MAPLE TREE
PUBLISHING HOUSE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY
TECHNOVATION (IRJMT)

http://www.mapletreejournals.com/index.php/IRJMT
Received 21 August 2019 ISSN 2582-1040
Accepted 15 September 2019 2019; 1(6); 152-155
Published online 02 November 2019

Predicting Digital Geotechnical Forensic Investigation using Internet of Things (IoT)

D. Sivakumar[1*], E. Ravi[2]

[1] Assistant Professor Department of Civil Engineering, K.S.Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India.
[2] Professor & Head Department of Civil Engineering, VCET, Erode Tamil Nadu, India.

**Corresponding author E-Mail ID: dsivakumar.kumar@gmail.com,*

Doi: https://doi.org/10.34256/irjmtcon19

ABSTRACT

Digital Forensic Investigations is explained as are sponse to an event that has already occurred in relation to information which is highly classified or is of prime importance to a criminal incident. Forensics Challenges in IoT Environments IoT would soon pervade all aspects of our life from managing our home temperature to thinking cars and smart management of the cities. The application of professional engineering principles and methodologies to investigating failures and incidents, usually to determine causation. Normally, it involves preparing a report of findings, which may form the basis for testimony in legal proceedings as an expert witness. A forensic engineer may serve as an engineering consultant to members of the legal profession and as an expert witness in courts of law, arbitration proceedings and administrative adjudication proceedings. Forensic engineering is a part of professional engineering practice that may cover all disciplines of engineering. It is a specialized set of skills that can include multidisciplinary training in failure analysis, simulation, safety, accelerated life testing and statistical analysis, as well as knowledge of the specific engineering field.

Keywords: Internet of things, Investigation and documents.

1. INTRODUCTION

The main research challenge in Internet of things (IoT) for the forensic investigators is based size of the objects of forensic interest, relevancy, blurry network boundaries and edgeless networks, especially on method for conducting the investigation. In fact, many engineers, architects, owners, and other associated parties do not appreciate or understand the geo forensic process when a structure may be damaged because of inadequate ground conditions. When failure of any structural element occurs, many factors are often responsible for it which includes: (i) improper foundation investigation, (ii) poor building design, (iii) poor materials and (iv) in experience of the handler as the case maybe. In addition to determining the specific cause of the substantive errors that specifically caused the damage and recommending repairs, it may be important to assess responsible parties leading to the damage. Three different Stage of inspection are needed namely design stage, construction-inspection stage and forensic investigation stage.

INFORMATION GATHERING

Engineers are reminded that information in addition to the following suggestions can be consulted regarding the collection and storage of all manner of physical evidence.

Non-destructive information gathering

Observations

It is advisable to take detailed notes of the observed conditions, either as physical notes or audio recordings. In the event of audio recordings, it is preferable to have these transcribed as soon as possible and the accuracy of the transcription verified by the person who made the observations.

Photography and Videography

To the extent possible, all relevant aspects should be photographed and or videotaped. It should be recognized, however, that not all observations can be appropriately photographed or videotaped. Use standard formats and compact size to enable sharing of data. When selecting the storage medium, it is useful to consider both reverse compatibility and forward compatibility issues.

Measurements

Useful measurements that do not interfere with the evidence should be taken.

Other information or documents

It is advisable to access and consider any other relevant information or documents. Some examples are: original equipment manufacturer (OEM) information, design documents (drawings, specifications), operating data, inspection records, maintenance procedures, literature review, and modifications/changes made.

Destructive information gathering

Evidence collection

Chain of custody: A chain of custody should be recorded with the evidence, and engineers have an obligation to keep evidence that is collected. Engineers should be knowledgeable of standards regarding evidence collection.

Field simulations/In situ testing/laboratory testing

Standard procedures: Generally, these may be difficult to complete outside of a laboratory environment. If such testing is undertaken, consideration should be given to a given laboratory’s ability to complete the testing. Also, the suitability of a test should be considered, including the influence of the collection method on the test results.

SOFTWARE ACCEPTANCE TEST

a) Back-end Test

Back end test is the server side test of our device. Back end development is very critical because it is what makes the front end possible. Back end questions consist of where all the data will be stored and how our software team will handle the problems with the database. One way to test the back end side was to connect multiple devices to the cloud and store and process data for long times.

b) Front-end Test

Front end development is the client side, so the user can see the data readings processed by the web application and interact with the device directly. The most important acceptance test in the front end site is the quality of data visualization and user interface. The user is able to login to our web app either with his Face book or email.

