http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 8 Issue 1, January. 2019, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

GIRI
Global IT Research Institute

Journal Editorial Board

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

- **Step 1. Journal Full Paper Submission**

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

- **Step 2. Full Paper Review**

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

- **Step 3. Acceptance Notification**

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

- **Step 4. Payment Registration**

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

- **Step 5. Camera Ready Form (CRF) Manuscripts Submission**

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

➢ How to submit your Journal paper and check the progress?

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Volume. 8 Issue. 1

A Triage Triangle Strategy for Law Enforcement to Reduce Digital Forensic Backlogs

Da-Yu Kao*, Ni-Chen Wu*, Fuching Tsai**

*Department of Information Management, Central Police University, Taiwan

**Department of Criminal Investigation, Central Police University, Taiwan

dayukao@gmail.com, niniwu841223@gmail.com, fctsai@mail.cpu.edu.tw

***Abstract*—The explosive growth of computer technologies creates many electronic data and produces much digital evidence of people's lives. As technology has improved, the volume of data for cybercrime investigation keeps growing at unprecedented rates and creating a quandary for Law Enforcement Agencies (LEAs). This study discusses the rise of digital evidence and the triage needs in digital forensic processing. It requires the sincere examination of all available data volumes at the scene or in the lab to present digital evidence in a court of law. In order to maintain the relevance, reliability, and sufficiency of digital evidence, investigators must establish a process model that can provide a quick response at the scene. This study proposes the novel triage triangle strategy of digital forensic components and illustrates TEAR phases from the viewpoint of THOR dimensions to describe the proper practices for identifying, collecting, acquiring, and preserving the digital data. It facilitates the efficiency and effectiveness of reducing digital forensic backlogs for LEAs.**

***Keyword*—Digital Evidence, Digital Triage Forensics, THOR dimensions, Data Network, Law Enforcement**

I. Introduction

The digital forensic process commences with any piece of digital media. Every action taken has to adhere to the legitimacy rules so that the obtained digital evidence could be presented in the court. When investigators evaluate evidence, its relevance, reliability, and sufficiency are of grave importance both in the investigative and probative stages of a case. Digital forensics addresses the collection, examination, analysis, and presentation of evidence located on computers, cell phones, or networks. It brings the evidentiary fruits of electronic data for many types of decisions, such as divorce, child custody, contract resolution, or criminal judgments [9]. The digital forensic process is very time-consuming because it requires the examination of available data volumes from the scene.

Cybercrime is a growing problem year after year. The ability of Law Enforcement Agencies (LEAs) to investigate and prosecute criminals for these crimes still leaves much to be desired on the process, tools, or training. There is a lack of awareness of available training courses or educational materials on cybercrime investigation and digital forensics, especially for LEAs [5]. This study provided a digital evidence assessment in investigating crimes. Conducting digital forensics on the original evidence sources should be avoided if possible since the examination on forensic copies or images maintains the data integrity of digital evidence. However, evidence triage provides valuable quick intelligence without subjecting digital evidence to a full examination and determines if a media is worth to be examined under significant time constraints [11]. This quick intelligence can be used at the scene to guide the search and seizure, and in the lab to determine if a media is worth to be examined. With the development of information technology, LEAs need to improve the speed and quality of cybercrime investigations. Performing forensic triage can be required to quickly and efficiently review several target systems. This study tries to propose a practical strategy to mitigate the enormous backlog of cases for law enforcement.

The structure of this study is organized as follows. Section 2 provides a review of digital evidence and forensic investigations in LEAs. The proposed triage triangle strategy of digital forensic components described in Section 3. Section 4 demonstrates the discussions and analyses. Finally, the last section concludes the study.

II. Reviews

A. Digital Evidence

Most of our daily activities and interactions are recorded in electronic devices. Digital devices are everywhere and help people communicate locally and globally. Computers, cell

Manuscript received Dec. 27, 2017. This work was a follow-up of the invited journal to the accepted & presented paper of the 21st Conference on Advanced Communication Technology (ICACT2019), and this research was partially sponsored by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109) and the Ministry of Science and Technology of the Republic of China under the Grants MOST 107-2221-E-015-002..

Da-Yu Kao is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dayukao@gmail.com).

Ni-Chen Wu is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dorislovesnoopy@gmail.com).

Fuching Tsai is with the Department of Criminal Investigation, Central Police University, Taoyuan 333, Taiwan (Corresponding Author phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: fctsai@mail.cpu.edu.tw).

phones, and the Internet are valuable sources for digital evidence. Digital data is always stored in various locations across a system or physical location. Any piece of information technology can be used criminally. Digital evidence is defined as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device [3]. Digital evidence can help answer any questions in an investigation ranging from the whereabouts of a victim at a given time to the state of mind of the criminal. Answering these questions requires some degree of crime reconstruction, including a combination of temporal, functional, and relational analysis of available evidence [3]. This evidence can be acquired when electronic devices are seized and secured for examination. When investigators attempt to retrieve digital data, critical evidence in cybercrime investigations must be extracted from that digital domain. Digital evidence is [2]:

1) *Fragile:* It can be altered, damaged, or destroyed with little effort.

2) *International:* It can cross jurisdictional borders instantly and effortlessly.

3) *Latent:* It is hidden like fingerprints or DNA evidence.

4) *Volatile:* It is volatile and sensitive.

B. Forensic Investigations in LEAs

Cybercrimes often raise new challenges for the LEAs. Criminals were keeping up with the new technology while law enforcement lagged. The knowledge, skills, and abilities of investigators in the field of digital evidence are a necessary step in successfully pursuing cybercriminals. Investigators must have the capability to analyze any evidence retrieved in investigating cybercrimes [5]. Crime scene investigation in LEAs includes case analysis, report writing, and legal presentation [12].

1) Case Analysis

Different experts should independently report the case analysis.

2) Report Writing

Different reports from various experts involved in a case are called to give evidence explanations at the courtroom since the reports only have validity after being confirmed in court.

3) Legal Presentation

Legal presentation in court is to give evidence explaining the relevance and the implications of their actions. Evidence is specific to his/her specialty so that forensic experts can be cross-examined and present their cases objectively without fear, uncertainty, or doubt.

III. THE PROPOSED TRIAGE TRIANGLE STRATEGY OF DIGITAL FORENSIC COMPONENTS

Cyberspace introduces a wide range of new vulnerabilities criminals can use to take advantage of their victims. As new crimes emerge from the misuse of cyberspace, LEAs must change and develop their strategies to address previously unknown issues [8]. The proposed triage triangle strategy of digital forensic components is divided into three categories (Fig. 1): principles, forensics, and governance. This strategy helps LEAs deal with reducing digital forensic backlogs.

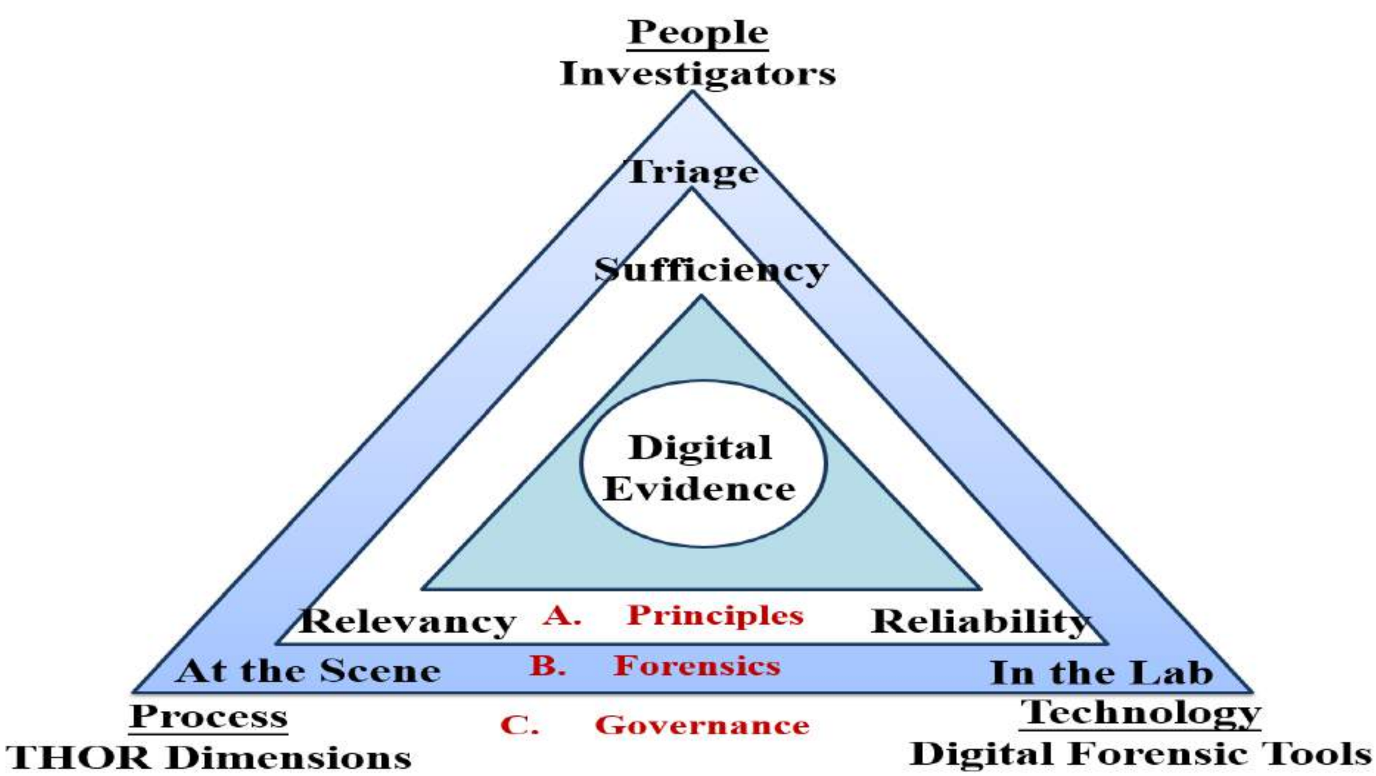

Fig. 1. Triangle strategy of digital forensics process

A. Principles

Digital forensics is a branch of forensic science to encompass the investigation in electronic devices. It focuses on the recovery and analysis of raw data in digital devices. Investigators face numerous challenges, technical difficulties, or legal issues surrounding cybercrime investigations. It is essential not to overlook or minimize the vast amount of information stored in a computer, the nature of volatile memory, and a lack of sufficient strategies. The required principles for digital evidence handling should be satisfied as follows [6]:

1) Sufficiency

Investigators should be able to decide how much and which material to collect or acquire at the scene. They need to exhaust different methods, tools, and practices to identify, extract, and convert data to unequivocal evidence. There must be sufficient evidence to make the investigation convincing. They should have taken into consideration that enough material has been gathered to prove somethings.

2) Relevance

The data value can assist the investigation of the particular incident. Investigators should be able to describe the followed procedures form auditing records and explain how the decision to collect each data was made. The relevance of pertinent data affects the weight and usefulness of the evidence. Time, efforts, and cost spent in an investigation could be well controlled if investigators know what should be collected during the investigation. Then they can demonstrate that the acquired material is relevant to the investigation.

3) Reliability

Data extracting is not merely copying of data. All processes used in handling potential digital evidence should be auditable. Chain of custody should be preserved during collecting, examining, analyzing, preserving, and transporting of data. If the evidence cannot be repudiated and rebutted, then the digital evidence would be reliable and admissible in a court of law.

B. Forensics

Digital forensics deals with how data is gathered, investigated, recovered, found, analyzed, and stored in electronic devices in a court of law. Trace evidence in the computer environment falls within the realm of digital forensics. When people interact with people, places, and objects in the digital realm, these virtual traces will be kept as deleted file fragments, activity logs, document metadata, or email headers. They may be deemed to be of evidence value in identifying the origins of the parties involved in a criminal case. In Fig. 1, there are three forensic elements in our proposed triage triangle strategy. The detailed description is demonstrated in the following:

1) Triage

Most digital evidence investigation is completed at the scene promptly. Increasing cases and computers need to be analyzed effectively and efficiently. Specific investigations with a high level of technical difficulty are likely to be conducted in the lab [5]. As the data loads increase exponentially, triage has become an increasingly important part of digital forensics. Triage aims to identify the most relevant data as quickly as possible. It helps investigate in a limited time. Some digital forensic tools meet this need by extracting the recently changed files from a computer.

2) At the Scene

Investigators to any criminal complaint must ask the pressing questions at the very beginning and handle any relevant digital evidence appropriately at the scene. That will directly impact the effectiveness of an investigation and the admissibility of that evidence in court [5]. When first responders arrive at the scene, they will look for all relevant evidence, explore some questions, and find the follow-up answers on whom, which, what, when, where, and how. Everything can be evidential to support or refute something.

