ACTA SCIENTIFIC COMPUTER SCIENCES

Volume 2 Issue 7 July 2020

Research Article

The Use of Internet of Things Crime Collector Model in Curbing Crime

Gibson Kimutai[1]* and Njeri Kiaritha[2]

[1]*Department of Mathematics, Physics and Computing, Moi University, Kenya*

[2]*Department of Educational Psychology, Moi University, Kenya*

***Corresponding Author:** Gibson Kimutai, Department of Mathematics, Physics and Computing, Moi University, Kenya.

Received: June 27, 2020

Published: July 30, 2020

Abstract

Crime is evolving across the world in the modern technological 21st century era in terms of prevalence and technicality involved. Thus, prevention of crimes is complicated with the advance in technology for the criminals. It therefore becomes paramount that the technological security measures should be put in place to counteract this criminal technological advancement. This paper therefore, explores the development of the Internet of Things (IoT) based crime collector model with an aim to redefining regional, national and international security measures.

Keywords: Model; Crime; Internet of Things (IoT)

Introduction

Trends in crime throughout the world are frequently evolving, giving law enforcement the difficult task of remaining vigilant. With advancements in global technology comes the emergence of criminal activity. In Kenya, the major problems include: Terrorism, maritime piracy, human/drugs/arms trafficking, theft, bribery and cybercrime among others. The goal of this research was to develop a Crime collector model that runs on a mobile platform which allows the members of the Kenya Defense Force to collect crimes and evidence for prosecution from the crime scene and send them to a central database on real-time.

The term "Internet of Things" (IoT) is a term first coined by a British visionary, Kevin Ashton, back in 1999 [1] As the phrase "Internet of Things" reveals, the IoT paradigm will provide a technological universe, in which many physical objects or "Things", such as sensors, everyday tools and equipment enhanced by computing power and networking capabilities will be able to play a role, either as single units or as a distributed collaborating swarm of heterogeneous devices [2].

Research Methodology

Document analysis

Choosing 'document analysis' as research method can have several attractions: it helps the researcher to reach "inaccessible persons or subjects" [3]. Many documents in "public domain" are prepared by professionals and contain very valuable information and insights [4]. And documentary sources have the highest level of accessibility (Denscombe, 2007:230) and are very cost effective [3].

In this research, document analysis was chosen as it gives an opportunity to analyse information gathered by group of professionals, which is almost impossible to get by any other research method and moreover, these documents are very easy to access. For example, reports prepared by different international organizations, are based on a long-term studies, which is impossible to conduct by one researcher. Therefore, these types of documents were very useful for this thesis and most of them were available through official web-pages of specific organizations and also journals. Moreover, this type of documents can be a very reliable source of information, as it is prepared for state or international purposes.

Prototyping

The prototype presented in this research is a general-purpose crime collector application software for use in the defence ministry. Accordingly, data gathering for this study was focused on the modern researches and developments in the field of defence. Therefore, no interviews or surveys on companies and company personnel were conducted during the course of the study, as they were not necessary.

Design science

Research in computing are concerned with people, organizations and technology [5]. Researches try to understand problems related to developing and successfully implementing models in organizations [5]. Development of models are often performed to help an organization and people to increase the efficiency and effectiveness [5]. People, existing systems, development methodologies, and the capabilities of the information system are factors that

affect this process [5]. This is the paradigm that was used in this research to maintain control over the development, and research results.

Development process

For the implementation of the model, figure 1 shows the stages that was followed. The first step was on project planning where project planning, needs assessment and scope definition. The next phase was on design where database design and application design.

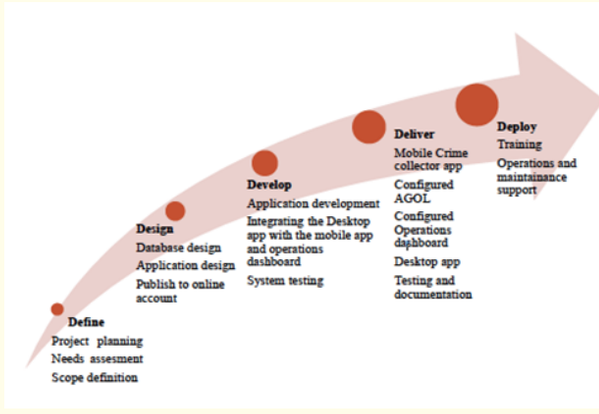

Figure 1: Development process.

The third phase was on development. In this phase, application development, integration desktop and system testing. The final phases were on delivery and deployment.

