A TIERED BLOCKCHAIN FRAMEWORK FOR VEHICULAR FORENSICS

Marcel C. Ugwu[1], Izunna U. Okpala[2] and Collins I. Oham[3], Cosmas I. Nwakanma[3]

[1]Seamfix Nigeria Limited, Lagos, Nigeria
[2]Department of Communication Arts,
National Institute for Nigerian Languages, Aba, Abia, Nigeria
[3]Department of Information Management Technology,
Federal University of Technology, Owerri. Nigeria

ABSTRACT

In this paper, we present a tiered vehicular forensics framework based on permission BlockChain. We integrate all entities involved in the forensics process and record their interactions in the BlockChain to generate comprehensive evidence for settling disputes and appropriating blame. We incorporate a watchdog entity in our tiered framework to prevent collusive tendencies of potentiality liable entities and to prevent exploitation of evidence. Also, we incorporate a state mechanism to prove the state of a smart vehicle when an accident occurs. Furthermore, we conduct a security analysis to demonstrate the resilience of our framework against identified attacks and describe security mechanisms used to achieve key requirements for vehicular forensics. Finally, we comparatively evaluate our framework against existing proposals.

KEYWORDS

BlockChain, Smart Vehicles, Dispute settlement, Vehicular forensics

1. MOTIVATION AND INTRODUCTION

The existing liability attribution model is not well-adapted for the anticipated *smart vehicles*. This is because compared to modern day vehicles where blame is significantly attributed to the driver when an accident occurs, smart vehicles are equipped with sensors which facilitate independent decision making and therefore underpin a new liability model where blame is also attributed to entities responsible for keeping the vehicle operator such as the vehicle manufacturer, auto-technician and vehicle owner. Given the possibility to share blame among multiple entities and the possibility to remotely interact with the smart vehicle, these entities become motivated to execute rogue actions to evade liability. A solution to mitigate this possibility must keep track of the interactions between potentially liable entities in a way that an executed action cannot be repudiated and ensure that data emanating from a vehicle in the event of an accident must be reliable for making liability decisions and to facilitate the vehicular forensics process.

Previous proposals that address vehicular forensics has relied on eyewitness accounts [1], data recorded in the vehicle's black box [2] and centralized storage of evidence [3].

However, several challenges remain open for smart vehicles including (1) that eye witnesses accounts are hardly reliable for making liability decisions [4], (2) vehicle's black box data only describes the state of the vehicle when the accident occurs and not sufficient for making liability

decisions involving multiple potential liable entities [5] and evidence required for vehicular forensics are stored in centralized servers that are susceptible to a single point of failure [6].

Block Chain [7], a distributed and decentralized ledger technology first proposed by Satoshi Nakamoto is perceived to possess salient features such as immutability, security, privacy, and undeniability. These features make it a veritable technology to address the aforementioned problems.

BlockChain could be public or permissioned [8] and this classification is based on the capabilities of users in the BlockChain network. While public BlockChain permits wide entry and allows every user to distributedly manage the BlockChain network, permissioned BlockChain restricts BlockChain participation to invited members and restricts the management of the BlockChain network to selected network members. Also, compared to public BlockChain, permissioned BlockChain users are known. Given the requirement to keep track of interaction between potential liable entities and appropriate blame to a known entity, we propose a permissioned BlockChain framework for vehicular forensics and liability attribution.

The main contributions of our paper are itemized below:

- We present a tiered vehicular forensics framework for smart vehicles based on permission BlockChain. We demonstrate the efficacy of our proposal via a practical use case scenario.
- We introduce a watchdog entity in our framework to prevent evidence tampering and propose a state mechanism to prove the state of a smart vehicle in event of an accident.
- We conduct a security analysis to demonstrate the resilience of our proposed framework against selected attacks and highlight how key requirements for vehicular forensics are met.
- We comparatively evaluate our proposal against existing BlockChain based proposals for vehicular forensics.

The rest of the paper is organized as follows. We present a review of previous works on vehicular forensics in Section 2. In Section 3, we describe the proposed Block Chain based framework for vehicular forensics and present a use case scenario to demonstrate the efficacy of our proposal. In Section 4, we discuss the security of our proposed framework and comparatively evaluate it against existing Block Chain based framework for vehicular forensics. Section 5 concludes the paper and outlines our future work.