3) In the Lab

Due to the limitations of technology or knowledge, some evidence cannot be identified at the scene and must be brought back to the laboratory for further examination.

C. Governance

There is always a continuous need for investigators to utilize tools in the effective handling of digital evidence and ensure a timely, valid, and accurate presentation to a court. These abilities of investigators may affect the tools used and the understanding of any evidence retrieved to ensure that the evidence is admissible in court [5]. This study proposes a minimum requirement for compliance with digital forensic processes.

1) People: Investigators

The dependence on using digital forensic tools or techniques brings about the detection and recovery of hidden data in LEAs. The trend of digital forensics implies the imperative need for governance on digital forensics. Investigators should persistently upgrade their skills, tools, and know-how to keep pace with changing technology. They should know how to extract the volatile evidence, use appropriate tools, and perform live investigative response [7]. It is no longer able to unplug a computer and expand the backlog as a mountain in the lab.

2) Process: THOR Dimensions

Investigators need proper processes to identify, collect, acquire, and preserve digital data. The goal of the CAMINO (Comprehensive Approach to cyber roadMap coordINation and develOpment) project was to develop a comprehensive cybercrime and cyber terrorism research agenda. THOR dimensions are the foundation of the CAMINO roadmap and address the following aspects [4]:

a) *Technical*-related to technology, technological approaches, and solutions.

b) *Human*-related to human factors, behavioral aspects, privacy issues, as well as raising awareness and knowledge of society.

c) *Organizational*-related to processes, procedures, and policies within organizations, as well as cooperation between organizations.

d) *Regulatory*-related to law provisioning, standardization, and forensics.

3) Technology: Digital Forensics Tools

The ability to use appropriate digital forensic techniques and tools varies by agency and geographic location. These techniques and tools are not sufficient to keep pace with changes in digital devices. Proprietary sources for the software or hardware generally limit the particular discipline of purchased training courses in the digital forensics process. The need for freeware or open-source tools within digital forensics across all LEAs is critical for the nature of the discipline in legal proceedings [8]. The range of digital forensics includes computer devices, network servers, and mobile handsets. The following of digital forensic tools is designed for different types of examined targets.

a) Memory Forensics: Volatility, WindowsSCOPE, RAM Capturer, Magnet RAM Capture, and Memoryze.

b) *Mobile Device Forensics:* CelleBrite UFED, XRY, and Oxygen Forensic Suite.

c) *Network Forensics:* Wireshark, Network Miner, Xplico, and E-Detective.

d) *Computer Forensics:* EnCASE, FTK, Sleuth Kit Autopsy, TCT, and DEFT.

IV. DISCUSSIONS AND ANALYSES

Computers now hold more information and more processing power than before. That brings a great challenge for LEAs to deal with increasingly large amounts of digital evidence. Investigators must have the capability to process large amounts of information accurately, completely, and promptly [8]. This practical method of reducing digital forensic backlogs becomes critical for LEAs.

A. Reducing Digital Forensic Backlogs: Triage

As the prevalence of digital evidence in criminal, civil, or administrative cases becomes popular, backlogs in forensic labs continue to proliferate [6]. Triage originally means that when medical resources are insufficient to deal with all injuries, they are classified, sorted, or selected to determine the priority order of emergency treatment. Then the injured can be treated efficiently and based on the injury situation of the patients to determine the priority treatment process [10]. First responders need to set up a series of digital triage processes to classify the various cases or scenes and to determine whether some devices need further examinations in the lab. The purpose of digital triage is to prioritize digital media and obtain quick intelligence. It is a solution to the problem of case backlogs [11]. Digital triage is the investigative beginning of the forensic examination. Fig. 2 demonstrates two types of digital triage: live and dead. A triage assessment does not replace the forensic analysis. Some initial tasks can be performed at the scene by non-digital evidence specialists to increase the efficiency of an investigation promptly and to decrease the examination backlog in the lab.

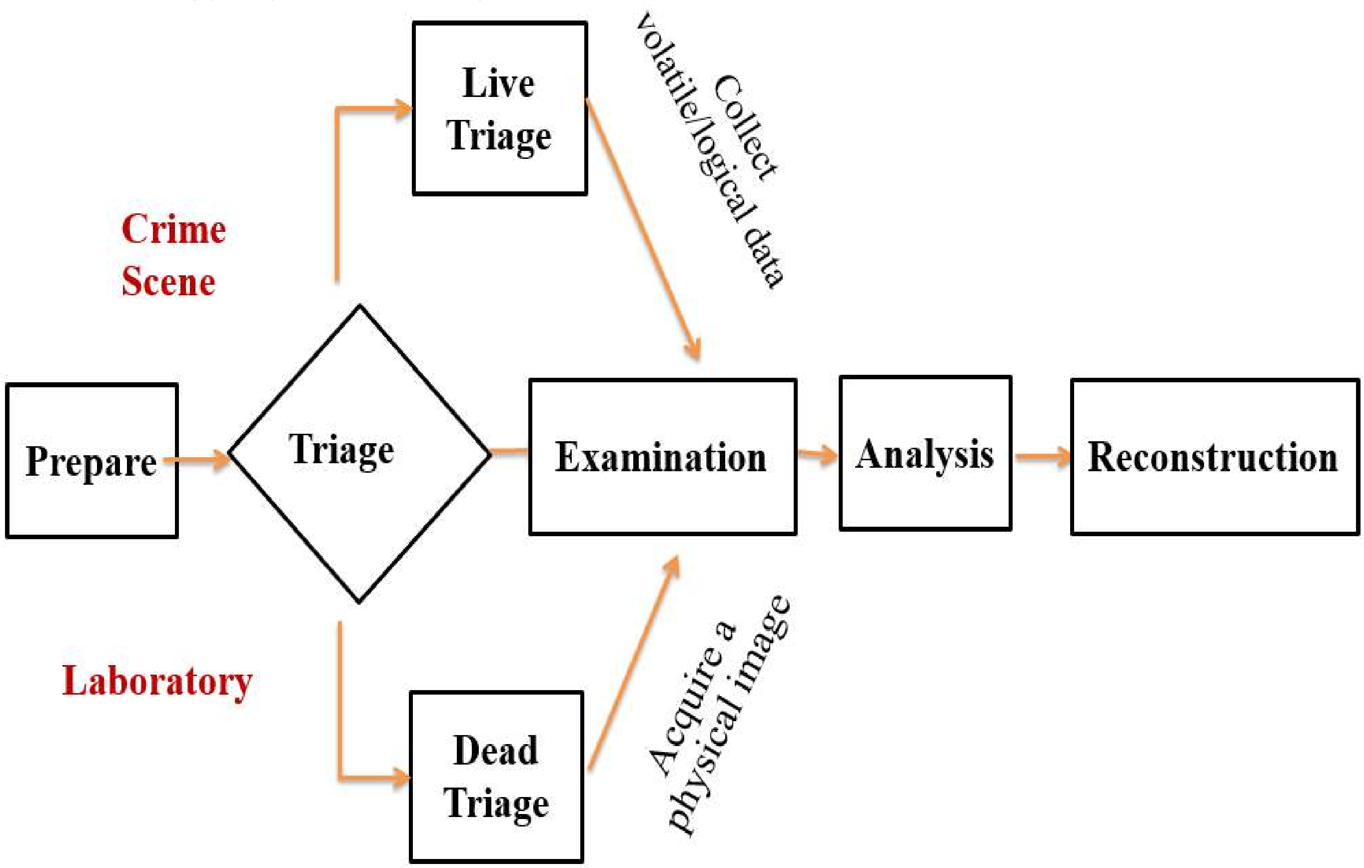

Fig. 2. The triage evidence process of TEAR phases in reducing digital forensic backlogs

1) Live Triage: Volatile/Logical Data

The primary purpose of live triage is a rapid extraction of quick intelligence from online sources. Live triage has the potential to identify evidential data quickly. First responders need to find the following volatile and logic data from the power-on device.

a) Volatile Evidence: memory, network connections, running process, and open files.

b) Logical Data: operating system setting, network status, execution information, and system log records.

2) Dead Triage: Physical Image Files

Dead triage is conducted in the lab for the possible existence of the relevant evidence. Some types of tools are [10]:

a) Acquiring a copy of the image file.

b) Indexing, searching, cracking, and analyzing digital content in digital media.

c)Presenting a forensic report

3) Scene Investigation

Scene investigation focuses on the compelling evidence of the power-on status to detect and explore any possible answers to scenarios. At the scene, an active investigation of the primary memory content can be conducted to collect the volatile evidence under the power-on state quickly. The scene must be photographed or recorded appropriately. Turning off computer power is not the first thing to do at the scene since immediately turning off the power of the computer will inevitably result in the loss of programs and data running in memory. Sometimes, it will destroy valuable evidence.

4) Lab Forensics

Lab forensics focuses on identifying results in the static evidence of shutdown status. In the lab, dead forensics analysis for digital storage media can be repeatedly verified for integrity. However, this time-consuming processing can result in excessive backlogs from a large number of new cases for LEAs.

B. TEAR Phases of THOR Dimensions in Digital Forensics

An additional concern was the inability to communicate with other investigators, cross into other jurisdictions, and coordinate cybercrime investigations during investigations [5]. This proposed triage triangle strategy helps LEAs produce a quality report [6]. Fig. 3 also illustrates TEAR phases from the viewpoint of THOR dimensions to describe the proper practices for identifying, collecting, acquiring, and preserving the digital data [12]. The two axes represent the perspectives and processes of digital forensic investigation.

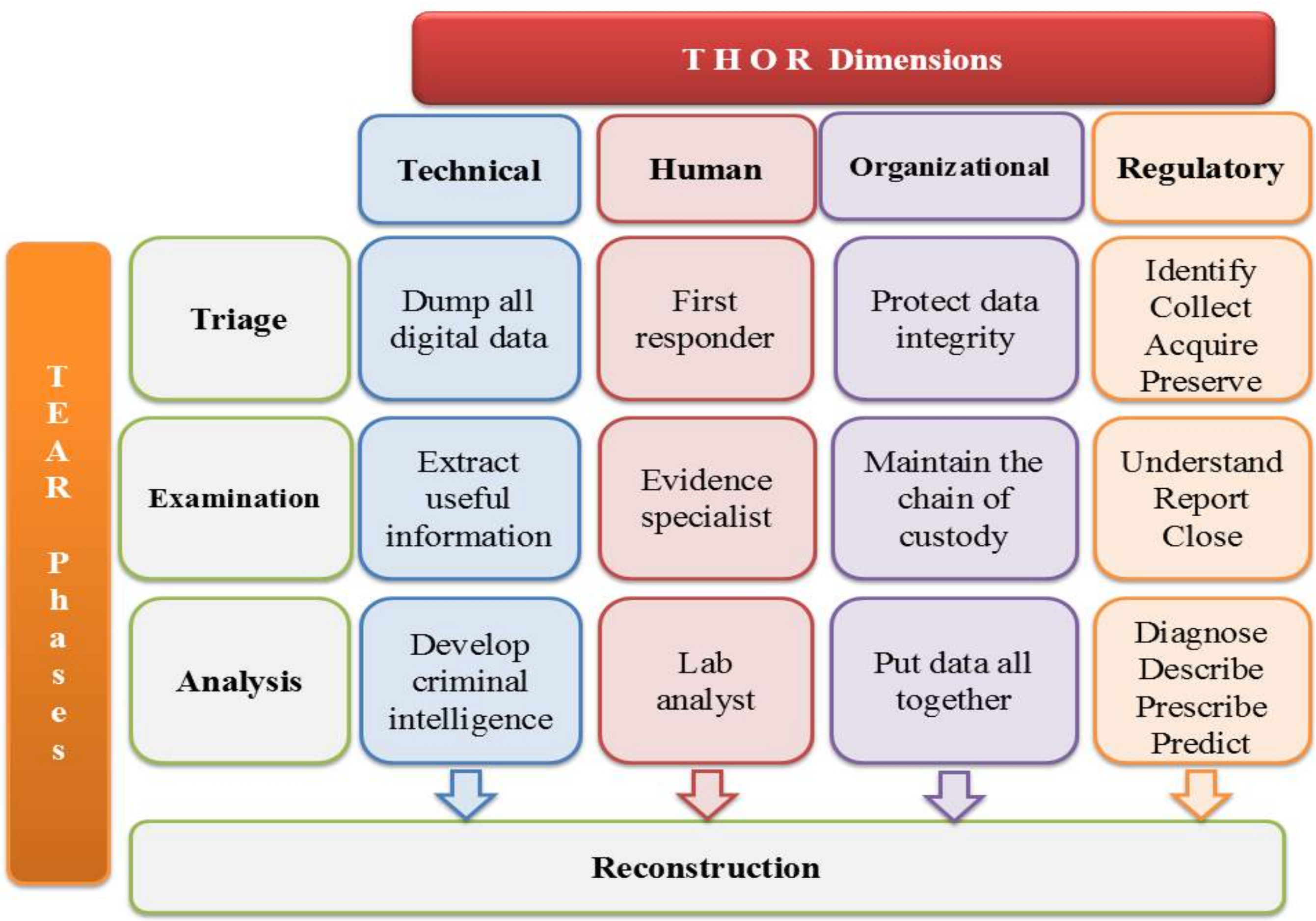

Fig. 3. The TEAR phases of THOR dimensions in the proposed triage triangle strategy

1) Triage

First responders can use a triage tool to preview data at the scene.

a) Technical: Some tools are available to dump relevant data.

b) Human: As technology changes, first responders must continually update their devices and training. They assist at the scene.

c) *Organizational:* Evidence integrity refers to the preservation of evidence in its original form. The inspection process must be supervised or recorded.

d) Regulatory: The ISO/IEC 27037:2012 guidelines for identification, collection, acquisition, and preservation in handling potential digital evidence are required in an investigation to maintain the integrity of the digital evidence.

