital information for education, healthcare and other purposes [20]. Like PirateBox, it also requires technical personnel to configure and setup. Therefore this is a limitation to ordinary users who do not have the skills to distribute content across the network.

VI. Conclusion and Future Work

This paper presented the design and implementation of a secure context-aware sharing Kiosk. It identifies the key requirements that must be satisfied by such an implementation: (1) spontaneous Kiosk discovery (2) user specified content sharing conditions and (3) transitive and propagated security and privacy mechanism. Consequently the paper proposed a context-aware content sharing Kiosk that supports the above requirements through key properties: (1) online and offline support, (2) discovery of client Kiosks and device connections, (3) and content replication across multiple devices. This is further enhanced with a hybrid of lease-based and role-based security models resulting into a secure context-aware content sharing Kiosk. The model is validated by implementing a proof-of-concept, case study, of content sharing in a hospital setting. The secure Kiosk was designed to ensure that information is disseminated over a wide range of different people with interest in information sharing and services in an effective low cost manner. Other than hospitals, results show that it can be re-used in other settings with minimal customization. With the advantages of privacy, online and offline support, and if the kiosk model is adopted by people living in remote regions, it will enable them to share information with other users as well as enjoy the support of data replication on local mobile devices.

As future work, this model can be considered in different scenarios and consideration can be given to develop more contexts beyond just time and location. The infrastructure described in this paper provides the software technology to implement more sophisticated contexts, for example, lightweight content sharing strategies based on the network signal strength or the risk profile of the intended recipient.

References

[1] GSM Association,(2019) *The Mobile Economy Sub-Saharan africa 2018*, accessed on (March 28, 2020), https://www.gsma.com/subsaharanafrica/resources/the-mobile-economy-sub-saharan-africa-2019

[2] GSM Association,(2019) *The State of Mobile Internet Connectovity 2019*, accessed on (March 28, 2020), https://www.gsma.com/mobileeconomy/sub-saharan-africa/

[3] Minn Watts marketing groups, (2018), *Africa Internet Usage, 2018 Population Stats and Facebook Subscribers*, https://www.Internetworldstats.com/stats1.htm

[4] Greenhalgh, C., Chamberlain, A., Davies, M., Glover, K., Valchovska, S., Crabtree, A. (2014) *'Displaying Locality: Connecting with Customers and Visitors In−Situ via their mobile Devices'*,The University of Nottingham School,of Computer Science Wollaton Rd, Nottingham, UK

[5] John B. Rose *"Multipurpose Community Telecentres: In support of People−Centred Development (Uganda) "*, UNESCO, Uganda, 1999.

[6] David Darts and Mathias Strubel (2014,November 26) [online] Available http://piratebox.cc

[7] Sulait Tumwine; Charles Omagor and Agaba Gershom *Newspaper copy sales and the performance of the print media in Uganda*, International Journal of Management and Business Studies ISSN: 2167−0439 Vol. 4 (2), pp. 138−150, February, 2014. Available online at http://internationalscholarsjournals.org International Scholars Journals

[8] Guy berger *Challenges And Perspectives Of Digital Migration For African Media*(2016,May 27) The Panos Institute west Africa.

[9] Ninghui Li et alA *Critique of the ANSI Standard on Role-based Access Control*, CERIAS and Department of Computer Science Purdue University

[10] Ravi et al , *Role−Based Access Control Models* (2016,Jul 27), IEEE Computer, Volume 29,Number 2,pages38−47.

[11] Jinglan Zhang et al, *Using mobile Phones to Improve Offline Access to Online Information: Distributed Content Delivery, Andrew Trotman Department of Computer Science*, University of Otago Dunedin, New Zealand

[12] Cary G. Gray and David R. Cheriton, *Leases: An Efficient Fault-Tolerant Mechanism for Distributed File Cache Consistency*, Computer Science Department, Stanford University, (October 2016).

[13] Iker Burguera and Urko Zurutuza, Simin Nadjm-Tehrani,*Crowdroid: Behavior-Based Malware Detection System for Android*, Electronics and Computing Department, Mondragon University, 20500 Mondragon, Spain, Dept. of Computer and Information Science, Linköping University SE-581 83 Linköping, Sweden,(October 2016).

[14] William Enck et al , *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, The Pennsylvania State University,Duke University, Inter Labs,(October 2016).

[15] Erika Chin et al, *Analyzing Inter-Application Communication in Android*, University of California, Berkeley Berkeley, CA, USA, (October 2016).

[16] Lok Kwong Yan and Heng Yin, *DroidScope: Seamlessly Reconstructing the OS and Dalvik Semantic Views for Dynamic Android Malware Analysis*, Syracuse University,Syracuse, New York, USA, Air Force Research laboratory, Rome, New York, USA(October 2016).

[17] Nath, Keshab et al, *Web 1.0 to Web 3.0 - Evolution of the Web and its various challenges. ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology*. 86-89. 10.1109/ICROIT.2014.6798297, 2014.

[18] Nyanchama, Matunda and Osborn, Sylvia L.. *Access Rights Administration in Role-Based Security Systems*, Paper presented at the meeting of the Proceedings of the IFIP WG11.3 Working Conference on Database Security VII, Amsterdam, The Netherlands, The Netherlands, 1994.

[19] A. Crabtree et al. *Doing innovation in the wild.* In Proceedings of the Biannual Conference of the Italian Chapter of SIGCHI (CHItaly '13). ACM, New York, USA. DOI=10.1145/2499149.2499150, 2013.

[20] *LibraryBox*. http://librarybox.us/. Accessed on March 30, 2020.

[21] *PirateBox*. https://piratebox.cc/. Accessed on March 30, 2020.

[22] Beresnevichiene, Yolanta, *A Role and Context Based Security Model. Technical Report, University of Cambridge, UK*, 2003.

Achilley Kiwanuka Ssebwana holds an MSc. and BSc. Computer Science from Makerere University. He has over 6 years experience in implementing web-based systems for large organizations including local and international non governmental organizations as well as Government. Over time he has engaged in different aspects of software engineering across the software development life-cycle. He is passionate about research and is a prospective PhD candidate.

Engineer Bainomugisha is an Associate Professor of Computer Science at Makerere University, Uganda. His research focuses on Computer Science-driven solutions to the prevailing world challenges. He is also passionate about contributing to quality Computer Science education that is of sufficient breadth and depth, practical and fast enough. He currently leads several innovative and research initiatives that aim to create and apply computational methods and tools that can improve the quality of life especially in the developing world setting. His research interests distributed systems, Internet of Things, Context-aware systems, programming language engineering, software security, cloud computing, and data science.

Previously he investigated and developed programming languages and software tools to help programmers easily write highly adaptive and distributed mobile software without worrying about low-level concerns. His research in this area helped create `iScheme` and `Flute` programming languages.