2. RELATED WORKS

In this section, we provide a critical review of already proposed works on vehicular forensics. We describe the works that highlight problems of previous work described in Section 1 and we describe proposed work on vehicular forensics using BlockChain.

2.1. EYE WITNESS ACCOUNT, VEHICLE'S BLACKBOX AND CENTRALIZED STORAGE

The author in [3] proposed an evidence generation protocol to facilitate vehicular forensics. However, the proposed solution relies significantly on the availability of witnesses that are not guaranteed to be available. The authors in [9, 10] proposed a vehicular forensic solution that

relies on the data generated by the vehicle and stored in its black box when an accident occurs. While data stored in a vehicle's black box only presents partial information for liability decision making, we also argue that given the exposure of the vehicle to the internet a rogue entity in the liability model such as a vehicle manufacturer could remotely exploit the data stored in the black box to deny its complicity in the accident. Furthermore, evidence generated are stored in different central servers which pose a single point of failure challenge [6].

2.2. BLOCKCHAIN BASED SOLUTIONS FOR VEHICULAR FORENSICS

The author in [11] proposed Block4Forensic, a BlockChain based vehicular forensic solution for smart vehicles. However, in their work they neither considered the reliability of messages generated by a smart vehicle nor did they consider that liable validators could execute malicious actions to deny their complicity in event of an accident. The author in proposed a BlockChain based liability attribution solution for autonomous vehicles. While their proposal represents an improvement of Block4Forensics [11], they also did not consider the reliability of messages generated by an autonomous vehicle also, their solution is vulnerable to sophisticated collusion attacks where rogue validators could collaborate to exploit the validation process.

3. BLOCKCHAIN BASED FRAMEWORK FOR VEHICULAR FORENSICS

In this section, we describe the proposed BlockChain based framework for vehicular forensics. We begin by identifying the components of the proposed framework. Following this, we present a use case that shows the efficacy of our proposed Blockchain solution for vehicular forensics.

3.1. COMPONENTS OF BLOCKCHAIN FRAMEWORK

In this section, we describe the components of our proposed architecture. The components of our architecture are classified as interacting entities and transactions. We provide a detailed description of these components below.

3.1.1 INTERACTING ENTITIES

The interacting entities in our proposed framework include smart vehicles, auto-technicians, smart vehicle manufacturers, insurance provider, law enforcement, transport authority, and roadside units. Their roles are described as follows:

SMART VEHICLES: They generate data as evidence to facilitate the vehicular forensics process. We assume that smart vehicles possess a tamper-proof device for storing accident-related data and security credentials. For communication of accident related data, we also assume that smart vehicles possess 5G technology [12] for the swift communication of accident-related data to relevant authorities.

AUTO-TECHNICIANS: The auto technicians are responsible for providing maintenance service for smart vehicles. They generate a report after their action on the vehicle as a proof of their interaction with the vehicles.

VEHICLE MANUFACTURERS: Vehicle manufacturers periodically receive sensor data information from smart vehicles and provide updates for smart vehicle sensors when necessary.

INSURANCE PROVIDER: Insurance companies receive data from smart vehicles when an accident-related event occurs for attributing liability. The insurance company also receives complimentary evidence from legal and transport authorities to facilitate liability attribution.

LAW ENFORCEMENT: Law enforcement authorities include police and law courts who use evidence received to make dispute settlement decisions. The law enforcement authorities also provide supporting or complimentary evidence to insurance companies for liability attribution.

TRANSPORT AUTHORITY: The transport authority issues communication credentials to vehicles in a given region for vehicular communication. Vehicular communication involves the interaction between vehicles (vehicle-to-vehicle) and the interaction between smart vehicles and roadside units (v2R). The transport authority is responsible for the management of road side units.

ROADSIDE UNITS: For vehicular forensics, we consider roadside units as witnesses that record accident related events in their line-of-sight and receives accident related data from vehicles that witness the collision event. The roadside unit also contains a tamper-proof device for storing cryptographic secrets for vehicular communication and communication with the transport authority.

The communication between interacting entities occurs either as a direct communication or a Block chain communication. Direct communication in our architecture occurs as a point-to-point communication between two interacting entities. The interaction between operational smart vehicles, between a smart vehicle and a roadside unit or the interaction between a road side unit and a transport authority, is classified as a direct communication. Communication described in the above scenarios is facilitated by the transport authority who provides communication credentials to smart vehicles during their initial registration and the road side units when installed on the roads. For this communication, we use a public key infrastructure where the transport authority is the certified authority and provides digital identities to communicating entities to facilitate authorized and authenticated communications.

