Blockchain Enabled Intelligent Digital Forensics System for Autonomous Connected Vehicles

Ranu Tyagi
Department of Computer Science and Engineering
Graphic Era (Deemed to be University)
Dehradun, Uttarakhand, India
rxsharma95@gmail.com

Sachin Sharma
Department of Computer Science and Engineering
Graphic Era (Deemed to be University)
Dehradun, Uttarakhand, India
sachin.cse@geu.ac.in

Seshadri Mohan
System Engineering Department
University of Arkansas at Little Rock
Little Rock, Arkansas, USA
sxmohan@ualr.edu

2022 International Conference on Communication, Computing and Internet of Things (IC3IoT) | 978-1-6654-7995-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/IC3IOT53935.2022.9767987

Abstract— **Autonomous connected vehicles are revolutionizing the automotive industry vision and impacting their business model. This trend will likely impact other related industries and their business model such as automotive insurance companies, tier-II automotive manufactures, and automotive maintenance service companies. The growing number of connected vehicles will require new policy formulation by the government about privacy and security issues in the era of massive digitalization and automation. Organizations such as 3GPP and IEEE are evolving standards that address security issues for connected vehicles. However, since Artificial Intelligence (AI) and Machine Learning (ML) will play a significant role in 5G networks and beyond, we address the privacy and security issues with a blockchain-based intelligent digital forensics system for autonomous connected vehicles (ACVs) in a connected smart world incorporating artificial intelligence. The proposed system includes a novel algorithm for the autonomous connected vehicles and the users' security and privacy. We utilize short randomizable signatures to anonymously authenticate witness's identities and to protect the witnesses' privacy. Then, we leverage fine-grained access control based on ciphertext-policy attribute-based encryption for evidence access and evaluate the feasibility of the proposed system by simulating the proposed model, its computational costs and communication overhead by implementing a prototype on a local Ethereum blockchain network platform. The simulation results show the proof-of-concept of the proposed system. We envision the application of the proposed system to ensure security and privacy of ACVs and their security applications for use with 5G-V2X and future XG-V2X networks.**

Keywords— Autonomous connected vehicles, blockchain, digital forensics, privacy and security

I. Introduction

Autonomous connected vehicles (ACV) have capabilities to manoeuvre around without any human intervention. The variety of heterogeneous sensors in vehicles sense and process the input digital data and navigate it automatically with accuracy, reliability and accountability of vehicle and driver safety from any type of collisions. When the digital data is being communicated among multiple control system in the vehicle, there can be a number of ways to launch threats and carry out attacks to interefere with the system functions [1]. Digital data forensic offers a way to record an incident, increase the reliability and trust in the system, and avert threats [2]. In this paper, we focus on the development of blockchain based intelligent digital forensics system for ACVs where blockchain consists of variable blocks to keep the incident data with their timestamps. However, complex computational processes are involved that consume considerable power and resources of the ACVs [3]. The proposed AI-based system is a hybrid system with both centralized and distributed systems, where the centralized system helps to provide the pool of resources and the decentralised system helps to increase the energy efficiency.

The proposed system eliminates the actual bitcoin concept and offers a new advanced system. In the proposed system, each incident is stored in a new block in the decentralized system and until a legitimate observer such as a law enforcement agency or an insurance agency requests the proof of the incident, the data will not be uploaded to the centralized system. To calculate the hash value, the incident is recorded in the new block of the decentralized system and the neighbouring vehicles that were present at the time of the incident as witnesses of the incident so that when an observer investigates the case, the hash value has the incident record with their witnesses' data. The hash value will be generated when an unfortunate incident such as an accident occurs and the witnesses will be created at that time. Otherwise, for regular purposes the process of digital data communication will continue as usual. This innovative approach in autonomous connected vehicles involves numerous sensors, processors, and smart controllers so the storage and validation of incident data will be a time consuming process. The new generation vehicles will consist of on-board diagnostic devices to retrieve the vehicle characteristics data that can be utilized in digital forensics. For example, when an incident occurs then an observer who investigates the incident will try to find out as many possible ways that caused the incident by utilizing the data associated with the witnesses [4]. In autonomous connected vehicles, where everything is automated and dependent on fast and efficient computation, there should be a mechanism to store an account of the incident through a digital record of the incident with witnesses to figure out the incident details. The physical evidences may not work in some cases as there are many stakeholders such as passengers, insurance companies, vehicle manufacturers and law enforcement bodies involved and get affected, compensated or penalized based on the incident report [5]. The blockchain based digital forensics system will help to figure out the actual report of the incident without any bias. Since numerous sensors and witnesses are involved in the creation of the digital record of the incident, AI and ML will play a significant role in data mining possibly terabytes of data to gather accurate and useful record information regarding the incident. The ITU-T Focus Group on AI for Autonomous and Assisted Driving (FG-AI4AD) has formulated 'The Molly Problem' [16], [17] stated as follows: "A young girl called Molly is crossing the road and is hit by an unoccupied self-driving vehicle. There are no eye witnesses. What should happen next?" This scenario and others can be addressed by our proposal for conducting blockchain-based intelligent digital forensics.