2) Examination

Evidence specialists extract useful data from digital devices, bring raw data to the lab, and maintain the chain of custody at the same time.

a) Technical: They use tools to extract useful information from collected evidence.

b) Human: They are responsible for documenting and preparing evidence once it arrives at the scene.

c) Organizational: They should comply with the chain of custody, which includes the documentation of physical and digital evidence.

d) *Regulatory:* The forensic examination aids the understanding of the evidence and assists the court to close the case.

3) Analysis

Lab analysts should determine the processes necessary to complete the analysis.

a) *Technical:* They should integrate the extracted data and develop an intelligence analysis platform.

b) *Human:* Forensics analysts who work in the lab combine relevant events into exploring the fact.

c) *Organizational*: They should put data altogether to help the court make the right decisions.

d) Regulatory: Investigators can use big data analytics to diagnose, describe, prescribe, or predict the case.

4) Reconstruction

Reconstruction refers to the systematic process of piecing together evidence and information gathered during a crime to gain a better understanding of what transpired between the victim and the criminal [3]. It involves ordering the evidential associations from temporal, relational, and functional analysis. Crime reconstruction is the determination of the actions and events for establishing the continuity of a crime. It can leverage a wide range of forensic methods to establish a hypothesis about the sequence of events and test whether the hypothesis is correct or not. If the hypothesis is confirmed, then one possible explanation can be identified. If it is refuted, then the explanation is not possible, and other hypotheses will have to be considered [1].

C. Proposed Tools in Digital Forensic Investigations

Many LEAs use tools to examine a target machine or network [5]. Available tools can increase the speed of the digital forensic process and reduce the number of devices in the lab. That will reduce case backlog and improve the quality of first responders, evidence specialists, lab analysts, or investigators. Several tools for conducting cybercrime investigations in TEAR phases are introduced below (Table I) [11]. Well-planned use of digital forensic tools can improve efficient and effective investigations.

TABLE I
AVAILABLE TOOLS IN TEAR PHASES

Phases	Functions	Tools
Triage	Identify artifacts in memory	Volatility, WindowsSCOPE, RAM Capturer, Magnet RAM Capture, and Memoryze
Examination	Examine images	FTK Imager
	Examine information from browsers	Dumpzilla
	Carve data files	SIFT
Analysis	Analyze information from a phone	CelleBrite UFED, XRY, and Oxygen Forensic Suite
	Parse the data of USB devices	USB Historian
	Acquire web pages	FAW
Reconstruction	Investigate the network-related activity	Wireshark, Network Miner, Xplico, and E-Detective
	Recover data from computer devices	EnCASE, FTK, Sleuth Kit Autopsy, TCT, and DEFT

1) Triage

a) Volatility: It can identify the running processes, network activities, and open connections for volatile memory analysis of Windows, Linux, Mac & Android systems.

b) *WindowsSCOPE:* It enables memory forensics for Windows computers and provides the memory forensics analysis for security breaches. It can identify the processes, threads, and drivers running on the system.

c) *RAM Capturer*: It can dump the data from the computer's volatile memory, which may contain encrypted volume's password and login credentials for web services.

d) *Magnet RAM Capture*: It can capture the physical memory of a computer and analyze artifacts in memory.

e) *Memoryze:* It can create, acquire, and analyze an image and identify all running process, drivers, or malicious activities in live memory.

2) Examination

a) FTK Imager: It can create MD5 or SHA1 file hashes and examine files, memory dumps, or images.

b) Dumpzilla: It can examine the information from browsers.

c) *SIFT:* SANS Investigative Forensic Toolkit (SIFT) can carve data files, generate a timeline from system logs, and carry out forensic analysis.

3) Analysis

a) *CelleBrite UFED*: Cellebrite Universal Forensic Extraction Device (UFED) can extract information and recover deleted data from mobile devices.

b) *XRY:* It can analyze and recover information in a forensically sound manner from mobile phones, smartphones, and tablet computers.

c) Oxygen Forensic Suite: It can identify app accounts, communicated contacts, geolocation metadata, and other information from a mobile phone. It can further analyze photos, documents, videos, and device database.

d) *USB Historian:* It can parse the USB history data from the computer.

e) *FAW:* Forensics Acquisition of Websites (FAW) can acquire web pages and files online.

4) Reconstruction

Evidence on computers and networks should be included to gain an understanding of a crime reconstruction [2].

a) Wireshark: It can capture the network-related activity, analyze network protocols, and support Windows, Linux, and Mac OS.

b) *Network Miner:* It can examine hostnames, sessions, open ports, and operating systems from network traffic.

c) Xplico: It can analyze email, HTTP contents, and VoIP call data from network traffic.

d) *E-Detective:* It can capture, decode, reassemble, and reconstruct various types of network traffic such as Email, Webmail, Instant Messaging, File Transfer, and VOIP.

e) *EnCase:* It can collect Internet artifacts, acquire data, and produce a report.

f) *FTK:* Forensic Toolkit (FTK) can crack a password, analyze emails, or look for specific characters in files.

g) *Sleuth Kit Autopsy:* It consists of command-line tools. It can analyze smartphones and hard disks.

h) *TCT:* The Coroner's Toolkit (TCT) can recover data from computer disasters under several Unix-related systems.

i) *DEFT:* Digital Evidence and Forensics Toolkit (DEFT) can gather, acquire, and preserve digital evidence on running systems.

V. Conclusion

Cybercrimes have put LEAs at a significant disadvantage. There is still much work to ensure that LEAs have the necessary resources or tools in investigating cybercrimes. Digital forensics is a continuous procedure. Each phase has a high impact on the relevance, reliability, and sufficiency of the evidence. The increase of substantial digital evidence backlogs is encountered in a criminal investigation by LEAs throughout the world. The crime scene is often the driving force behind a successful criminal investigation. Properly collecting digital evidence is essential in cybercrime investigation. The examination of digital sources should be completed empirically, logically, and systematically consistent with organizational policy. With the development of information technology, investigators need to get the evidence quickly and sufficiently. This study explores this backlog challenge in digital forensics from a technical standpoint, proposes a triage triangle strategy, and contribute to an efficient digital forensic process. It is also critical to quickly assist the court in finding the root reasons for a case. This proposed strategy may improve the speed and quality of investigations.

References

[1] Brooks, C. L., *CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide (1st Edition)*, McGraw-Hill Education, pp. 13-50, 2015.

[2] Casey, E., *Handbook of Digital Forensics and Investigation*, Burlington, MA: Elsevier Inc., pp. 21-208, 2010.

[3] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd Edition)*, Elsevier Inc., pp. 187-306, 2011.

[4] Choraś, M., Project Final Report: Comprehensive Approach to cyber roadMap coordINation and develOpment, ITTI Sp. Z o.o., Poland, pp. 15-39, 2016.

[5] Cummins Flory, T. A., "Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies," *Journal of Digital Forensics, Security and Law*, Vol. 11. No. 1, pp. 7-38, 2016.

[6] International Organization for Standardization (ISO), "ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence," ISO Office, 2012.

[7] International Organization for Standardization (ISO), "ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes," ISO Office, 2015.

[8] Keeling, D. G. and Losavio, M., "Public Security & Digital Forensics in the United States: The Continued Need for Expanded Digital Systems for Security," *Journal of Digital Forensics, Security and Law*, Vol. 12. No. 3, pp. 47-60, 2017.

[9] Losavio, M.M., Chow, K.P., Koltay, A., and James, J., "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security, *Security and Privacy,* Vol. 1, No. 3, pp. 1-11, 2018.

[10] Pearson, S. and Watson, R., *Digital Triage Forensics: Processing the Digital Crime Scene*, Elsevier Inc., Burlington, 2010.

[11] Stephenson, P., *Official (ISC) 2® Guide to the Certified Cyber Forensics Professional (CCFP) Common Body of Knowledge (CBK)*, Auerbach Publications, pp. 293-404, 2014.

[12] Ubelaker, D. H., *The Global Practice of Forensic Science*, John Wiley & Sons Ltd, pp. 34-263, 2015.

Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.

Ni-Chen Wu received the B.S. degree in Information Management from Central Police University, Taiwan, in 2019. Since 2019, she is a police officer in Taiwan. Her current research interests include information security, incident response, cybercrime investigation, digital forensics, information systems management, criminal profiling, and cyber criminology.

Fu-Ching TSAI received the B.S. degree in Information Management from Central Police University, Taiwan, in 2001, the M.S. and Ph. D degrees in Institute of Information Management from National Cheng Kung University, Taiwan, in 2005 and 2013. Since 2018, he has been with Central Police University, Taiwan, where he is currently an assistant professor in the Department of Criminal Investigation. His research interests include big data analysis, data mining, text mining, and artificial intelligence.

ICT Enabling Technologies for Smart Cities

Dzung Van DINH*, Byeong-Nam YOON**, Hung Ngoc LE***, Uy Quoc NGUYEN****,
Khoa Dang PHAN*, Lam Dinh PHAM*
*Information Technology Institute, Vietnam National University (VNU), Vietnam
**Global IT Research Institute (GIRI), Korea
***VKX Ltd. (Viet Nam Korea Exchange Joint Venture Company), Vietnam
****PTIT (Posts and Telecommunications Institute of Technology), Vietnam
dzung.dinh@vnu.edu.vn, tomayoon@hotmail.com, lnhung@vkx.com.vn,
nguyenquocuy2008@gmail.com, khoapd@vnu.edu.vn, phamdinhlam@vnu.edu.vn

Abstract— **A smart city adjusts its social, business, and natural needs, improving the assets it has accessible. Information and Communications Technology (ICT) for shrewd urban areas is to give city answers for encourage an improvement and manageability of a city for the advantage of its population, its economy, and the greater ecosystem in the city. It is to gauge a keen city as far as the enhancements in personal satisfaction and monetary prosperity that are accomplished through applying ICT innovations to design, outline, fabricate, and work the city foundation. In smart city applications, the initial phase in the information's voyage through the application is its gathering by the diverse advancements conveyed all through the city. This paper surveys data acquisition technologies such as Sensor Networks, MANETs, Unmanned Aerial Vehicles (UAVs), Vehicular Ad hoc Networks (VANETs), Internet of Things (IoT), Software-Defined Networking(SDN), Network Functions Virtualization (NFV), 5G. Next, it demonstrates information processing technologies, for example, Cloud Platform, IoT Platform, Big Data Platform, Machine Learning, Deep Learning, and IoT Analytics. Encouraging data spread between various nodes is vital to savvy city acknowledgment. Last, because of the presence of various types of end users (e.g., residents, organizations, government offices, and so forth.) requiring distinctive levels of nature of management, the paper exhibits a proposed testbed solution and recent associated experiments.**

Keywords— **IoT, SDN, NFV, 5G, Cloud Platform, IoT Platform, Big Data Platform, IoT Analytics**

Manuscript received October 9, 2018. This work was supported in part by the "ASEAN forum for Software Defined System on Disaster Mitigation and Smart Cities" and "IoT Open Innovation Platform", which are funded by National Institute of Information and Communications (NICT, Japan) under the ASEAN IVO program (ICT Virtual Organization of ASEAN Institutes and NICT).

Dzung Van DINH is with the Information Technology Institute, Vietnam National University (VNU-ITI), Vietnam. (corresponding author phone: +84 91 3222 690 e-mail: dzung.dinh@vnu.edu.vn).