Block Chain communication, on the other hand, occurs in two-tiers to facilitate the communication of relevant data in each block chain tier. In the first tier, interacting entities exchange relevant information needed to facilitate the forensics process and make liability decisions. In the second tier, information exchanges in the first tier are analyzed and used for making liability decisions. The roles of interacting entities in both tiers are classified as senders, validators, and monitor. The senders are entities that send data to a Block chain network while validators validate data sent by senders. In the first tier, interacting entities include the smart vehicles, smart vehicle manufacturers, auto-technicians, law enforcement authorities and insurance companies. In the second tier, interacting entities include the insurance companies, smart vehicle manufacturers,

Transport authorities and law enforcement authorities. The senders in the first tier include the smart vehicle, auto-technician and the vehicle manufacturer. The validators include the vehicle manufacturer, insurance companies and the auto-technicians. The law enforcement authority acts as a monitoring entity in tier-1 that keeps track of changes in the state of tier-1 Block Chain. In the second tier, the senders are the insurance companies and the smart vehicle manufacturers while the validators are the law enforcement authority and the transport authority.

We present our proposed Block Chain based framework for vehicular forensics in Figure 1 which describes the interaction between entities in our framework.

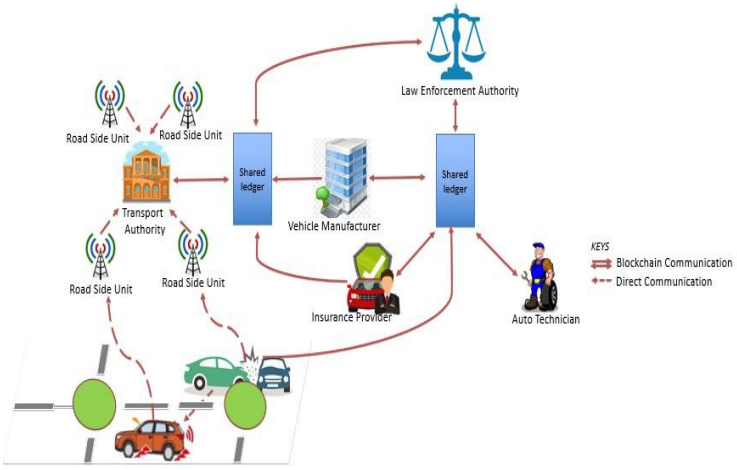

Figure 1. Proposed Block Chain Based Framework

For Block Chain communication, a membership service provider like the certified authority in public key infrastructure provides unique communication credentials including certificates for Block Chain communications to all interacting entities. The verification certificate of the membership service provider (VC) is however stored in the genesis block which initiates the Block Chain. The verification certificate is used by validators to authenticate Block Chain communications. Smart vehicles are envisaged to generate tons of personally identifiable data thus privacy preservation of vehicle owner is paramount in the proposed framework. For this, we assume that the membership service provider issues pseudonyms to smart vehicles which allow them to use unique keys for every Block Chain communication. In the next section, we describe the communications in our proposed framework.

3.1.2 TRANSACTIONS

We refer to communication exchanges between interacting entities in the Block Chain as transactions. The transactions considered in our framework ensures that all interactions contributing to evidence for dispute settlement are stored in the Block Chain. Given that all data contributing to evidence are generated in tier-1, the interactions between potentially liable entities occur in the tier-1 request for more evidence is made in tier-2, we classify transactions in our framework as evidence and request transactions.

EVIDENCE TRANSACTION: The evidence transactions considered in our framework include data generated when an accident occurs, interactions between potentially liable entities such as the interaction between a vehicle manufacturer and a smart vehicle or interaction between an auto-technician and a smart vehicle. To ensure that data generated by a smart vehicle is reliable for making liability decisions, we assume that the vehicle manufacturer locally stores the hash values of all sensors in a smart vehicle and stores the cumulative hash of these sensors in the first tier Block Chain to reflect the state of the Block Chain when manufactured. Post-manufacture interactions with other potential liable tier -1 entity as the smart vehicle becomes operational such as the notifications from a vehicle manufacturer to execute an update on a sensor or the execution of an action that changes the state of a sensor by an auto-technician are recorded in the Block Chain and updates the cumulative hash value of sensors. In the event of an accident, as part of the forensic process, to retrieve complementary evidence on the state of the smart vehicle, the current state of the vehicle is retrieved by extracting the current firmware image from the smart vehicle sensors and computing the cumulative hash value of all sensors. The computed value is then comparatively evaluated against the supposed state in the Block Chain.