The rest of this paper is organized as follows: Section II discusses the key role of blockchain based digital forensics for autonomous connected vehicles. Section III describes the proposed system for autonomous connected vehicles. Section IV presents the experiments and results and an analysis. Section V presents the conclusion of this paper.

II. Blockchain Based Digital Forensics For Autonomous Connected Vehicles

The process of blockchain based digital forensics has five phases which includes 1) digital data collection, 2) digital data pre-processing, 3) digital data witness examination, 4) digital data analysis, and 5) digital data reporting, as shown in Fig. 1.

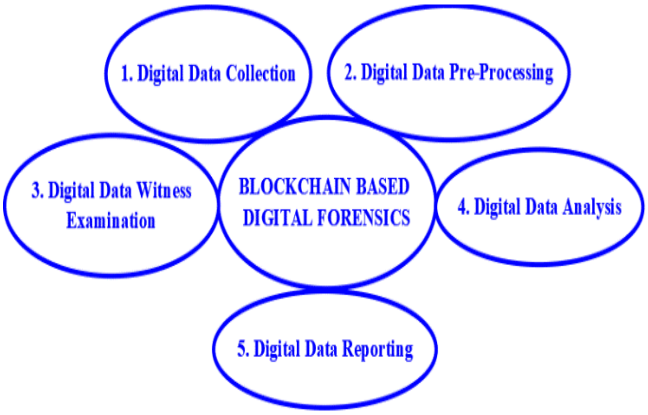
1. Digital Data Collection
2. Digital Data Pre-Processing
3. Digital Data Witness Examination
BLOCKCHAIN BASED DIGITAL FORENSICS
4. Digital Data Analysis
5. Digital Data Reporting

Fig. 1. Five phases of blockchain based digital forensics.

- **Digital data collection:** In digital data collection phase, a law executor or observer collects every possible data related to the incident from the heterogeneous set of sensors and devices. The collected data is stored on a secure cloud platform [6].
- **Digital data pre-processing:** In digital data pre-processing phase, an observer searches the appropriate data related to the incident on the secured cloud platform [7].
- **Digital data witness examination:** In digital data witness examination phase, an observer verifies the incident related data with the concerned witnesses [8].
- **Digital data analysis:** In this phase, an analysis correlating witness digital data with the incident data occurs in order to find out the relevant information.
- **Digital data reporting:** In the last phase of digital data reporting that follows digital data analysis, a report is prepared that serves as the final observation report of the incident.

The privacy of the digital witnesses is a critical factor for the observer, witness and victims and the proposed system ensures that the stakeholders can trust the system. Blockchain provides the support and privacy in incident report retrieval from the secured cloud. Blockchain-based system provides the evidence on trusted platform by incorporating the multi heterogeneous signature scheme by different devices and guaranteed tractability. This process inhibits unauthorized entities to enter into the cloud-based storage system and corrupt the stored data.

III. Blockchain-Based Intelligent Digital Forensics System For ACVs

The proposed system is based on an artificial intelligence algorithm to provide more privacy in blockchain-based digital forensics system for ACVs. The issue of privacy must be addressed to provide witness anonymity and witness location. The proposed system will provide the accountability to digital data using secure cryptographic technique and encrypted high computation at multiple ends. The combination of artificial intelligence and blockchain technologies reduces the process time and computation delay. ACVs generate large volumes of valuable digital data concerning vehicle performance, behaviors of passengers, vehicle and passenger insurance companies, vehicle maintenance companies, and driving history of vehicles. The proposed system inhibits the possibilities for tampering the data and conducting malicious activities to distort digital data evidence of ACVs. The proposed system guarantees victim traceability with enough number of evidence along with digital reports. The main objective of the proposed system is to identify the possible disputes from the different parties and prepare the secured digital forensics report with sufficient number of witnesses to resolve any ongoing or future disputes concerning the incident. The deployed sensors and features of heterogeneous devices will help to prepare a comprehensive digital forensics analytic report for multiple parties about the incident. The proposed system is described through the following steps:

1. Extraction of possible adapted features: In this step, we first search for possible adapted features related to the incident in digital data of autonomous connected vehicles for digital forensics report using artificial intelligence algorithm. The list of possible adapted features is the following:

i. Integrity: It is one of the important features to resolve the dispute among the multiple stakeholders.

ii. Flexibility: To provide the flexibility to all participating witnesses and physical devices is one of the key factors in digital information extraction.

iii. Accountability: It enhances the trust on the system among different stakeholder. The digital data collection with accuracy about the incident helps to increase accountability with the help of the proposed system.

iv. Feasibility: The feasibility in data collection from heterogeneous devices and sensors helps in accurate data processing and preparing an accurate account of the incident in the digital forensics report.

v. Security: The security of digital data related to the incident and witness is one of the important features.

vi. Privacy: The privacy of witness devices and their data is one of the key features in this step.

vii. Trust: The trust development among multiple authorities and stakeholders in digital forensics report is one of the key features.

viii. Comprehensive digital forensics reporting: This is one of the important features required to identify clues, however insignificant they may appear to be at first, related to the incident and search for the faulty party. The comprehensive reporting helps to understand the vehicle behavior and its physical condition that could play a major role in identifying the victim and the offender of the incident.

Artificial intelligence consists of various learning techniques. In this step, the Boltzmann Restricted Machine (RBM) is used as a generative stochastically artificial neural network that can distribute its inputs in a likelihood. In the forward transitive process, each input value F= F1, F2, and F3 merges with weight W1, W2 and W3 and bias. The result is then transmitted to the hidden layer. In the backward process, each activation merges with weight and bias. The result is then forwarded to the visible layer. In the visible layer, divergence is used to compare the quality based on the input and output analysis (Fig. 2).

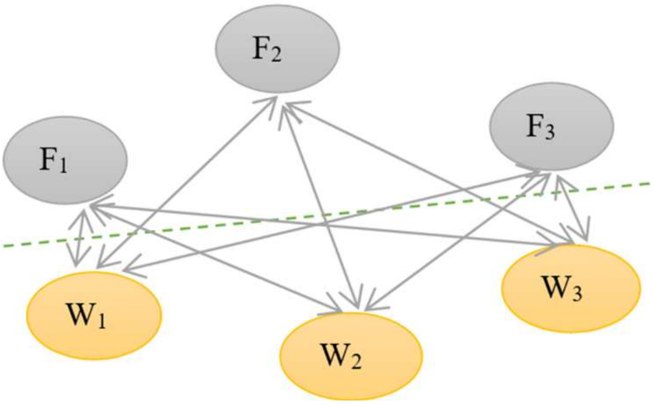

Fig. 2. Adapted features extraction using the weights of the inputs.

2. Identification of possible stakeholders: In this step, the proposed system searches for possible stakeholders and evaluates their role with regard to the incident. The key feature of the proposed system is based on the triggered system where the observer generates the trigger based on the digital data forensics report to the concerned stakeholders. In general, all heterogeneous devices installed in the autonomous connected vehicles do not disclose their data to any authority until it is approved by the service provider. The service provider only gives access to the observer when the incident occurs. It is very important in terms of privacy maintenance and accountability of the system [9]. The vehicle manufactures, vehicle insurance providers and vehicle maintenance service providers may collect vehicle related data at a certain frequency and digital data is encrypted and hash function of each transaction is shared with the blockchain for the proposed digital forensics system. The confidential data of autonomous connected vehicles can be stored in a personal cloud platform.