Byeong-Nam YOON is with the Global IT Research Institute (GIRI), south Korea. (phone: +82 010-9837-8839 e-mail: tomayoon@icact.org)
Hung Ngoc LE is with the Viet Nam Korea Exchange Joint Venture Company (VKX Ltd.), Vietnam. (e-mail: inhung@vkx.com.vn)

Uy Quoc NGUYEN is with the Posts and Telecommunications Institute of Technology (PTIT), Vietnam. (e-mail: nguyenquocuy2008@gmail.com)

Khoa Dang PHAN is with the VNU-ITI, Vietnam. (e-mail: khoapd@vnu.edu.vn)

Lam Dinh PHAM is with the VNU-ITI, Vietnam. (e-mail: phamdinhlam@vnu.edu.vn)

INTRODUCTION

By 2030, the total population is anticipated to be 8.5 billion and increment to 9.7 billion by 2050 and 11.2 billion by 2100. Half of humankind today lives in urban areas. Numerous urban communities are encountering exponential development as individuals move from rustic zones looking for better occupations and training. Subsequently, urban administrations and foundations are being extended as far as possible as far as adaptability, condition, and security as they adjust to help this population growth. Visionaries and organizers are subsequently looking for a maintainable, present carbon economy on enhance vitality productivity and limit carbon-emanation levels.

The European Parliament defined: "A smart city is a city seeking to address public issues via information and communication technology (ICT) - based solutions on the basis of a multi-stakeholder, municipality based partnership." This is very expansive, including many fields, while the Japanese definition is more particular, concentrating on energy, infrastructure, ICT, and lifestyle.

From these definitions, we derive ICT assumes an urgent part in building up a city that can adjust to the necessities of its nationals. By utilizing advanced power systems, networking, and communication technologies, a smart city aims to enhance the lives of its citizens and optimize territorial, economic, and environmental resources. Navigant Research says investment in smart cities is divided into smart government, smart building, smart transport, and smart utilities. By 2020, $13 billion in funding is expected to establish smart cities all over the world (see Figure 1). [1]

The rest of this paper is organized as follows. We have reviewed the ICT enabling technologies for data acquisition in the context of smart cities (Section II). Next, we have analyzed potential networking and computing technologies for smart cities (Section III). Section IV presents data processing technologies candidates for smart cities. The proposed solution and associated experiments are provided in Section V. Finally, we summarize and conclude this study in Section VI.

Figure 1. Smart city investments by the regions, 2014–2023 [1]

I. Data Acquisition Technologies for Smart Cities

In this section, a review of the ICT enabling technologies for data acquisition in the context of smart cities is given. These technologies include Wireless Sensor Networks (WSNs), Mobile Ad hoc Networks (MANETs), Unmanned Aerial Vehicles (UAVs), Vehicular Ad hoc Networks (VANETs), 5G.

A. Wireless Sensor Networks

Sensor networks are used for many applications (e.g., environment monitoring, waste management, health monitoring, smart grids, etc.), for collecting data in smart cities. Current cities are already deploying a wide range of sensors (e.g., motion sensors, cameras, sensors for collecting environmental parameters, etc.) [2]. In general, the applications can be divided into two types: monitoring and tracking. Monitoring is used for analysing and controlling a system in real-time (environment, agriculture, industry, health care, ecology, urban, smart house, military, etc.). Tracking is used for recording the change of an event, a person, an animal, and so on (industry, public health, ecology, military, etc.) [3].

1) Radio technologies: The standardization of WSN has been very active in the recent years. A comparison of emerging and existing radio technologies for WSNs is presented in Table 1.

TABLE 1. WSN standards and technologies [4]

	IEEE 802.15.4 (ZigBee)	UWB IEEE 802.15.4a	Blue-tooth	BLE	Z-wave	ANT	Wavenis	Dash7	EnOcean
Frequency (ISM)	868/915 MHz; 2.4 GHz	3.1–10.6 GHz	2.4 GHz	2.4 GHz	sub-1 GHz	2.4 GHz	868, 915, 433 MHz	433 MHz	868; 315 MHz
Max Data rate	250 kbps	110 Mbps	3 Mbps	1 Mbps	40 kbps	1 Mbps	100 kbps	200 kbps	125 kbps
Range	100 m	10 m	10–100 m	200 m	30 m		1–4 km	2 km	300 m
Battery life	Days–years	Multi-year		Months–years	Multi-year	Year	Multi-year	Multi-year	Battery-less
Network topology	Star, P2P, Mesh		P2P	P2P	Mesh	Star, P2P Tree Mesh	P2P		
Power consumption	Low	Low	Low	Ultra-low	Low	Ultra-low	Ultra-low	Low	Ultra-low
Open	✓	✓	✓	✓	✓	X	✓	✓	✓
IPv6	✓			✓	✓		✓		
Target Market/ Application	Smart-meter, Smart grid devices	Real-time monitor and track location (Indoor)	Consumer electronics	Health fitness, Smart devices	Home automation, security, consumer electronics	Health Fitness Heart- rate monitor, Speed sensors	M2M, smart meter, Telemetry, Home automation	Mobile payments, Smart meter, Supply chain,	Building, Industrial Automation self-powered sensors, switches

2) Machine Learning in Wireless Sensor Networks: WSNs screen dynamic conditions that change quickly after some time. This dynamic conduct is either caused by outer factors or started by the framework originators themselves. To adjust to such conditions, sensor networks often adopt machine learning techniques to wipe out the requirement for pointless upgrade. Machine learning additionally motivates numerous solutions that boost asset use and draw out the life expectancy of the network.

Supervised learning methods are broadly used to understand a few difficulties in WSNs, for example, localization and objects targeting, event detection and query processing, media access control, security and intrusion detection, and quality of service (QoS), data integrity and fault detection.

Unsupervised learning methods are not provided with labels. Fundamentally, the objective of an unsupervised learning calculation is to arrange the example set into various gatherings by examining the closeness between them. Of course, this subject of learning calculations is generally utilized as a part of node clustering and data aggregation problems.

Reinforcement learning empowers an agent (e.g., a sensor node) to learn by cooperating with its surroundings. The agent will figure out how to take the best actions that augment its long haul remunerates by utilizing its own particular experience. [5]

3) Software-Defined Wireless Sensor Networks: WSN is a low-rate wireless transmission platform with little resources and short communication ranges. As the scale of WSN increases, it faces some challenges, such as network management and heterogeneous-node networks. As Software Defined Networking (SDN) provides simplicity in network management, and computing resources configuration, it can solve these problems.

The SDN way to deal with remote sensor systems involves abstracting distinctive functionalities and revamping them along the three coherent planes in the SDN architecture: application, control and data. The advancement of the SDWSN design is still in its early research stages. Despite the fact that there are a number of models, they all fit in with the basics of SDN: decoupling. Fig. 2 shows the fundamental functionalities of SDWSN as proposed by different authors. SDN display brings along its own difficulties, particularly the trade-off between functionalities that should be held on the sensor node and the effect on basic network factors, for example, latency, congestion, and so on. [6]

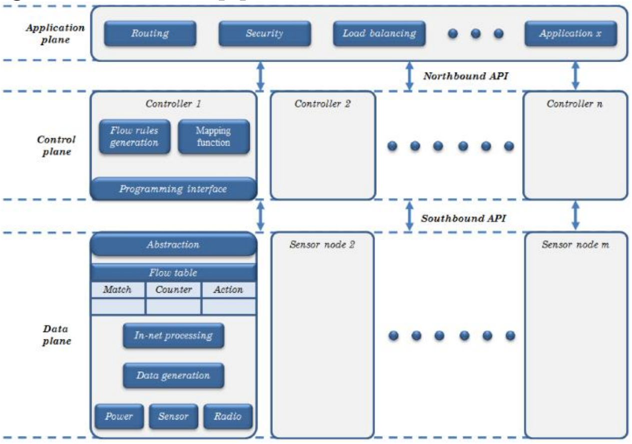

Figure 2. Basic SDWSN architecture [6]

4) Wireless Sensor Network Virtualization: WSNs' hubs are ending up increasingly intense, it is getting increasingly correlated to explore how different applications could share an exceptionally same WSN platform. Virtualization is an innovation that can possibly empower this sharing (see Fig. 3). It is a promising method that can permit the effective usage of WSN arrangements, as various applications will have the capacity to exist together on the same virtualized WSN.

There are open research issues that should be tended to for giving new WSN virtualization arrangements: propelled node level virtualization, network level virtualization, discovery and publication, service integration, sensor node choice and assigned task, application undertaking dispersal, reference design and structures, new protocols, techniques and simulation tools, WSN virtualization plan of action and standardization, energy effective arrangements, access control, authentication, and accounting, and WSN virtualization user cases and testing environments. [7]

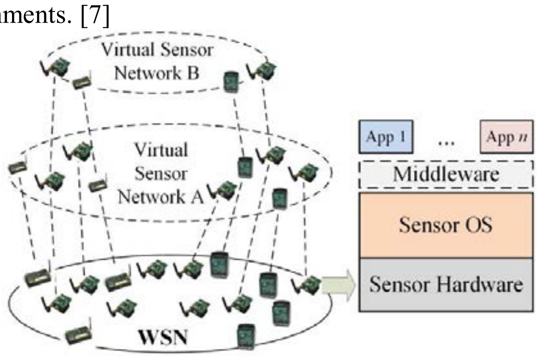

Figure 3. Middleware and virtual network-based solutions [7]

B. IEEE 802.11-enabled wake-up radio system

The Internet of Things is anticipated to comprise of billions of devices by 2020. The Wi-Fi, Mobile, and Bluetooth protocols are likewise the three main candidates for interfacing the Internet of Things - and each has own advantages and drawbacks. Huge numbers of these devices will keep running on batteries. To draw out the helpful existence of these batteries, while ensuring devices don't remain in a rest state too long and run gradually, devices must have the capacity to keep running in a low-control, low-inertness state. Wake-Up Radio, which is being created by the IEEE 802.11ba working group, offers an answer for this challenge. The IEEE 802.11ba Wake-Up Radio adds an additional low-power radio receiver to the device (see Fig. 4). The low-power radio listens for the system call. [11]

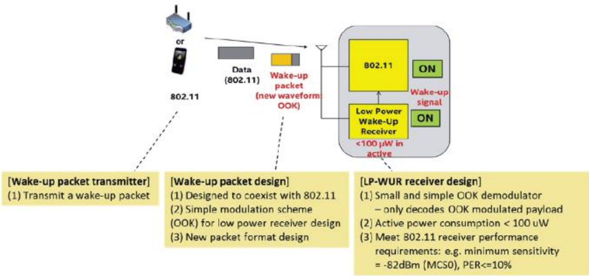

Figure 4. Overview of low-power radio for IEEE 802.11ba [11]

C. Vehicular Ad hoc Networks (VANETs)

VANETs are a sort of MANETs that are widely considered with regards to smart mobility and intelligent transportation. VANETs encourage Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I). Vehicle-to-anything (V2X) communications represent both V2V and V2I. Since VANETs are a variation of MANETs, the issues that torment MANETs additionally impact the data obtaining process in VANETs. Distinctive sorts of uses can use the information gathered in VANETs. These applications can be sorted into security and infotainment applications. Security applications are utilized to enhance street wellbeing, for example, forward collision warning, while infotainment applications are equipped towards solace and amusement for vehicle travellers, for example, traffic and weather information. [8]

V2X innovation has an extraordinary capability of empowering an assortment of novel applications for street safety, traveller infotainment, car producer administrations, and car traffic optimization. Today, V2X communications depends on one of two fundamental methods: dedicated short range communications (DSRC) and mobile communications networks (see Fig. 4).

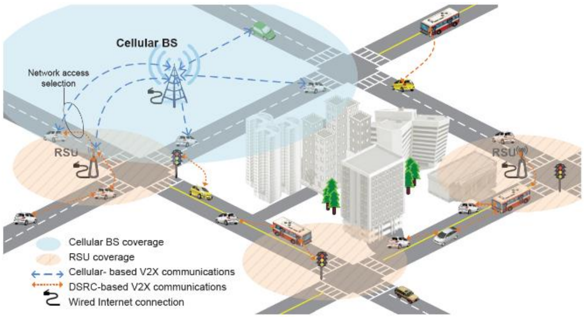

Figure 5. V2X communications in a DSRC-cellular hybrid scenario [9]

To enable V2X applications for an expansive number of vehicles, interworking amongst DSRC and cell arrange advancements is a promising methodology, which can be founded on a flat or a hierarchical DSRC-cellular hybrid architecture. Nonetheless, so as to proficiently accomplish such DSRC-cell interworking, we have to determine numerous specialized issues, primarily starting from the profoundly unique vehicular system topology, together with the pattern of little cell arrangement in cutting edge cell systems, which requires successful vertical handover strategies and system determination plans. What's more, DSRC is accomplished over saved radio range groups, which contrast in North America (IEEE 1609), Europe (ETSI EN 102/202/300/302), and Japan (ARIB STD-T55/75/88/109/110), leading to incompatibility problems among these regions. [9]

D. Unmanned Aerial Vehicles (UAVs)

Unmanned Aerial Vehicles (UAVs) show potential in the general the public and civil areas. These are especially helpful in applications where human lives would some way or another be jeopardized. Multi-UAV frameworks can cooperatively entire missions all the more effectively and financially when contrasted with single UAV frameworks. Be that as it may, there are many issues to be settled before viable utilization of UAVs can be made to give steady and solid setting particular systems.