Results and Discussion

Figure 2 shows the architecture of the developed model. As it can be seen from the figure, the application runs in desktop computer and also mobile phones. It can also be seen that the server is hosted remotely and the delivers communicated via LORA network.

Figure 2: Development process.

The mobile application component was used to collect the location and particulars of the crime. The application used phone's GPS to capture location and pre-templated crimes form to capture all the details associated with the crime, including the pictorial evidence. The collected data was transmitted to the online portal where it could be visualized on a map and at the same time the real-time statistics of the crimes being collected were seen on the operations dashboard in the offices. Even when offline, crime could still be collected and later synchronized them in the office on a WIFI. The application runs on both iPhone and android platforms as shown in figure 3.

Figure 3: Platforms the application can run on.

The second component of the solution was on an online portal that housed the collected crimes. This provided an interactive platform that was used to visualize the spatial distribution of the crimes on the map.

It also provided a platform for doing GIS analysis on the collected data. The supported analysis that could be done here includes: proximity analysis, Data enrichment with demographics data, analysing patterns, Data summary and generation of drive times to the scene of crime among others.

The crime analysis done here focused on mapping incidents, identifying hot spots where the most crime occurs and analysing the spatial relationships of targets and these hot spots. Apart from the spatial analysis our solution also supported statistical analysis to view crime data as Reports, Graphs and Charts based on Category.

The Crime-related data at the portal could also be enriched with other datasets like demographics, economic classes and analysed with other external data sources to reveal the trends and behaviour of crimes at different locations.

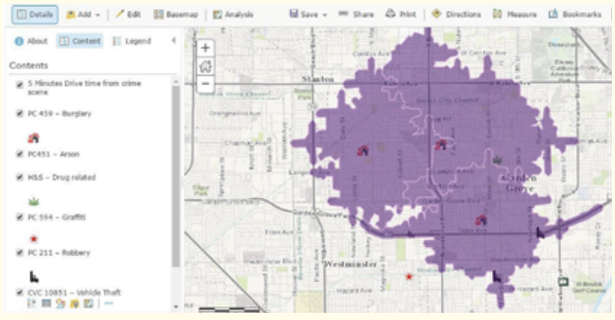

Figure 4: Visualisation of crime.

Crime incident data could be geocoded (assigning an x and y coordinate to an address so it can be placed on a map) by using either street centrelines (every address within a block is encoded) or parcels. All the crime data collected via mobile phone by the Patrol Officers were synchronized here and will be seen by the other officers in the office through a web browser.

Model security

Crime Collector is a secured, reliable geographic information system (GIS) delivered using the software - as-a-service (SaaS) model. With the developed model, the admin had privileges of assigning duties and roles to other members of the security team who could access the content. Additionally, the content in the portal was only available to security team unless they decide to share with the public. Additional security features include hosting the Crime Collector within Kenya Defence Force IT. Other security means included: methods of Cross site Request Forgery, protection of SQL injection.

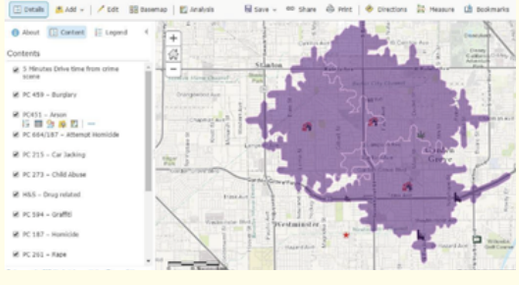

Figure 5: Security of the model.

Conclusion

In this paper, development of an IoT based crime collector model is shown. The model developed was tested and its performance was promising. In the future, the model can be improved by incorporating notifications through use of push notifications and Short Messaging Service (SMS). The model can also be advanced to cover for crime predictions.

Acknowledgement

The authors wish to thank the GIS Laboratory technicians of Moi University for running the experiments on the model alongside the authors. Author GK also wishes to appreciate author N.K for all the time and sacrifice in reviewing the paper and her wise suggestions.

Bibliography

1. BC Chifor., *et al*. "A security authorization scheme for smart home Internet of Things devices". *Future Generation Computer Systems* 86 (2018): 740-749.

2. A Tzounis., *et al*. "Internet of Things in agriculture, recent advances and future challenges". *Biosystems Engineering* 164 (2017): 31-48.

3. R Kumar. "Research Methodology: A Step-by-Step Guide for Beginners, Fourth edition". Thousand Oaks, CA: SAGE Publications Ltd (2014).

4. CR Kothari. "Research Methodology: Methods and Techniques, 2nd edition". New Age International Pvt Ltd Publishers (2013).

5. A Dresch., *et al*. "Design Science Research: A Method for Science and Technology Advancement". Springer International Publishing (2015).