3. Encrypted digital forensics report preparation: When an incident occurs, the proposed system assigns one node as an observer and multiple slave nodes as report generators among Road Side Units (RSU's) or other vehicles [10]. This process is encrypted and, consequently, the enabled nodes can access the vehicle data only with the service provider permission. An observer node issues trust certificate to multiple nodes for access to their digital data. When an incident occurs. the concerned nodes restore the data of relevant nodes with their last locations and the latest communicated messages among sensors for the purpose of observation. For example, the traffic lights were working fine at the inter-section but the incident occurs due to the failure of sensor communication networks in the autonomous vehicle. The failure may be the fault of the vehicle manufactures and/or network service providers. Digital data forensics system helps in the search and determination of faulty parties and inspire different stakeholders to improve their existing systems based on the system generated report [11]. This encrypted digital forensics report consists of videos or other pertinent information to recreate the chain of events that led to the incident. The blockchain infrastructure facilitates the victims and witness nodes management and incident related data storage issues. The software development kits, various sensors, road side units and on-board units play important roles to facilitate the preparation of reliable and secured digital forensics report. The AI system learns from the past experiences and identifies possible features to extract and prepare the digital forensics report. When an incident occurs, the AI system searches for different sensors deployed near the incident and collects digital data from them for evaluation. AI system can help in increasing the safety of vulnerable pedestrians on the road and provide a solution to the Molly problem. Deep learning neural network helps in visual representation of future risk and decision making in autonomous connected vehicles. This advanced technology can be helpful in quickly searching for the location of the offender, the victim, and the witnesses after the incident occurs. It also plays an important role in data fusion and digital data filtering from multiple sensors in autonomous connected vehicles. In this step, multiple filters such as Bayesian filter, Kalman and Particle filter are used for digital data filtration, and efficient computation. Kalman filter provides discrete linear prediction state estimator algorithm. The Bayesian filter facilitates a recursive frame for efficient computation in the dynamic environment involving an incident. The particle filter is based on the non-linear decision algorithm to deliver offenders, victims and witness location to observer in real-time. The forensics system will activate or trigger the relevant digital data collection related to the incident and prepare report accordingly.

The blockchain technology facilitates five critical nodes to provide security in information exchange among autonomous connected vehicles [12]. The five critical nodes are witness, victim, offender, observer, and validator. A validator node is assigned to vehicle insurance companies, passenger insurance companies, vehicle manufacturers, and vehicle maintenance garages. An observer node is assigned to law enforcement authorities. An offender, victim, and witness nodes are assigned just after the incident occurs based on the forensics report outcome. This blockchain technology is very helpful to ensure that trust prevails over the network of different stakeholders [13].

The blockchain allows public users to involve themselves in the process for validation and verification of results. The communication among the heterogeneous components may strictly be controlled by facilitating privacy membership services among trusted authenticated users [14]. It allows the validity certification for internal communication and helps in validation of information data transactions. The overhead issue in communication and storage may occur during the authentication process [15]. This issue may be resolved by utilizing the distributed ledger of blockchain to keep the digital forensics proofs of the incident. These digital proofs may be shared with multiple trusted authorities for investigation purposes. The trusted authorities involve police, prosecution atorney, defense attorney, a judge and digital forensic report analyst [Fig.3]. The followings components are part of this proposed system

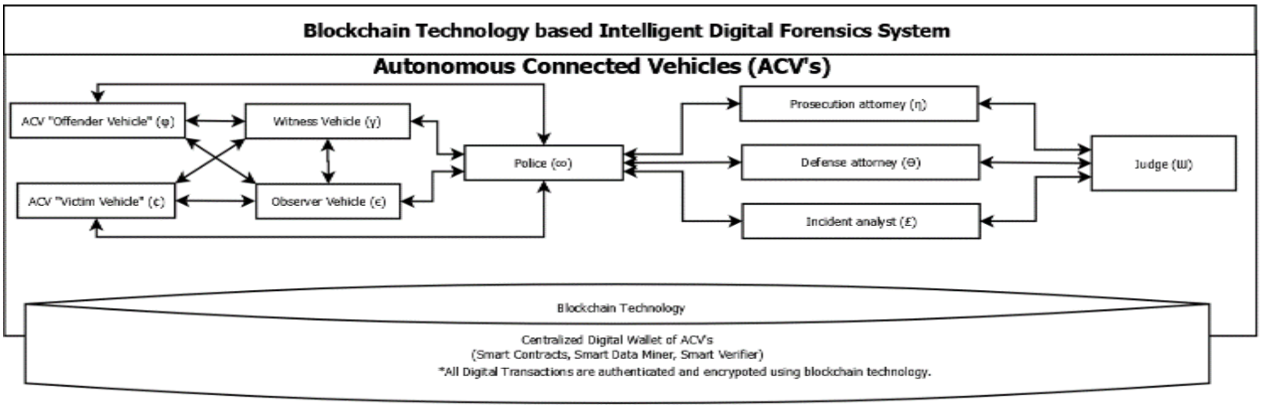
Blockchain Technology based Intelligent Digital Forensics System
Autonomous Connected Vehicles (ACV's)
ACV "Offender Vehicle" (φ)
Witness Vehicle (γ)
ACV "Victim Vehicle" (¢)
Observer Vehicle (϶)
Police (∞)
Prosecution attorney (η)
Defense attorney (ϴ)
Incident analyst (£)
Judge (Ш)
Blockchain Technology
Centralized Digital Wallet of ACV's
(Smart Contracts, Smart Data Miner, Smart Verifier)
*All Digital Transactions are authenticated and encrypoted using blockchain technology.