Table 2 provides a summary of MANETs, VANETs and UAV systems. Most of the studies of MANETs, and VANETs does not address the exceptional attributes of the UAV systems. UAV systems may change from ease back unique to dynamic; have discontinuous connections and fluid topology. While it is trusted that ad hoc mesh network would be most reasonable for UAV arranges yet the engineering of multi-UAV systems is for a further study. SDN could encourage deployment and management of new services and help decrease cost, increment security and accessibility in systems. Steering requests of UAV systems go past the necessities of MANETs and VANETs. Conventions are required that would adjust to high versatility, dynamic topology, irregular connections, control imperatives and changing connection quality. UAVs may come up short and the system may get divided making deferral and disturbance resistance a critical outline thought. Restricted existence of the node and dynamicity of the system prompts the necessity of seamless handovers where investigators are taking a result at the work done for MANETs and VANETs. As vitality supply on UAVs is restricted, conventions in different layers ought to contribute towards greening of the system. [10]

E. 5G Communications

1) Vision: The fifth generation mobile communications system (5G) is expected to launch in 2020, is required to give around 1000 times higher wireless area traffic capacity and save up to 90 percent of energy consumption per service compared with the current 4G system. More than 1000 Gb/s/km2 area spectral capacity in dense urban environments, 10 times higher battery life of associated devices, and five times lessened end-to-end (E2E) delay are expected in 5G systems. The new 5G air interface and range ought to be joined together with the Long Term Evolution (LTE) and WiFi to give all inclusive high-rate coverage and seamless user experience. [12]

Figure 6 shows the key 5G requirements in contrast with earlier mobile networks generations, for example, IMT-Advanced. [13][14]

TABLE 2. AD-HOC NETWOKS COMPARISION [10]

	MANET	VANET	UAV Networks
Description	Mobile wireless nodes connect with other nodes within communication range in an ad-hoc manner (No centralized infra-structure required)	Ad-hoc networks in which vehicles are the mobile nodes. Communication is among vehicles and between vehicles and road side units	Ad-hoc or infrastructure based networks of airborne nodes. Communication among UAVs and with the control station
Mobility	Slow. Typical speeds 2 m/sec. Random movement. Varying density, higher at some popular places	High-speed, typically 20-30 m/s on highways, 6-10 m/s in urban areas. Predictable, limited by road layout, traffic and traffic rules	Speeds from 0 to typically as high as 100 m/s. Movement could be in 2 or 3 dimensions, usually controlled according to mission.
Topology	Random, ad-hoc	Star with roadside infrastructure and ad-hoc among vehicles	Star with control center, ad-hoc/mesh among UAVs.
Topology Changes	Dynamic - nodes join and leave unpredictably. Network prone to partitioning.	More dynamic than MANETs. Movement linear. Partitioning common.	Stationary, slow or fast. May be flown in controlled swarms. Network prone to partitioning
Energy Constraints	Most nodes are battery powered so energy needs to be conserved.	Devices may be car battery powered or own battery powered.	Small UAVs are energy constrained. Batteries affect weight and flying time
Typical use cases in public and civil domains	• Information distribution (emergencies, advertising, shopping, events) Internet hot spots	• Traffic & weather info, emergency warnings, location based services • Infotainment	• Rescue operations • Agriculture-crop survey • Wildlife search • Oil rig surveillance

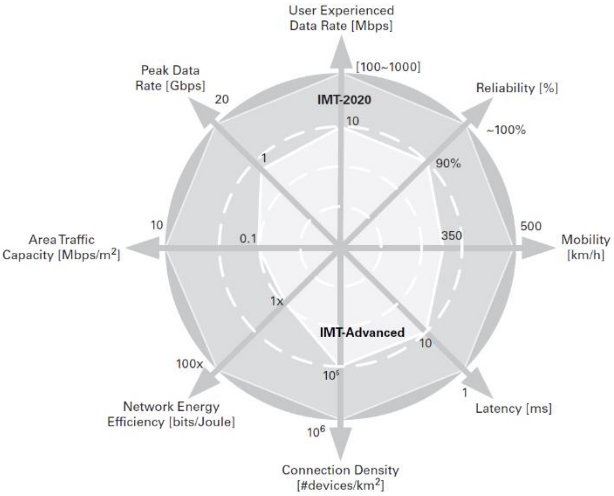

Figure 6. IMT-2020 and IMT-A requirements [14]

2) Machine-Type Communication (MTC): MTC indicates the wide territory of wireless communication with sensors, actuators, physical articles and different devices not straightforwardly used by people, shaping the supposed Internet of Things (IoT). The present view on the 5G wireless systems specifies MTC into two groups, as appeared in Figure 7: massive MTC (mMTC) and ultra-reliable and low-latency MTC (uMTC). mMTC accept delay-tolerant services for regularly occasional data transmissions, with a huge number of devices that are now and then even battery-worked. Meanwhile, uMTC can provide reliable and low delay communications for controlling objects and processes in real-time. [14]

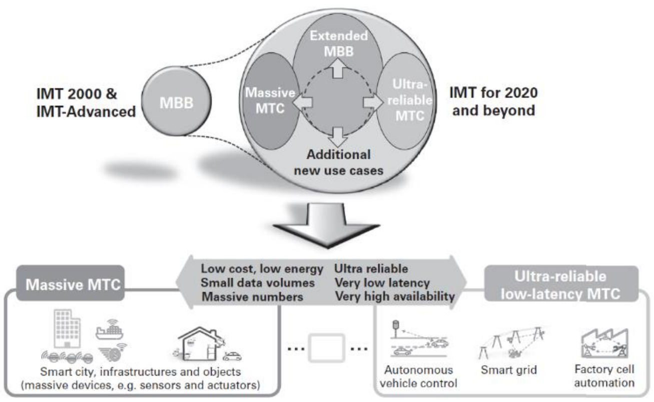

Figure 7. MTC in the 5G wireless systems. [14]

3) The 5G radio-access technologies: Table 3 gives a short diagram on the radio-access technologies, featuring some of their attributes and properties. [14]

Orthogonal multiple-access techniques depend on partitioning radio assets (in time or frequency) between different subscribers. The schemes are respectively Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) and Orthogonal Frequency Division Multiple Access (OFDMA). FDMA and OFDMA are very similar, however, FDMA has non-overlapping frequency sub-bands, while OFDMA has overlapping frequency sub-bands. In a single cell infrastructure with AWGN channels, all orthogonal multiple-access schemes are almost equivalent with respect to capacity. The differences between multiple-access schemes become visible when transmission channels exhibit frequency selectivity and time variability.

Novel various access plans take into account for overloading the spectrum by multiplexing users in the power and the code domain, resulting in non-orthogonal access, where the number of simultaneously served users is no longer bound to the number of orthogonal resources. This approach empowers the quantity of associated devices to be expanded by a factor of 2–3 and, in the meantime, to obtain gains in user and system throughput of up to 50%. Potential schemes are Non-Orthogonal Multiple Access (NOMA), Sparse Code Multiple Access (SCMA) and Interleave Division Multiple Access (IDMA).

TABLE 3. 5G MULTIPLE AND MEDIUM ACCESS SCHEMES. [14]

Name	Type[1], direction[2]	Separation of resources	Advantage	Disadvantage
OFDM	Multiple, UL & DL	Time, frequency	Simple implementation, simple equalization	Large side lobes require tight sync and large guard bands
FBMC-OQAM	Multiple, UL & DL	Time, frequency	Small side lobes enable coexistence and relaxed sync	Orthogonality in the real field requires redesign of selected algorithms
UF-OFDM	Multiple, UL & DL	Time, frequency	Reduced side lobes, compatible with OFDM, relaxed sync	Vulnerable to large delay spread
SCMA	Multiple, UL & DL	Code & power	Limited CSIT	Complex receiver (MPA)
NOMA	Multiple, UL & DL	Power	Limited CSIT	SIC receiver
IDMA	Multiple, UL	Code	Limited or no CSIT	Iterative receiver
Coded Slotted Aloha	Medium	Not applicable	High reliability with minimal coordination	Complex receiver
Coded Access Reservation	Medium, UL	Not applicable	compatible with LTE	High overhead for small packets
Coded Random Access	Medium, UL	Not applicable	Suitable for small packets	MUD

4) Network Slicing for 5G with SDN/NFV: One of the key drivers of 5G systems is the need to help an assortment of vertical businesses, for example, manufacturing, automotive, healthcare, energy, and media and entertainment. Such verticals begin altogether different utilize cases, which force a significantly more extensive scope of requirements than existing mobile services. The present systems, with their "one-estimate fits-all" compositional approach, can't address the separating execution prerequisites that verticals force as far as latency, scalability, availability, and reliability. System softwarization, a trend that looks to change systems utilizing programming based arrangements, can be a potential empowering influence for comprehending this. Through innovations like SDN and Network Functions Virtualization (NFV), organize softwarization can give the programmability, adaptability, and measured quality that is required to make numerous consistent (virtual) systems, each customized for a given utilize case, over a typical physical system. [15]

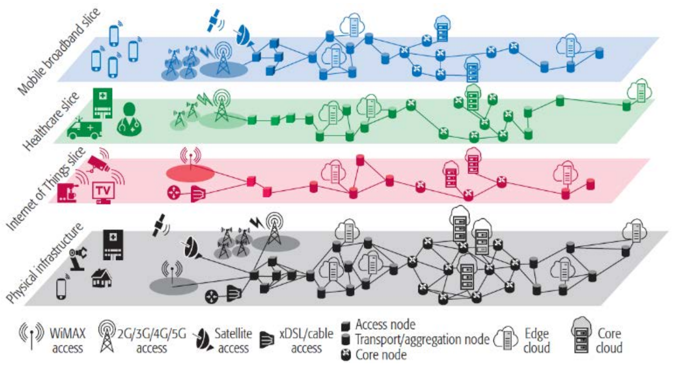

Figure 8. 5G network independent slices running on a common underlying physical multi-vendor and multi-access network for user cases. [15]

5) 5G Standardisation: The overall 5G roadmap is summarized in Figure 8, capturing trials phases and the high-level standardization time plans. The standards for 5G are to be prepared by the ITU-R. Working Party (WP) 5D is at present getting ready assessment criteria to be trailed by entries of recommendations and assessment of candidate technologies. This procedure is relied upon to be finished by late 2019, prompting the first certified 5G standards. 3GPP distributes major releases roughly once per year. Standardisation of 5G technologies is broken into two stages. Stage 1 will be finished by September 2018 in Release 15. Stage 2 will fuse more capacities to stretch out the abilities of 5G to dynamically bolster more services, case studies and significantly higher frequency bands (e.g., over 40 GHz). Stage 2 will be finished around the end of 2019 in Release 16. IEEE has as of late started a 5G track to supervise the guide of upgrades that will happen for various existing and new IEEE standards, for example, 802.11ax (WLAN), 802.15 (short range communications), 802.22 (Fixed Wireless Broadband), P1914.3 (for Cloud RAN), P1918.1 (tactile and haptic Internet). Standardization roadmaps vary for the individual specification groups. [17]

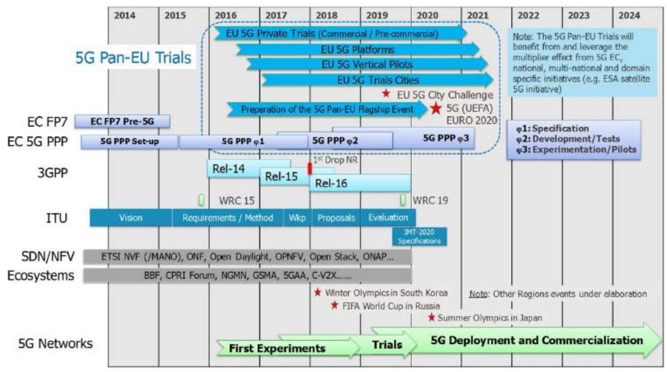

Figure 9. 5G Trials and Standardization Roadmaps [16]

II. Networking and Computing Technologies for Smart Cities

A. Software-Defined Networking

SDN is a generally novel approach to program the switches used in present day networking systems. SDN's uses a centralized control architecture which is better suited to the extremely large networks prevalent in today's mega-scale data centers [18]. The solid coupling amongst control and data planes has made it hard to add new features to existing networks (see Fig. 10). Solving these issues, SDN decouples the control plane from the network devices and becomes an external entity: the Network Operating System (NOS) or SDN controller. [19]

SDN provides extreme flexibility and high programmability. The data plane managed by the controller enables cost-effective and dynamic network configuration in support of smart cities. SDN is being proposed as a networking candidate for smart cities, by extending connectivity to homes using SDN for capacity sharing, securing communications and user mobility management. [2]

B. Network Functions Virtualization

Network Function Virtualization (NFV) has drawn huge consideration from both industry and the scholarly world as a critical move in media transmission benefit provisioning. By decoupling Network Functions (NFs) from the physical nodes on which they run, NFV can possibly prompt huge diminishments in Operating Expenses (OPEX) and Capital Expenses (CAPEX) and encourage the deployment of new services with increased agility and faster time-to-value. Network Function Virtualization (NFV) has drawn significant attention from both industry and academia as an important shift in telecommunication service provisioning.