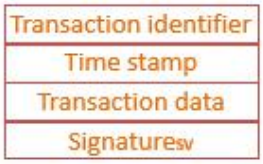

Figure 2. Single-sign Evidence Transaction Structure.

Evidence transactions could be single-signed transactions or *MultiSig* transactions signed by multiple interacting entities. Data generated by a smart vehicle when an accident occurs are single signed and data generated by a tier-1 entity interacting with the smart vehicle such as a vehicle manufacturer and auto-technician are signed by both the data generator and the smart vehicle.

Figure 2 describes the structure of a single sign evidence transaction generated by a smart vehicle when an accident occurs. The *Transaction identifier* is the hash of the transaction contained in the transaction. The *Time stamp* is the event time of occurrence. The *Transaction data* contains the data generated by the smart vehicle when the event occurred. It includes the speed of the vehicle, smart vehicle location, and encrypted witness accounts such as those from neighboring vehicles where the accident occurred or from the road side units. Signature**SV** is the signature of the smart vehicle that generated the transaction. Once generated, the data is sent to the tier-1 validators for verification and validation of the transaction. In contrast to the vehicle generated by a smart vehicle when an accident occurs, transactions generated by a vehicle manufacturer and sent to the smart vehicle also include the signature of the vehicle manufacturer and a metadata field which describes the details of the interaction between the vehicle manufacturer and the smart vehicle.

REQUEST TRANSACTION: The request transaction is a transaction initiated by an insurance company to the tier-2 validators to obtain complimentary evidence such as the decrypted accounts of witnesses to facilitate liability decisions. It is a single sign transaction that includes the transaction data contained in the evidence transaction sent by a smart vehicle in the event of an accident and the signature of the insurance company.

3.2. USE CASE SCENARIO

In this section, we present a use case that describes the efficacy of our proposed framework as a veritable solution for vehicular forensics for smart vehicles. In this use case, we assume that a smart vehicle is involved in a stationary collision in the presence of two operational vehicles called witnesses. Upon colliding with a stationary object, the smart vehicle generates the evidence transaction and stores the perception of the witnesses and sends the transaction to the tier-1 validators. Once received by tier-1 validators, the validators verify the authenticity of the smart vehicle and upon a successful verification, the validators validate the transaction and reach consensus on the state of the current block as described in [5] by computing the hash of the block when a transaction is added to the block until the block reaches maximum capacity. At this point, it is appended to the BlockChain. After a successful validation of the transaction, the insurance company sends a request transaction to the tier-2 validators. Upon receipt of the transaction, the transport authority retrieves the transaction data contained to retrieve the time of event and location of event. Once retrieved, it queries road side units in the location if available for supporting evidence, once retrieved, it collaborates with the law enforcement authority to decrypt the encrypted accounts of users in the transaction data sent by the insurance company. Once decrypted, the law enforcement authority and transport authority cross validate all presented evidence including the evidence retrieved from the road side units. After the cross-validation exercise, they present the complimentary evidence to the insurance company to finalise liability attribution. If a faulty sensor is deemed responsible for the accident, the forensic process would also include the extraction of the firmware of the sensors in the smart vehicle and the computation

of the cumulative hash value of the sensors in the vehicle, if the cumulative value is same as the value in the BlockChain, the vehicle manufacturer or auto-technician is blamed for the accident based on what actor last acted on the faulty sensor. This is achieved by going through all *MultiSig* transactions stored on the tier-1 BlockChain to identify what actor last influenced the state of the faulty sensor. If the value differs, the smart vehicle owner is blamed for its action on the sensor.

4. EVALUATION AND DISCUSSION

4.1. SECURITY ANALYSIS

In this section, we discuss and evaluate the security of our proposed framework. We also comparatively evaluate the framework against proposed Block Chain based architecture for vehicle forensics. We begin by describing the mechanisms that allow our framework meet identified requirements.