Fig. 3. Blockchain based intelligent digital forensics system.

Victim (¢): It provides the allegations with evidences to the police.

Observer (϶): It extracts the valid and authenticated information from multiple witness nodes nearby the incident place.

Offender (φ): It has allegation as per the victim report to police.

Witness (γ): It has all the crucial information stored related to the incident scene.

Police (∞): It communicates with the observer about the evidence report and matches with the incident report.

Prosecution attorney (η): It raises the charge during case trial and upload relevant documents in the repository.

Defense attorney (ϴ): It pleads during the case trial court trial and upload relevant documents in the repository.

Incident analyst (£): It analyzes evidence, discover new evidence and send report to police.

Judge (Ш): It studies and verifies the observer report with the other possible circumstances and declares the appropriate result.

IV. Experiments And Results Analysis

The proposed system needs to validate the observer digital signature in digital forensics report with the detailed factual information about victims, witness, and offender before broadcasting the report to law enforcement authorities. The prediction of the various nodes location can be done by linear or non-linear estimators. We simulated the proposed model in OMNeT++, and SUMO with different scenarios using a local Ethereum blockchain network platform [17]. These open source tools helped to provide several interesting results concerning the efficiency of the systems. In simulations, the following parameters have been observed at different steps: observer data security, authentication, access control, witness location privacy, integrity, availability, auditability, access control, and traceability. We have taken 100 nodes for victims, 100 nodes for witnesses and 100 incident analyst nodes, 100 observer nodes, 100 police nodes, one judge node, one defense lawyer node and one prosecutor lawyer node on local host machine with Intel 10th Gen. i7-10750HH, 15.6" FHD Workstation Laptop (16GB/256GB NVMe SSD + 1TB HDD/Windows 10 Pro/Nvidia and Visual Studio 2019. The witness nodes provided more than 50 evidences and incident analysts processing evidences repeatedly. We used Ethereum, Ripple and Corda as blockchain platforms. The new block creation time was set to 1 sec. The transaction is generated randomly and authentication signature is verified by police node. The contract is triggered by virtual node once the transaction is initiated by observer node for digital forensics purpose. There are different states introduced for transition of data from one node to another. Those are: evidence collection (c), evidence verify (v), evidence uploading (u), evidence rejection (r), evidence storage (s), and evidence access (a). At each state transition digital signature is attached for the purposes of verification. Table I lists the simulation time consumed by different components. Table II explores the list of the simulation time consumption in different states.

Table I: Simulation time consumption by components.

Components	¢	ϵ	φ	γ	∞
Time (ms)	5.5	10.2	17.8	19.6	14.8
Components	η	ϴ	£	Ш	
Time (ms)	20.9	12.6	15.5	25.7	

Table II: Simulation time consumption by states.

States	c	v	u	r	s	a
Time (ms)	25.5	30.2	37.8	29.6	24.8	30.9

Fig. 4 depicts time consumed by digital evidences collection. Witness, victim and observer consume time of 25.5 ms, 20.3 ms and 12.5 ms, respectively, at a maximum number of hundred digital evidences.