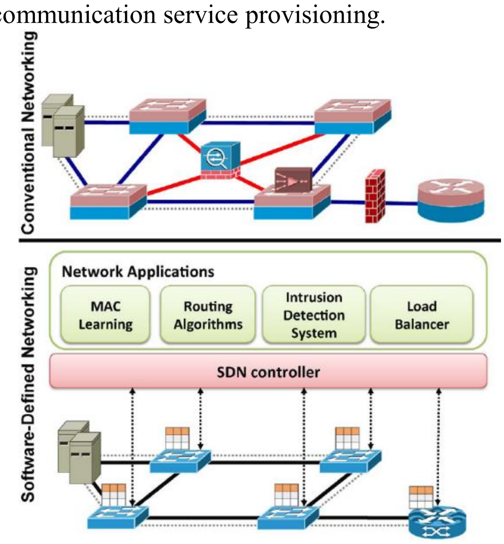

Figure 10. Traditional networking versus SDN. [19]

Connection between NFV, SDN, and Cloud computing is depicted in Figure 11. Each of these fields is a deliberation of various assets: figure for distributed computing, organize for SDN, and capacities for NFV. The points of interest that gather from each of them are comparable; readiness, cost diminishment, dynamism, computerization, asset scaling and so forth. The inquiry isn't whether NFs will be relocated to the cloud, as this is in reality the general thought of NFV. It is whether the cloud will be an open one like Amazon, or if TSPs will want to client private ones appropriated over their infrastructure. In any case, it is to make the cloud carrier-grade in terms of performance, reliability, security, communication between functions and so on. Then again, NFV objectives can be accomplished utilizing non-SDN instruments, and depending on the systems at present being used in numerous server farms. Nonetheless, approaches depending on the division of the control and data forwarding planes as proposed by SDN can improve execution, disentangle similarity with existing infrastructure, and encourage operation and upkeep systems. Similarly, NFV can bolster SDN by giving the framework whereupon the SDN programming can be run. At long last, the cutting edge variation of a data center (the cloud and it's self-benefit perspective) depends on automated management that might be gotten from SDN and NFV. Specifically, functions such as network as a service, load balancing, firewall, VPN could run via APIs. [20]

C. Cloud and Fog/Edge computing

Figure 12 demonstrates the customary Cloud processing structure. Information makers create crude information and exchange it to cloud, and consumers send ask for expending information to cloud, as supported by the blue line. The red dotted line shows the demand for expending information being sent from information consumers to cloud, and the outcome from cloud is spoken to by the green specked line. In any case, this structure isn't adequate for IoT. Data amount at the edge is too big, which will prompt enormous pointless data transmission and registering asset use. Also, the security assurance requirement will represent an impediment for Cloud registering in IoT. Ultimately, most of the end IoT nodes are energy constrained, so releasing some computing tasks at the edge could save their energy.

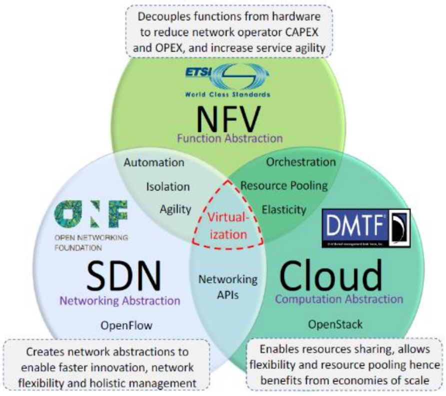

Figure 11. Fog/Edge computing paradigm. [20]

Fog/Edge computing refers to the enabling technologies allowing computation to be performed at the edge of the network, on downstream information in the interest of cloud services and upstream data in the interest of IoT services (see Fig. 13). Edge computing is tradable with Fog computing, yet Edge computing concentrates more toward the Things side, while Fog computing does more around the the infrastructure side. [21]

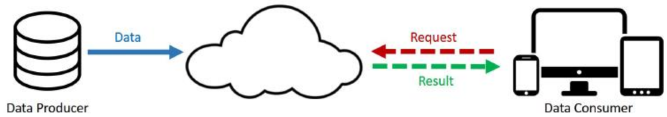

Figure 12. Cloud computing paradigm [21]

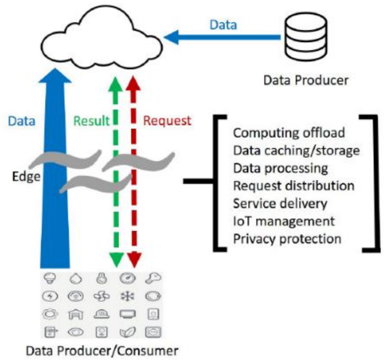

Figure 13. Fog/Edge computing paradigm. [21]

Different sorts of smart city applications can be planned and executed with the help of Cloud and Fog/Edge computing. These include applications for intelligent transportation systems, smart energy systems, infrastructure and environment monitoring, and public safety applications. Table 4 shows some smart city applications and how they can benefit from both the Cloud and Fog / Edge computing. [22]

III. DATA PROCESSING FOR SMART CITIES

A. Database Technologies

Database innovation has experienced over three decades of improvement. Different database frameworks have been proposed for various sizes of datasets and assorted applications. Current relational database systems certainly cannot address the variety and scale challenges required by big data. Due to certain essential characteristics, including being schema free, supporting easy replication, possessing a simple API, eventual consistency and supporting a huge amount of data, the NoSQL database is becoming a solution to solve big data problems. Table 5 shows a comparison of NoSQL databases with different data models such as key-value stores, column-oriented databases, and document databases.

B. Big Data Analytics

1) Techniques for Content Analytics

The data of the substance could be gathered from both social and physical detecting nodes. Social detecting is to gather data by means of web-based social networking, and physical detecting is gathering data through sensors in the physical world. We chiefly concentrate on the famous procedures embraced in social big data analytics, in spite of the fact that the said methods can be utilized as a part of the physical data analytics area.

A distinction exists between utilizing huge data analytics and regular counterfeit consciousness to remove knowledge from information. Manmade brainpower has focused on the improvement of calculations and models. It particularly endeavors to set up however many principles as could reasonably be expected to influence registering nodes to comprehend the data sources and afterward get expected results. The current enormous information approach focuses on the nonstop learning process after the calculations or potentially models are created. This approach particularly concentrates on the issue of how a right arrangement can be created in a brief span (i.e., constrained time). The arrangement is spoken to by the methodologies for getting and applying the outcomes.

Content analytics which isn't another field of study, depends on existing hypotheses and techniques, for example, data mining, machine learning, and measurements and likelihood. From a more extensive point of view, these techniques can be perceived as statistical learning. Despite the fact that these techniques have been changed to meet the reasons and needs in various zones of enormous information issues, for example, item advancement, producing, production network administration, medicinal services applications, promoting, deals forecast, human relationship examination, and so forth., they can be basically arranged in the frame appeared in Fig. 14.

TABLE 4. SMART CITY APPLICATIONS BASED ON CLOUD AND FOG COMPUTING. [22]

Smart City Application	Sub-applications	Fog Roles	Cloud Roles
Intelligent transportation	• Route planning and congestion avoidance • Intelligent traffic light controls • Intelligent parking services • Accident avoidance • Self-driving buses/cars	Fogs in the form of Road Side Units (RSUs) or other computerized units provide low-cost relays among vehicles', roads' and parks' sensors, traffic lights, and the cloud. They provide fast response and control services.	Cloud collects, filters, and stores traffic information. It helps in coordinating city traffic and parking optimizations. It also helps in planning for enhancing traffic systems.
Smart energy	• Smart grid • Smart buildings • Renewable energy plants • Smart meters • Wind farms • Hydropower plants	Fogs provide local controls for energy systems, distribution units, and consumer locations. They also enable smooth integration of different energy systems.	Cloud collects, filters, and stores energy information. It supports decision making for utilizing smart grids and renewable energy features based on collected and analyzed data for consumers' needs and renewable energy productions.
Smart water	• Leakage detections • Water leakage reduction • Water quality monitoring • Smart water meters • Smart irrigation	Fogs provide better and faster local monitoring and controls for smart water networks. They also offer real-time monitoring for faults and leakages and support repair and maintenance operations.	Smart water networks information is collected, stored, and utilized by cloud services to enhance the water networks, production, and quality and to reduce water losses.
City structure health monitoring	Health monitoring for • Bridges • Large public buildings • Tunnels • Train and subway rails • Oil and gas pipelines	Fogs help reduce data traffic between the sensors monitoring the structures and their main control stations. In addition, they provide fast safety controls for some applications.	Cloud collects, filters, and stores structure health information. The cloud can help analyze collected data to enhance the maintenance processes and improve the health of the city structures.
Environmental monitoring	• Air quality monitoring • Noise monitoring • River monitoring • Coastal monitoring	Fogs help enhance environmental monitoring processes by providing smart environmental monitoring closer to the monitored areas.	Cloud provides processes to collectively analyze city environmental and health status.
Public safety and security	• Crowd control for large events (sports games, parades, and outdoor celebrations) • City crime watch and alerts • Large-scale emergency response services (e.g. floods, earthquakes, terrorist attacks, volcanoes, and wars)	Fogs help reduce the communication traffic between these places and the main security monitoring stations.	Cloud provides a powerful platform for analyzing the collected data about the current situation to help in providing possible actions for better controls and emergency relief.

TABLE 5. COMPARISION OF NOSQL DATABASE SYSTEMS. [23]

Data Model	Name	Producer	Data Storage	Concurrency Control	CAP Option	Consistency
Key-Value	Dynamo	Amazon	Plug-in	MVCC	AP	Eventually Consistent
	Voldemort	LinkeId	RAM	MVCC	AP	Eventually Consistent
	Redis	Salvatore Sanfilippo	RAM	Locks	AP	Eventually Consistent
Column	BigTable	Google	Google File Systems	Locks + stamps	CP	Eventually Consistent
	Cassandra	Facebook	Disk	MVCC	AP	Eventually Consistent
	Hbase	Apache	HDFS	Locks	CP	Eventually Consistent
	Hypertable	Hypertable	Plug-in	Locks	AP	Eventually Consistent
Document	SimpleDB	Amazon	S3 (Simple Storage Solution)	None	AP	Eventually Consistent
	MongoDB	10gen	Disk	Locks	AP	Eventually Consistent
	CouchDB	Couchbase	Disk	MVCC	AP	Eventually Consistent
Row	PNUTS	Yahoo	Disk	MVCC	AP	Timeline consistent

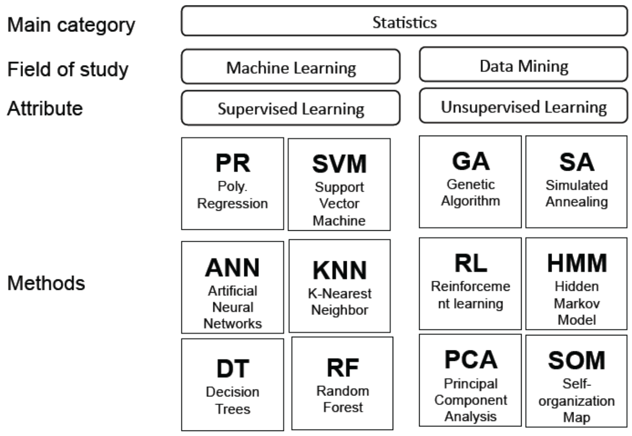

Figure 14. Family Tree of Statistical Learning. [24]

By and large, two fields of study, which are machine learning and data mining, are best executed in the statistical learning process. *Machine learning* predicts a specific result through the info information. An arrangement of calculations is regularly connected to remove data consequently without online human direction. Some of these methodology incorporate thoughts got specifically from or roused by traditional measurements. Most sensible strategies for machine learning can be planned as a formal probabilistic model. Subsequently, machine gaining from this perspective is especially the same as measurements, however it contrasts in that the parameter gauges have less significance and the emphasis is on computational effectiveness and huge datasets. *Data mining* focuses on design disclosure from the raw data earlier/after the procedure of machine learning. Data mining is completed by a man in a particular circumstance, on a specific data set, and on account of an objective. The data set is often big and sophisticated, and may have special problems, which we can expect from raw data. Usually, the goal is either to discover some preliminary insights in an area with little knowledge acquired beforehand or to predict future observations accurately. Note that the goal is generally not to develop a more sophisticated knowledge of the underlying data generating process.