INTEGRITY: Each transaction includes the hash of every other field contained in the transaction.

NON-REPUDIATION: Transactions communicated in each Block Chain tier is authenticated and stored in the Block Chain where no entity can repudiate their action.

COMPREHENSIVE EVIDENCE: By keeping track of the interactions between liable entities and the interaction between a smart vehicle and witnesses, we offer comprehensive evidence to facilitate the process of liability attribution.

Next, we demonstrate the resilience of our proposed framework to selected attacks. The following attacks have been identified in our framework and we describe how we prevent them in our proposed framework.

ALTERATION OF EVIDENCE: An evidence submitted in tier-1 is validated and stored in the current block of transactions. However, because the evidence is not yet appended to the Block Chain, a rogue validator such as a vehicle manufacturer or auto-technician could Tamper evidence if it senses that it could be liable for the accident. This possibility would disrupt the consensus process as tier-1 validators would find it difficult to reach consensus on the current state of the block. We prevent this possibility in our framework by allowing the law enforcement authority record validation process outputs which could be used to prevent rogue tendencies from potential liable validators. Also, by cross validating evidence generated from witnesses, our framework is able to identify cases of evidence alteration.

SENSOR ALTERATION: A smart vehicle owner could conduct or permit the conduct of a chip tuning attack as described in [13] for his gains by altering a sensor in his vehicle. Also, a vehicle manufacturer or auto-technician could remotely exploit a sensor in the smart vehicle to evade liability. In our framework, we prevent this attack from the owner's exploit by keeping track of the changes in the state of the smart vehicle's sensors and recording changes in our immutable Block Chain. If the value in the Block Chain differs from the computed value of the current state of the vehicle when an accident occurs, the smart vehicle owner is blamed for its action on the vehicle. From the vehicle manufacturer and auto -technician's point of view, their interaction with the vehicle is also acknowledged by the vehicle owner and recorded in the Block Chain.

COLLUSION: A smart vehicle owner could collude with its vehicle manufacturer in the event of a multiple collision to generate false and misleading information to deny complicity. For this to be possible, the vehicle manufacturer with the permission of the smart vehicle owner would remotely exploit an evidence generating sensor. In our framework, we argue that there is no

incentive for the smart vehicle owner to collude with its vehicle manufacturer due to the following reasons:

- When data from the vehicle is cross verified against other accounts from vehicles or roadside units, the discrepancies in reports would be identified; and

- If after the cross-verification exercise and the vehicle is deemed liable due to a faulty sensor. The feedback is sent to the insurance company whose adjuster along sides forensic investigators computes and compares the cumulative hash values of the sensors in vehicle with the state of the vehicle in the Block Chain. As stated in Section 3.2, if the value differs, the vehicle owner is blamed.

4.2. COMPARATIVE EVALUATION

In this section, we compare our proposed framework to Block4Forensic [11] and the proposed BlockChain based framework in [5] for dispute settlement and liability attribution. Table 1.0 presents the comparative analysis and reflects the strength of our proposed framework to existing BlockChain based framework for dispute settlement.

Table 1. Comparative Evaluation of our Framework against existing BlockChain Architectures

Evaluation criteria	Our proposal	Block4Forensics [11]	Proposed BlockChain framework [5]
Proof of vehicle state	By storing the state of smart vehicle sensors on the BlockChain, we prove the state of the sensors in a smart vehicle and identify cases of sensor exploitation.	Not possible.	Not possible.
Proof of interaction	By keeping track of the interactions between liable entities and storing it on the BlockChain, we identify a case of instruction negligence.	Not possible	Possible
Proof of BlockChain state	The monitoring entity in tier-1 BlockChain, also keeps track of changes of the state of the BlockChain after a successfulvalidation. This possibility makes it difficult for colluding entities to exploit the state of the BlockChain.	Not applicable	Partially possible.

5. CONCLUSIONS

In this paper, we present a tiered Block Chain based framework for vehicular forensics. We introduce a watchdog entity in our proposed framework to prevent the possibility of evidence alteration and state management mechanism that ensures all changes in the state of the smart vehicle is recorded in the Block Chain to prevent unauthorized vehicle sensor tampering. We present a use case to demonstrate the strength of our proposed framework and conduct security analysis to demonstrate the resilience of our framework against identified attacks. Furthermore,

via comparative analysis, we demonstrate the strength of our proposed framework against existing Block Chain based frameworks. In the future, we will develop a prototype implementation of our proposed framework to understand its performance in real-world scenario.