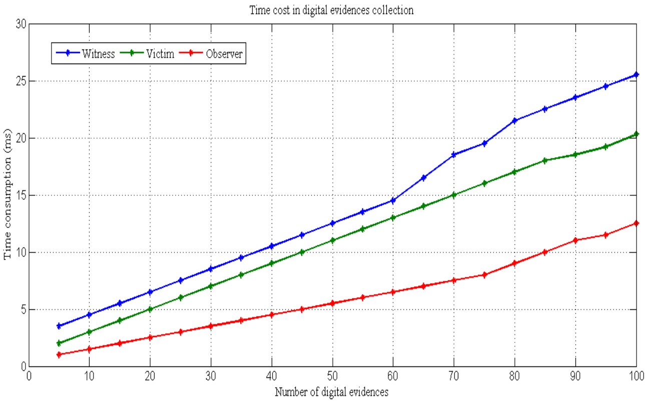

Fig. 4 Time cost in digital evidences collection.

Fig. 5 pictures the time cost in evidence digital data verification. An observer, police and analyst consume time of

30.2 ms, 18.3 ms and 10.5 ms, respectively, at a maximum number of hundred digital evidences.

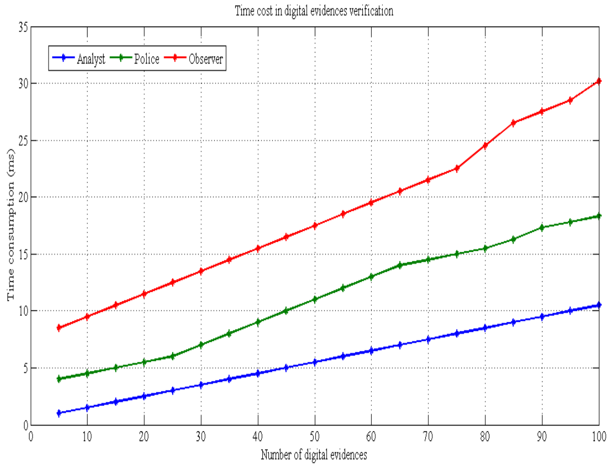

Fig. 5 Time cost in digital evidences verification.

Fig. 6 graphs the time cost in digital evidences uploading. A police and analyst consume time of 37.8 ms, and 17.8 ms, respectively, at maximum number of hundred digital evidences.

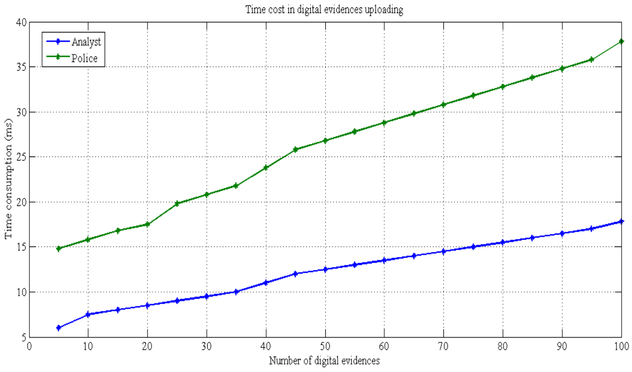

Fig. 6 Time cost in digital evidences uploading.

Fig. 7 provides time cost in digital evidences rejection. A police, and analyst consume time of 37.8 ms, and 17.8 ms. Respectively. at a maximum number of hundred digital evidences.

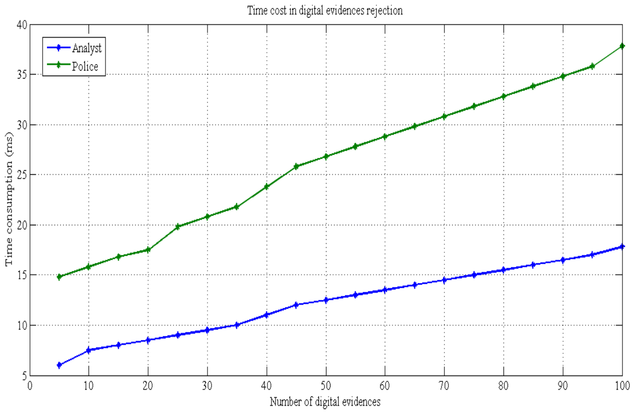

Fig. 7 Time cost in digital evidences rejection.

Fig. 8 provides the time cost in digital evidences storage. An observer, police and analyst consume time of 29.6 ms, 19.8 ms and 9.8 ms, respectively, at maximum number of hundred digital evidences.