2) Big Data Analytics for Disaster Management

A smart communication network is essentially critical in a disaster happen to a city, since both rescue and recovery greatly depend on the provided communication channels. Notwithstanding, the regular correspondence arrange is delicate once a debacle happens. A worldly correspondence framework, to be specific, an emergency communication network (ECN) of a smart city, must be immediately built to connect people together.

Thinking about the highlights of a disaster (e.g., constrained assets and dynamic changing of condition), it is dependably a key issue to utilize restricted assets viably to give the best response communications. Big data analytics in the hazardous situation gives conceivable answers for comprehend the circumstances occurring in a disaster zones, with the goal that constrained assets can be ideally sent in light of the analysis results. Analysing different stages of disaster such as before and after a disaster, content analytics can support the disaster management as listed in Table 6.

TABLE 6. CONTENT ANALYTICS CAN SUPPORT THE DISASTER MANAGEMENT. [25]

Stage	Possible Results from Content Analysis	Possible Enhancement of ECNs
Before Disaster	We may expect the use of information from social media to: (1) inform the public around or near the scene on how to be prepared if a disaster takes place; (2) inform the public where to seek necessary information if a disaster takes place; (3) provide public confidence that the action plan(s) from the emergency center are capable of conducting a real-time response if a disaster takes place; and (4) keep the public informed on the situation of a disaster.	The above contents can be published by a user or government account. Through analysis of the contents, the situation/distribution of people and resources, the action plan/policy of government can be understood, so that ECNs can be quickly deployed in an optimized way after a disaster occurs.
During Disaster	We may expect the use of information from social media to: (1) provide information on evacuations in specific regions, especially those with limited or blocked communication; (2) keep the public aware of regions that they should avoid; (3) provide the public with information on road closures; and (4) inform the public affected by the disaster about the actions that are being taken to support them.	Through instant retrieval and analysis of social posts, situations during disaster, e.g., (1) a glance of the level of damage in a specific place; (2) a minimum requirement to survive in refuges; (3) the supplies, such as energy, food, and water, needed in a specific area; (4) the communication requirement to optimize ECNs
After disaster	We may expect to use the information from social media to: (1) reunite families who have been separated from each other; (2) inform the public on recovery efforts; (3) assure support of disaster survivors.	We may expect to use the analysis result to: (1) understand recovery situations to optimize communication resources; (2) provide ECNs that can transmit instant messages in areas where survivors need support.

3) Deep Learning for Health Informatics

With a huge convergence of multimodality data, the data analytics in health informatics has developed quickly in the most recent decade. This has likewise provoked expanding premiums in the age of systematic, data driven models in light of machine learning in wellbeing informatics. Deep learning technique with the artificial neural networks, is emerging in recent years as a powerful tool for machine learning, promising to reshape the future of artificial intelligence. Quick improvements in computational power, fast data storage, and parallel processing have also contributed to the rapid uptake of the technology in addition to its predictive power and ability to generate automatically optimized high-level features and semantic interpretation from the input data.

Table 6 outlines the important applications in the five regions of health informatics: translational bioinformatics, medical image processing, sensing, medicinal informatics, and public healthcare.

TABLE 7. SUMMARY OF DEEP LEARNING METHODS BY AREAS AND APPLICATIONS IN HEALTH INFORMATICS. [25]

Area	Applications	Input data	Base Method
Bioinformatics	Cancer diagnosis Gene selection/classification Gene variants	Gene expression MicroRNA Microarray data	Deep Autoencoders Deep Belief Network Deep Neural Network
	Drug design	Molecule compounds	Deep Neural Network
	Compound-Protein interaction RNA binding protein DNA methylation	Protein structures Molecule compounds Genes/RNA/DNA sequences	Deep Belief Network Deep Neural Network
Medical Imaging	3D brain reconstruction Neural cells classification Brain tissues classification Alzheimer/MCI diagnosis	MRI/fMRI Fundus images PET scans	Deep Autoencoders Convolutional Neural Network Deep Belief Network Deep Near Network
	Tissue classification Organ segmentation Cell clustering Hemorrhage detection Tumour detection	MRI/CT Images Endoscopy images Microscopy Fundus Images X-ray images Hyperspectral images	Convolutional Deep Belief Network Convolutional Neural Network Deep Autoencoder Group Method of Data Handling Deep Neural Network
Pervasive Sensing	Anomaly detection Biological parameters monitoring	EEG ECG Implantable device	Deep Belief Network
	Human activity recognition	Video Wearable device	Convolutional Neural Network Deep Belief Network Deep Neural Network
	Hand gesture recognition Obstacle detection Sign language recognition	Depth camera RGB-D camera Real-Sense camera	Convolutional Neural Network Deep Belief Network
	Food intake Energy expenditure	Wearable device RGB Image Mobile device	Convolutional Neural Network Deep Neural Network
Medical Informatics	Prediction of disease Human behaviour monitoring Data mining	Electronic health records Big medical dataset Blood/Lab tests	Deep Autoencoders Deep Belief Network Convolutional Neural Network Recurrent Neural Network Convolutional Deep Belief Network Deep Neural Network
Public Health	Predicting demographic info Lifestyle diseases Infectious disease epidemics Air pollutant prediction	Social media data Mobile phone metadata Geo-tagged images Text messages	Deep Autoencoders Deep Belief Network Convolutional Neural Network Deep Neural Network

4) Big data analytics for the smart grid

The data from smart meters, Phasor-Measurement-Units (PMUs), charging, climate sensors, and other intelligent electronic devices (IEDs) has opened-up a plenty of chances, for example, predictive analytics, demand-side-management, real-time grid awareness, outage detection, asset management, and theft detection to name a few. Big data can help take grid management to another level. For example, expanding demand-response for saving energy has been made possible as a result of enhanced accessibility to customer's energy usage data. In addition, evaluating data from PMUs and IEDs is to maximize safety, ensure service reliability, improve customer service, and prevent outages. Moreover, electric utilities are using predictive analytics on the smart grid data to forecast several indicators that can support running the grid operations efficiently, economically, and reliably. [26]

5) Big Data Analytics for Geolocation Prediction

Geolocation prediction (GP) can be applied to geolocation-based services (GBS). GP is based on Markov-based and Bayesian network-based methods. Mobility Big Data (MBD) rises new challenges and opportunities for geolocation prediction. The geolocation prediction can be divided into three stages as shown in Fig. 15. First, mining popular geolocation region is to pre-process raw geolocation data collected by smart mobile devices; second, mining personal trajectory information; third, building a geolocation prediction model. [27]

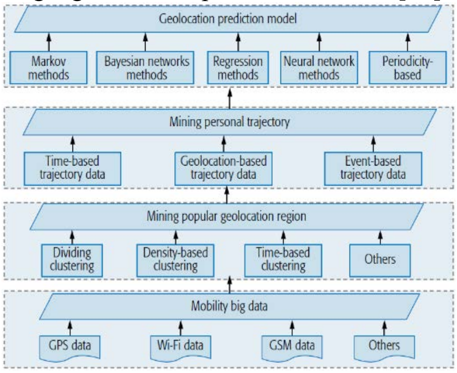

Figure 15. Mobility big data-based geolocation prediction. [27]

IV. PROPOSED SOLUTION AND EXPERIMENTS

A. Inter-Smart Cities Testbed

Our inter-smart cities testbed is to connect smart city testbeds located in Hanoi, Manila, Myanmar. This platform is being connected to SDN testbed (RISE) and IoT testbed in Japan (JOSE). This is to investigate ICT enabling technologies for smart cities such as IoT protocols, SDN/NFV, edge/fog/cloud computing, big data platform, IoT data analytics, and smart city applications (see Fig. 16).

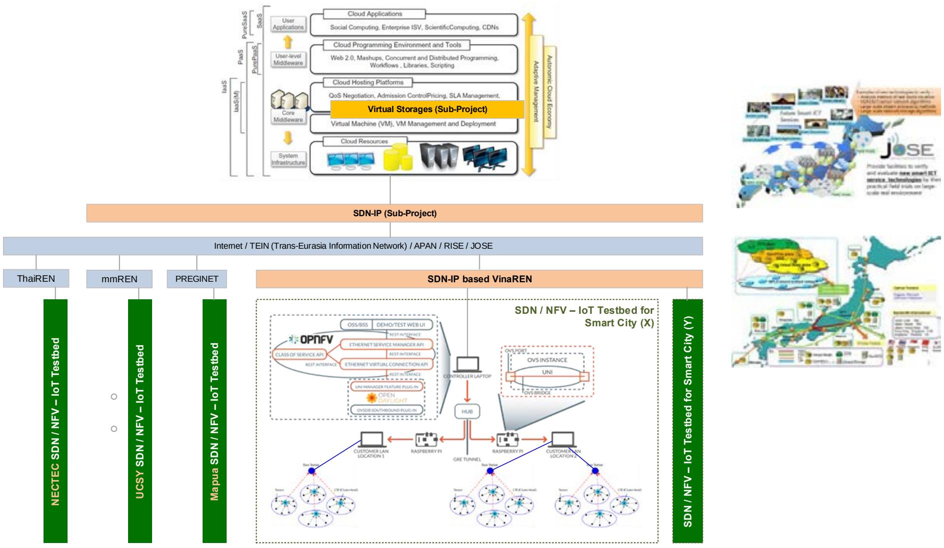

Figure 16. Inter Smart Cities Testbed

B. IoT Gateways, WSNs

In order to compare the pros and cons between MQTT and CoAP protocols, we use Raspberry Pi3 as IoT Gateway, which collects data sensor through ESP8266, using MQTT (see Fig. 16). The messages collected by the gateway from the sensors are usually very small because they contain only the current value of the temperature, humidity, light… measured by the sensor and they are just decimal numbers. This is a very important thing to remember: the gateway collects and operates on a very large number of small messages. The gateways are connected to the Internet using WiFi, or Ethernet. After collecting data sensors, it sends data to the IoT server. In our experiment, we use laptop as a IoT server.

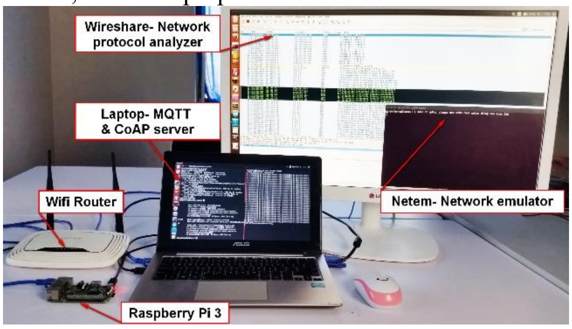

Figure 17. IoT system for testing MQTT và CoAP protocols

Raspberry Pi 3 acts as publisher and subscriber. The data is sent to the server and received using two protocols MQTT and CoAP, with different QoS. The two open source servers used on laptop are Mosquitto and libcoap, and a Python-built program will repeatedly emulate the data received from the sensor, and then send it to the server. and also receive data from the server, then calculate the difference between the time from sending data to receiving. NetEm software is used to create delay, lost in network. To ensure the reliability of the results, each message sent and received is closely monitored by the Wireshark software.

In Figure 17, data flow simulation in the IoT system is used for the experiment. Data published from the IoT gateway, via the LAN or Wifi, which is simulated parameters such as latency, lossy ... with the NetEm software, is sent to the server, and then the data returned from the server to the subscriber through LAN or Wifi.

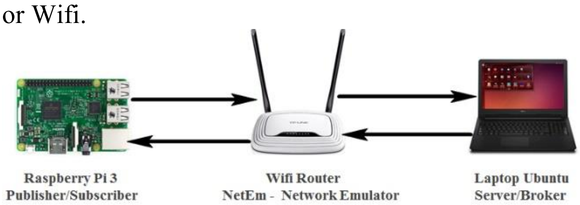

Figure 18. IoT system using MQTT và CoAP

We also tested to send Data from IoT Gateway to IoT server, which is installed IoT Platform Kaa.