REFERENCES

[1] C. P. Young, B. R. Chang, J.J. Lin and R. Y. Fang, Cooperative Collision Warning Based Highway Vehicle Accident Reconstruction. Eight International Conference on Intelligent Systems Design and Applications. 2008.

[2] C. Anderson, and D. Robbins, Toyota secretive on blackbox data. Also available on: http://www.drive.com.au/motor-news/toyotasecretiveon-black-box-data-20100305-14bi0.html March 2010.

[3] J. Fuentes, A. Tablas, A. Ribagorda, Witness-based Evidence Generation in Vehicular Ad-hoc Networks. ESCAR, 2009.

[4] S. Rahman and U. Hengartner, Secure Crash Reporting in Vehicular Adhoc Networks. University of Waterloo, 2017.

[5] C. Oham, S. S. Kanhere, R. Jurdak and S. Jha, A Blockchain Based Liability Attribution Framework for Autonomous Vehicles. Also available on: https://arxiv.org/abs/1802.05050

[6] Z. Liu, J. Ma, Z. Jiang, H. Zhu and Y. Miao, LSOT: A Lightweight Self-Organized Trust Model in VANETs. Mobile Information Systems, 2016.

[7] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. 2008.

[8] A. Kulkarni, How to Choose Between Public and Permissioned Blockchain For Your Project. Also available on: https://blog.chronicled.com/how-to-choose-between-public-andpermissioned-blockchain-for-your-project-3c5d4796e3c8

[9] Y. Kopylova, C. Farkas, and W. Xu, Accurate Accident Reconstruction in VANET. Data and Applications Security and Privacy XXV. Springer Berlin Heidelberg, 2011. 271-279.

[10] Richard Boon, Post-accident Analysis of Digital Sources for Traffic Accidents. 21st Twente Student Conference on IT, June 23rd, 2014, Enschede, The Netherlands.

[11] M. Cebe, E. Erdin, K. Akkaya, H. Aksu and S. Uluagac, Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. Also available at: https://arxiv.org/pdf/1802.00561.pdf 2018.

[12] L. Nkenyereye, J. Kwon and Y. Choi, Secure and Lightweight Cloud-Assisted Video Reporting Protocol over 5G-Enabled Vehicular Networks.Sensors, MDPI 2017.

[13] A. Wasicek and A. Weimerskirch, Recognizing Manipulated Electronic Control Units. 2014.

AUTHORS

Marcel Ugwu is a software engineer by profession and holds a First Class Bachelor's degree in Information Technology from Federal University of Technology Owerri. Marcel works as a tech lead at Seamfix where he leads a development team, architect and drive software development. He loves to write code at least 40% of the time. His current work is on the application of BlockChain in the vehicular network domain.

Okpala Izunna Udebuana is currently a Graduate Research Assistant in Communication Arts department of National Institute for Nigerian Languages, Aba, Abia State, Nigeria. He's an ardent researcher, enterprising software developer passionate about Africa's Tech advancement. He does research on Artificial Neural Network, Machine Learning, IOT and IOE, Blockchain Technology, Natural Language Processing, cyber security, Computer speech production and recognition, Fuzzy Logic, Data Mining, Decision Support system and Executive support system

Collins I. Oham is an undergraduate student of the Federal University of Technology, Owerri, Nigeria. His research interests focus on computer networks and process optimization. He is currently working on adopting Blockchain as a distributed solution for trust management in business processed and large scale networks.

Engr. Nwakanma, Ifeanyi Cosmas is a lecturer at the Federal University of Technology, Owerri Nigeria where he coaches and mentors undergraduate students of the Department of Information Management Technology. Specifically, he teaches Business Telecommunication, Data structure and Algorithm, Systems Evaluation and Implementation, C++ Programming and Introduction to Telecommunication Technology. He worked for about three years in First bank of Nigeria PLC prior to joining the lecturing profession Nine years ago (2009). He has a degree in Communication Engineering, Masters in Information Technology and an MBA in Project Management Technology. He is about concluding his PhD in Information Management Technology. He has over 25 articles and Conference papers to his credit