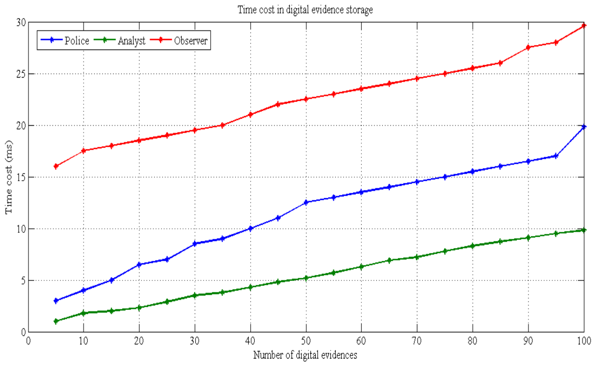

Fig. 8 Time cost in digital evidences storage.

Fig. 9 explores the time cost in digital evidence access. A police, and judge consume time of 24.8 ms, and 14.8 ms. Respectively. at maximum number of hundred digital evidences.

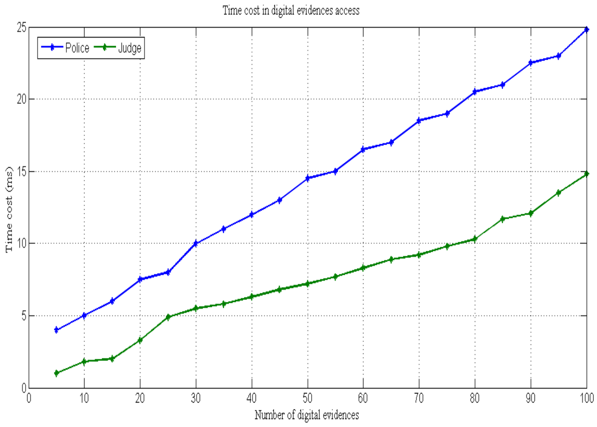

Fig. 9 Time cost in digital evidences access.

Fig. 10 pictures the network latency in evidence uploading. It consumes a time of 8 ms maximum at hundred experiments.

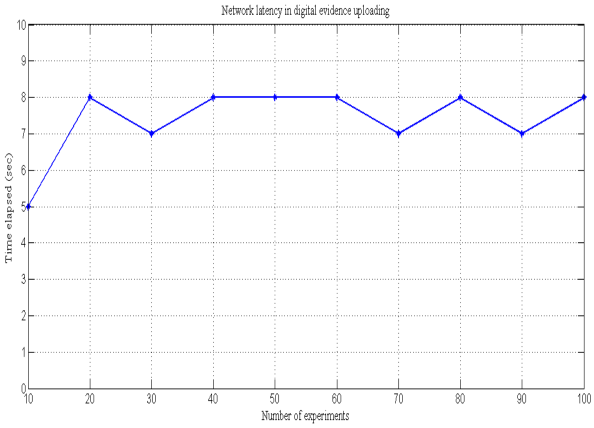

Fig. 10 Network latency in digital evidence uploading.

Fig. 11 depicts the network latency in digital evidence access. It consumes time of 5 ms maximum of hundred experiments.

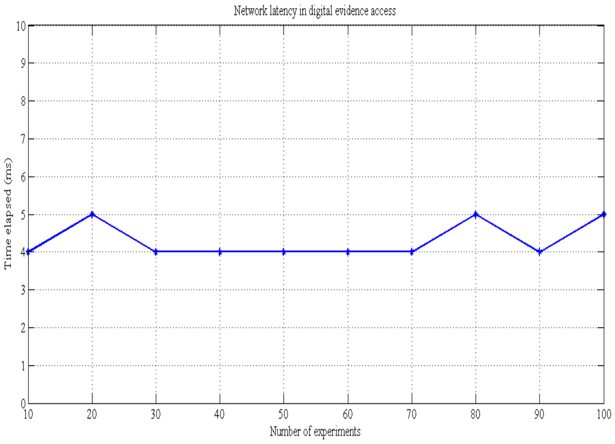

Fig. 11 Network latency in digital evidence access.

V. Conclusion

In this paper, we propose a blockchain-based system for intelligent digital forensics for ACVs in a connected smart world incorporating artificial intelligence and implement it on a local Etherium platform. The new emerging technologies of ACVs are facilitating the launch of a new era of intelligent transportation and fulfilling the growing demands of users. In terms of providing critical security to the network, our proposed AI-enabled blockchain digital forensics system plays an important role in ensuring the development of trust among multiple stakeholders. There exist a number of opportunities available to carry out further research in the field of security of ACVs. The enormous amount of data fetching into the central server and using blockchain and digital forensics techniques simultaneously may create system design opportunities for researchers that ensure the integrity and availability of the services. It is also a challenge for regulators and policymakers to forge the involvement of various stakeholders in the proposed system.