C. Networking solutions for smart cities

This model uses the Mininet tool and Opendaylight to simulate the virtual switches and controller. Opendaylight (ODL) is a modular open platform for customizing and automating networks of any size and scale. The Opendaylight Project arose out of the SDN movement, with a clear focus on network programmability. It was designed from the outset as a foundation for commercial solutions that address a variety of use cases in existing network environments.

Mininet simulates 3 virtual switches connected together, each virtual switch has a virtual host associated. The version of Opendaylight used here is Carbon SR1. Through Opendaylight, two networks between two Mininet machines are connected, exchanging data between virtual hosts in the network controlled by Opendaylight. Figure 19 shows a simplified model of the SDN testbed in Hanoi.

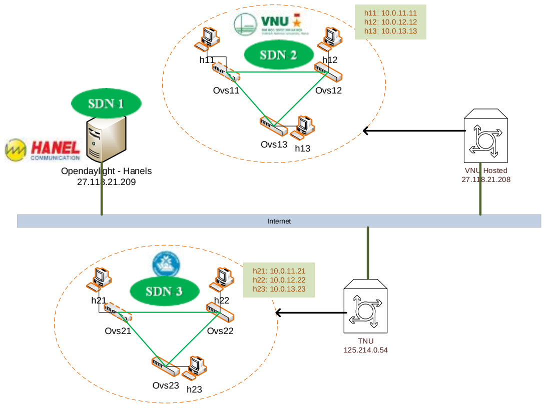

Figure 19. Simplified model of the SDN testbed in Hanoi

D. IoT Platform

Now we will describe about our ITI testbed using Kaa and HDP platform. The Kaa IoT Platform will be used for frontline activities that are real-time data collection across connected physical assets (humidity sensors) and dispatching that data to Cassandra of HDP for further processing and storage. The architecture of the ITI testbed is show in Figure 19.

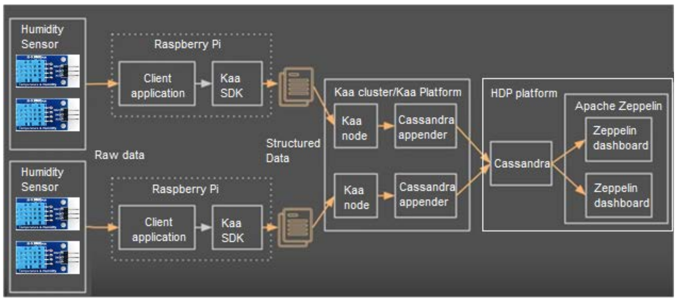

Figure 20. The IoT platform based on Kaa and HDP

In our testbed, we have a Kaa cluster and this cluster supports and handles request from Raspberry Pi application, so that application collects raw data from humidity sensors about relative humidity in air and then it pushes this data using Kaa SDK to the Kaa cluster. The Kaa SDK transfers not raw data but structured data to Kaa node. When the data is transferred to

Kaa node, the Cassandra appender of Kaa platform will used to push this data to Apache Cassandra of HDP. Cassandra appender and all other appenders, which are implemented and supported by the Kaa platform have ability to guarantee data delivery and in case of any delivery and data delivery errors the error message is pushed back to Kaa SDK. When data is pushed into Cassandra we will use Apache Zeppelin of HDP in order to build server dashboard and visualize the IoT data.

V. CONCLUSIONS

In this paper, we review the ICT enabling technologies for data acquisition in the context of smart cities. These technologies include Wireless Sensor Networks, Mobile Ad hoc Networks, Unmanned Aerial Vehicles, Vehicular Ad hoc Networks, 5G. Next, we analyze potential networking and computing technologies for smart cities such as SDN, NFV, Fog/ Edge/ Cloud computing. For data processing in smart cities, it is recommended to deploy scalable IoT platforms with advanced machine learning techniques.

For validating the proposed ICT architecture for smart cities, we have build local testbeds in Vietnam, Philippines, Myanmar which then being connected to SDN, IoT national testbeds in Japan.

ACKNOWLEDGMENT

Authors acknowledge support from the research projects: “ASEAN forum for Software Defined System on Disaster Mitigation and Smart Cities” and “IoT Open Innovation Platform”, which are funded by National Institute of Information and Communications (NICT, Japan) under the ASEAN IVO program (ICT Virtual Organization of ASEAN Institutes and NICT).

REFERENCES

[1] Rida Khatoun *et. al.* “Smart cities: concepts, architectures, research opportunities, “ *Communications of the ACM*, Vol. 59, Issue 8, 2016.

[2] Ammar Gharaibeh *et. al.* “Smart Cities - A Survey on Data Management, Security and Enabling Technologies, “ *IEEE Communications Surveys & Tutorials*, Vol. PP, Issue 99, 2017.

[3] Zesong Fei *et. al.* “A Survey of Multi-Objective Optimization in Wireless Sensor Networks: Metrics, Algorithms and Open Problems, “ *IEEE Communications Surveys & Tutorials*, Vol. 19, Issue 1, 2017.

[4] P. Rawat *et. al.* “Wireless sensor networks: A survey on recent developments and potential synergies, ” *The Journal of supercomputing*, Vol. 68, no. 1, pp. 1–48, Apr. 2014.

[5] Mohammad Abu Alsheikh *et. al.* “Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications, “ *IEEE Communications Surveys & Tutorials*, Vol. 16, Issue 4, 2014.

[6] Hlabishi I. Kobo *et. al.* “A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements, “ *IEEE Access*, Vol. 5, 2017.

[7] Imran Khan *et. al.* “Wireless sensor network virtualization: A survey, “ *IEEE Communications Surveys & Tutorials*, Vol. 18, Issue 1, 2016.

[8] S. Al-Sultan *et. al* .“A comprehensive survey on vehicular ad hoc network,” *Journal of Network and Computer Applications*, Vol. 37, pp. 380–392, 2014.

[9] Khadige Abboud *et. al* .“ Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey, ” *IEEE Transactions on Vehicular Technology*, Vol. 65, issue 12, 2016.

[10] Lav Gupta *et. al.* “Survey of Important Issues in UAV Communication Networks, “ *IEEE Communications Surveys & Tutorials*, Vol. 18, Issue 2, 2016.

[11] Douglas K. McCormick, “802.11ba Battery Life Improvement - Preview: IEEE Technology Report on Wake-Up Radio, “ *IEEE Technology Report*, 2017.

[12] Mugen Peng *et. al.* “System Architecture and Key Technologies for 5G Heterogeneous Cloud Radio Access Networks, “ *IEEE Network*, Volume 29, issue 2, 2015.

[13] International Telecommunications Union Radio (ITU-R), “Framework and overall objectives of the future development of IMT for 2020 and beyond,” *Recommendation ITU-R M.2083*, Sep. 2015, www.itu.int/rec/R-REC-M.2083

[14] Afif Osseiran *et. al.* (Ed.). *5G Mobile and Wireless Communications Technology*. Cambridge University Press, 2016.

[15] Jose Ordonez-Lucena *et. al.* “Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges, “ *IEEE Communications Magazine*, Vol. 55, Issue 5, 2017.

[16] 5G Infrastructure Association (5G-IA). *5G Pan-European Trials Roadmap Version 2.0*. www.5g-ppp.eu, 2017.

[17] Mansoor Shafi *et. al.* “5G - A Tutorial Overview of Standards, Trials, Challenges, Deployment and Practice, “ *IEEE Journal on Selected Areas in Communications*, Vol. 35, Issue 6, 2017.

[18] Paul Göransson, and Chuck Black . *Software Defined Networks - A Comprehensive Approach*. 2nd Edition, Morgan Kaufmann, 2017.

[19] Diego Kreutz *et. al.* “Software-Defined Networking: A Comprehensive Survey, “*Proceedings of the IEEE*, Vol. 103, Issue 1, 2015.

[20] Rashid Mijumbi *et. al.* “Network Function Virtualization: State-of-the-art and Research Challenges, “ *IEEE Communications Surveys & Tutorials*, Vol. 18, Issue 1, 2016.

[21] Weisong Shi *et. al.* “Edge Computing: Vision and Challenges, “ *IEEE Internet of Things Journal*, Vol. 3, Issue 5, 2016.

[22] Nader Mohamed *et. al.* “SmartCityWare: A Service-Oriented Middleware for Cloud and Fog Enabled Smart City Services, “ *IEEE Access*, Vol. 5, 2017.

[23] Han Ho *et. al.* “Toward Scalable Systems for Big Data Analytics: A Technology Tutorial, “ *IEEE Access*, Vol. 2, 2014.

[24] Junbo Wang *et. al.* “Big Data Analytics for Emergency Communication Networks: A Survey, “*IEEE Communications Surveys & Tutorials*, Vol, 18, Issue 3, 2016.

[25] Daniele Ravi *et. al.* “Deep Learning for Health Informatics, “ *IEEE Journal of Biomedical and Health Informatics*, Vol. 21, Issue 1, 2017.

[26] Zakia Asad *et. al.* “A Two-Way Street: Green Big Data Processing for a Greener Smart Grid, “ *IEEE Systems Journal*, Vol. 11, Issue 2, 2017.

[27] Guangxia Xu *et. al.* “A Survey for Mobility Big Data Analytics for Geolocation Prediction, “ *IEEE Wireless Communications*, Vol. 24, Issue 1, 2017.

Dzung Van DINH - Dr. Dzung has over 25 years of experience in ICT R&D, consulting, and training. He works in a number of research areas including network optimization, mobility management, Future Internet, IoT, 5G, and Big Data. Dr Dzung is a Fulbright Scholar at New York University, USA. He has obtained his Ph.D. from the Post and Telecoms Institute of Technology, Vietnam, the M.E. degree from University of Technology, Sydney, Australia, B.E. degree from the Odessa Institute of Telecommunications, the former Soviet Union.

Dr. Dzung led many national research projects, acted as a principle member of international projects at RisTI (Indonesia), NTT, NICT (Japan), LG, ETRI (Korea), and NYU (USA). He was the ICT project leader, trainer, and consultant for VNPT, Saigon Postel, EVNTelecoms, VNU HCM City, Thailand Telecoms, and AIT. He actively contributes to International Telecoms Union (ITU) and APT activities in the roles of Vice-Rapporteur, Vice-chairman of ITU-D Study Group 2. Dr. Dzung published more than 30 papers in national and international journals and conferences. He has been the Deputy Director of Research Institute of Post and Telecoms and the Assistant Director of Vietnam Branch - Korea Information and Communications Society (KICS). Dr. Dzung is the Deputy Director of Information Technology Institute – Vietnam National University, Hanoi (VNU). He has been appointed as an Adjunct Professor at the University of Technology, Sydney. Dr. Dzung’s education background:

Byeongnam Yoon (M'97) He became a Member of IEEE in 1997. He was born in Seoul Korea 15 November 1949. He got the PhD in computer science, Chungnam National University, Dejon city, Korea, 1997. He worked for the Sperryrand UNIVAC as a Computer Specialist 1974 -1978, Samsung as a Manager of Telecommunications Section 1978 -1982, Electronics & Telecommunications Research Institute (ETRI) as a Principal Researcher 1982 – 1999, National Information society Agency (NIA) as a Senior Executive Director General 1999 – 2010, Kyonggi University as an Associate Professor Faculty of Computer Science 2010 - 2016. Global IT Research Institute GIRI) as a President 1999 – current. His research area includes a Telecommunications, Internet, Software, Web programming & security, e-Government, Enterprise Architecture, Work Flow, Information Control Nets.

Le Ngoc Hung received the B.E in computer engineering from Hanoi university of science and technologies, Hanoi, Vietnam, in 1992 and the M.E in computer science from Hanoi national university, Hanoi, Vietnam, in 2000. His research interests are decision making, mobility management, computational moderling methods. He is currently working toward Ph.D degree at Post and Telecommunication Institute of Technology (PTIT), Vietnam.

Uy Quoc NGUYEN has obtained his Ph.D in Russia. He is with the Post and Telecoms Institute of Technology, Vietnam. His research area includes block chain, IoT, Artificial Intelligence.

Khoa Dang PHAN is with the Information Technology Institute, Vietnam national University, Hanoi. His research area includes big data analytics, Artificial Intelligence.

Lam Dinh, PHAM He was born in Vietnam 5 December 1986. He got the MSc in computer science, Thai Nguyen University, Thainguyen, Vietnam, 2010. He worked for Thainguyen University 2008-2016, Information Technology Institute, Vietnam national University, Hanoi, 2016-current as Deputy head of Science, Technology and Training Department. His research area includes Business Processing Management, Work Flow, Information Control Nets, Artificial Intelligence.

Volume 8 Issue 1, January. 2019, ISSN: 2288-0003

ICACT-TACT

JOURNAL

GIRI

Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591

Business Licence Number : 220-82-07506, Contact: tact@icact.org Tel: +82-70-4146-4991