SECURITY ISSUES IN STORING AND PROCESSING DATA

Cloud computing is a critical elements for smart cities that provides a reliable and resilient infrastructure for users to storing, accessing, and processing data on remote servers. There are many other advantages of this approach such as maintenance cost and the ability to analyze a very large volume of data in real time for making decisions

TECHNICAL RESPONSIBILITY

There are some disciplines in forensic engineering where engineers are asked to assess the technical responsibility of the parties that were potentially involved in decisions leading to the failure. An investigating engineer should make the assessment by comparing the work performed by each party with: the regulatory or statutory requirements; the standard of practice normally expected to carry out the work; and whether the problem causing the failure was common knowledge in the relevant industry. It is not the engineer's responsibility to assess the liability of the parties; this is the role of the court.

EVIDENCE

An investigating engineer must be careful to identify what evidence is independently obtained (i.e. physical or digital information) and what evidence is subjectively obtained (i.e. circumstances reported by witnesses). Both the frailty of human memory and the influence of bias among witnesses can render subjectively obtained information of limited value.

GEOTECHNICAL REPORTING DOCUMENTS

A number of different documents are generated from investigations for site characterization. The most common of these include field investigation logs, geotechnical data reports, and geotechnical design reports. The following sections provide general descriptions of different geotechnical reporting documents for the purpose of understanding common products that result from site characterization. More detailed description of the different reporting documents, including recommendations for specific content.

Field investigation logs, The most common products from investigations for site characterization are field investigation logs that may include boring logs, test pit logs, in situ testing (e.g., CPT, DMT, VST, etc.) logs, groundwater monitoring logs, and geophysical survey reports. Geotechnical data reports are from geotechnical investigations commonly include some form of "geotechnical data report", which generally includes a description of the investigations performed, field investigation logs, and results of laboratory and field test measurements. Geotechnical data reports, In contrast with geotechnical data reports, "geotechnical design reports" generally include much more than just factual data. Geotechnical design reports usually include relatively detailed descriptions of a characterized site along with additional content such as descriptions of analysis and design methods, results from design analyses, interpretation of analysis results, and recommendations for design and construction. Geotechnical design reports often include descriptions of the soil and/or rock encountered, interpretations of stratigraphy, descriptions of observed and anticipated groundwater conditions, descriptions of geotechnical hazards and potential risks that may be introduced by those hazards, and interpretations of relevant geotechnical design parameters. Geotechnical Baseline Reports (GBR) is The general content of a GBR is often similar to the site characterization content from geotechnical design reports in the sense that they include complete interpretations of ground conditions. The principal difference is that a GBR establishes a “baseline” for ground conditions that is accepted by all parties for contractual purposes prior to execution of construction. GBR, and the interpretations included therein, are therefore contractually binding and serve as the basis for claims and change orders associated with ground conditions.

REFERENCES

1. Abdmeziem, R. &Tandjaoui, D., 2014. Internet of Things: Concept, Building blocks, Applications and Challenges.
2. Atamli, A.W. & Martin, A., 2014.Threat-Based Security Analysis for the Internet of Things.*2014 InternationalWorkshop on Secure Internet of Things*, pp.35–43.
3. Attwood, A. et al., 2011. SCCIR: Smart cities critical infrastructure response framework. In *Proceedings -4th International Conference on Developments ineSystems Engineering, DeSE 2011*. pp. 460–464.
4. Carrier, B. &Spafford, E., 2004.An event-based digital forensic investigation framework.*Digital forensicresearch workshop*, pp.1–12.
5. Garfinkel, S.L., 2010. Digital forensics research: The next 10 years. *Digital Investigation*, 7(SUPPL.).
6. Giova, G., 2011. Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems.*International Journal of Computer Science andNetwork Security*, 11(1), pp.1–9.
7. Islam, S.M.R. et al., 2015. The Internet of Things for Health Care: A Comprehensive Survey. *Access, IEEE*, 3, pp.678–708.
8. Palmer, G., 2001. A Road Map for Digital Forensic Research.*Proceedings of the 2001 Digital ForensicsResearch Workshop (DFRWS 2004)*, pp.1–42.
9. Selamat, S.R., Yusof, R. & Sahib, S., 2008.Mapping Process of Digital Forensic Investigation Framework.*Journal of Computer Science*, 8(10), pp.163–169.
10. VanansiusBaryamureeba&Tushabe, F., 2004.Digital Forensic Research Workshop.In *Digital ForensicResearch Workshop DFRWS 2004*.

Conflict of Interest

None of the authors have any conflicts of interest to declare.

About the License