References

[1]. Li, Shancang, Tao Qin, and Geyong Min. "Blockchain-based digital forensics investigation framework in the Internet of Things and social systems." IEEE Transactions on Computational Social Systems 6, no. 6 (2019): 1433-1441.

[2]. Ruuhwan, Ruuhwan, Imam Riadi, and Yudi Prayudi. "Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology." International Journal of Electrical and Computer Engineering 7, no. 5 (2017): 2806.

[3]. Englbrecht, Ludwig, and Günther Pernul. "A privacy-aware digital forensics investigation in enterprises." In Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1-10. 2020.

[4]. Grigaliunas, Sarunas, Jevgenijus Toldinas, Algimantas Venckauskas, Nerijus Morkevicius, and Robertas Damasevicius. "Digital Evidence Object Model for Situation Awareness and Decision Making in Digital Forensics Investigation." IEEE Intelligent Systems (2020).

[5]. Shayau, Yazid Haruna, Aziah Asmawi, Siti Nurulain Mohd Rum, and Noor Afiza Mohd Ariffin. "Digital Forensics Investigation Reduction Model (DIFReM) Framework for Windows 10 OS." In 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), pp. 459-464. IEEE, 2019.

[6]. Abdullah, Haris Iskandar Mohd, Muhammad Zulhusni Mustaffa, Fiza Abdul Rahim, Zul-Azri Ibrahim, Yunus Yusoff, Salman Yussof, Asmidar Abu Bakar, Roslan Ismail, and Ramona Ramli. "Smart Grid Digital Forensics Investigation Framework." In 2020 8th International Conference on Information Technology and Multimedia (ICIMU), pp. 200-205. IEEE, 2020.

[7]. Ramadhani, Erika, Elyza G. Wahyuni, and Hanif R. Pratama. "Design of expert system for tool selection in digital forensics investigation." In IOP Conference Series: Materials Science and Engineering, vol. 852, no. 1, p. 012137. IOP Publishing, 2020.

[8]. Berdik, David, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh. "A survey on blockchain for information systems management and security." Information Processing & Management 58, no. 1 (2021): 102397.

[9]. Tanwar, Sudeep, Karan Parekh, and Richard Evans. "Blockchain-based electronic healthcare record system for healthcare 4.0 applications." Journal of Information Security and Applications 50 (2020): 102407.

[10]. Hasselgren, Anton, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, and Arild Faxvaag. "Blockchain in healthcare and health sciences—A scoping review." International Journal of Medical Informatics 134 (2020): 104040.

[11]. Frizzo-Barker, Julie, Peter A. Chow-White, Philippa R. Adams, Jennifer Mentanko, Dung Ha, and Sandy Green. "Blockchain as a disruptive technology for business: A systematic review." International Journal of Information Management 51 (2020): 102029.

[12]. Perera, Srinath, Samudaya Nanayakkara, M. N. N. Rodrigo, Sepani Senaratne, and Ralf Weinand. "Blockchain technology: Is it hype or real in the construction industry?." Journal of Industrial Information Integration 17 (2020): 100125.

[13]. Wamba, Samuel Fosso, and Maciel M. Queiroz. "Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities." (2020): 102064.

[14]. Sachin Sharma, Kamal Kumar Ghanshala, and Seshadri Mohan. "Blockchain-Based Internet of Vehicles (IoV): An Efficient Secure Ad Hoc Vehicular Networking Architecture." In 2019 IEEE 2nd 5G World Forum (5GWF), pp. 452-457. IEEE, 2019.

[15]. Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, and Joel JPC Rodrigues. "On the design of secure communication framework for blockchain-based Internet of intelligent battlefield things environment." In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 888-893. IEEE, 2020.

[16]. https://www.itu.int/en/myitu/News/2020/10/26/14/38/Self-driving-cars-autonomous-vehicles-Molly-Problem-AI-for-Good; see also https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/MollyProblem.aspx

[17]. https://github.com/ConsenSys/ethereum-developer-tools-list/blob/master/EcosystemResources.md accessed on 25 February 2021.